Hewlett Packard Enterprise Development LP

HPE BladeSystem c-Class Onboard Administrator Firmware

Firmware Version: 4.71

FIPS 140-2 Non-Proprietary Security Policy

FIPS Security Level: 1
Document Version: 1.2

Prepared for:

Hewlett Packard Enterprise

Hewlett Packard Enterprise Development LP
3000 Hanover Street
Palo Alto, CA 94304
United States of America

Phone: +1 281 370 0670
www.hpe.com

Prepared by:

Corsec

Corsec Security, Inc.

13921 Park Center Road, Suite 460
Herndon, VA 20171
United States of America

Phone: +1 703 267 6050
www.corsec.com

Table of Contents

List of Tables

List of Figures

1. Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the HPE BladeSystem c-Class Onboard Administrator Firmware from Hewlett Packard Enterprise Development LP (HPE), hereafter referred to in this document as OA Firmware, or the module.

This Security Policy describes how the HPE BladeSystem c-Class Onboard Administrator Firmware meets the security requirements of Federal Information Processing Standards (FIPS) Publication 140-2, which details the U.S.[1] and Canadian government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the National Institute of Standards and Technology (NIST) and the Communications Security Establishment (CSE) Cryptographic Module Validation Program (CMVP) website at http://csrc.nist.gov/groups/STM/cmvp.

This document also describes how to run the module in a secure FIPS-Approved mode of operation. This policy was prepared as part of the Level 1 FIPS 140-2 validation of the module.

1.2 References

This document deals only with operations and capabilities of the module in the technical terms of a FIPS 140-2 cryptographic module security policy. The following sources provide more information about the module:

- The HPE website (http://www.hpe.com) contains information on OA as well as the full line of products available from HPE.
- The CMVP website (http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm) contains contact information for individuals responsible for answering technical or sales-related questions for the module.

1.3 Document Organization

The Security Policy document is organized into two (2) primary sections. Section 2 provides an overview of the validated modules. This includes a general description of the modules' capabilities and their use of cryptography as well as a presentation of the validation level achieved in each applicable functional areas of the FIPS standard. It also provides high-level descriptions of how the modules meet FIPS requirements in each functional area. Section 3 documents the guidance needed for the secure use of the modules, including initial setup instructions, management methods, and applicable usage policies.

[1] U.S. – United States

2. HPE BladeSystem c-Class Onboard Administrator Firmware

2.1 Overview

The HPE BladeSystem c-Class Enclosure is a blade server enclosure designed to provide converged IT infrastructure while minimizing operational costs. The enclosure consolidates modular HPE ProLiant Gen10 server blades, interconnects, storage, power, and cooling components all into a single solution that can be managed as a unified environment.

The OA Firmware is the enclosure management solution used to support the HPE BladeSystem c-Class Enclosure and all the managed devices contained within the enclosure. It is designed to manage all power flow, cooling, connectivity, and access permissions for every component within the enclosure. This includes IP[2] addressing for the server blade's embedded Integrated Lights-Out (iLO) chip and the ability to access iLO management functionality from a single control plane. Onboard Administrator also provides basic management for other enclosure components such as interconnect modules, Virtual Connect (VC) modules, power supply modules, and fan modules.

Onboard Administrator also provides configuration information for the enclosure, enables run-time management and configuration of the enclosure components, and informs administrators of problems within the enclosure through email or the Insight Display. Several features are provided to simplify the management of the server blades and interconnects. The BladeSystem c-Class Enclosures can also be configured with a redundant Onboard Administrator module enabling uninterrupted manageability of the entire enclosure and server blades in the event of a failure of the primary OA or a network outage.

The OA Firmware cryptographic module is designed to run on the HPE BladeSystem BLc7000 OA (with KVM Option) installed in an HPE BladeSystem c-Class Enclosure.

The OA Firmware is validated at the FIPS 140-2 Section levels shown in Table 1.

Table 1 – Security Level per FIPS 140-2 Section

Section	Section Title	Level
1	Cryptographic Module Specification	1
2	Cryptographic Module Ports and Interfaces	1
3	Roles, Services, and Authentication	2
4	Finite State Model	1
5	Physical Security	1
6	Operational Environment	N/A
7	Cryptographic Key Management	1
8	EMI/EMC[3]	1
9	Self-tests	1
10	Design Assurance	1

[2] IP – Internet Protocol

[3] EMI/EMC – Electromagnetic Interference / Electromagnetic Compatibility

Section	Section Title	Level
11	Mitigation of Other Attacks	N/A

2.2 Module Specification

The OA Firmware is a firmware module with a multiple-chip standalone embodiment. The overall security level of the module is 1. The module is designed to run on the HPE BladeSystem BLc7000 Onboard Administrator blade (with KVM Option) installed in an HPE BladeSystem c-Class Enclosure.

The module implements the FIPS-Approved algorithms listed in Table 2 and Table 3 below.

Table 2 – FIPS-Approved Algorithm Implementations ("FIPS Mode ON")

CAVP Cert	Algorithm	Standard	Mode/Method	Key Lengths, Curves, or Moduli	Use
4776	AES[4]	FIPS PUB 197, NIST SP 800-38A	CBC[5]	128, 192, 256	Data Encryption/Decryption
			CTR[6]	128, 192, 256	Data Encryption/Decryption
			ECB[7]	128, 192, 256	Data Encryption/Decryption
			CFB[8]128	128	Data Encryption/Decryption
4776	AES	FIPS PUB 197 NIST SP 800-38D	GCM[9]	128, 256	Data Encryption/Decryption and Authentication
1421 1422 1423	CVL	NIST SP 800-135rev1	TLSv1.2, SSH, SNMPv3	-	Key Derivation No parts of the TLS, SSH, or SNMP protocols, other than the KDFs, have been tested by the CAVP and CMVP.
1500	CVL	NIST SP 800-56A	Partial DH (ECC)	P-224, P-256, P-384, P-521	Shared Secret Computation
1654	DRBG[10]	NIST SP 800-90A	CTR	-	Deterministic Random Bit Generation The module supports CTR_DRBG only with a derivation function.
3186	HMAC[11]	FIPS PUB 198-1	HMAC-SHA-1, HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512	160, 224, 256, 384, 512	Message Authentication

[4] AES – Advance Encryption Standard
[5] CBC – Cipher Block Chaining
[6] CTR – Counter
[7] ECB – Electronic Codebook
[8] CFB – Cipher Feedback
[9] GCM – Galois Counter Mode
[10] DBRG – Deterministic Random Bit Generator
[11] HMAC – (keyed-) Hashed Message Authentication Code

CAVP Cert	Algorithm	Standard	Mode/Method	Key Lengths, Curves, or Moduli	Use
2617	RSA[12]	FIPS PUB 186-4	SHA[13]-224, SHA-256, SHA-384, SHA-512	2048	Key Pair Generation
			SHA-224, SHA-256, SHA-384, SHA-512	2048	Signature Generation and Verification
2617	RSA	FIPS PUB 186-2	SHA-1	2048	Signature Verification
3920	SHS[14]	FIPS PUB 180-4	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	-	Message Digest
3921	SHS	FIPS PUB 180-4	SHA-1	-	Message Digest
3922	SHS	FIPS PUB 180-4	SHA-256	-	Message Digest
2538	Triple-DES[15]	NIST SP 800-67	TCBC[16], TECB[17]	112	Data Encryption/Decryption The TLS protocol governs the generation of Triple-DES keys. Refer to RFC2246, RFC4346, and RFC 5246 for details relevant to the generation of the Triple-DES keys. The user is responsible for ensuring the module limits the number of encryptions with the same key to 2^{32}.
Vendor Affirmation	CKG[18]	NIST SP 800-133	-	-	Key Generation Symmetric keys and generated seeds are produced using unmodified output from the approved DRBG.

Table 3 – FIPS-Approved Algorithm Implementations (“FIPS Mode TOP-SECRET”)

CAVP Cert	Algorithm	Standard	Mode/Method	Key Lengths, Curves, or Moduli	Use
4776	AES	FIPS PUB 197, NIST SP 800-38A	CBC	256	Data Encryption/Decryption
4776	AES	NIST SP 800-38D	GCM	256	Data Encryption/Decryption and Authentication

[12] RSA – Rivest, Shamir, Adleman
[13] SHA – Secure Hash Algorithm
[14] SHS – Secure Hash Standard
[15] DES – Data Encryption Standard
[16] TCBC – Triple DES CBC
[17] TECB – Triple DES ECB
[18] CKG – Cryptographic Key Generation

CAVP Cert	Algorithm	Standard	Mode/Method	Key Lengths, Curves, or Moduli	Use
1421 1422	CVL	NIST SP 800-135rev1	TLSv1.2, SSH		Key Derivation No parts of the TLS or SSH protocols, other than the KDFs, have been tested by the CAVP and CMVP.
1500	CVL	NIST SP 800-56A	Partial DH (ECC)	P-384	Shared Secret Computation
1654	DRBG	NIST SP 800-90A	CTR	-	Deterministic Random Bit Generation
1201	ECDSA[19]	FIPS PUB 186-4	-	P-224, P-384	Key Pair Generation
			-	P-224, P-384	Signature Generation and Verification
3186	HMAC	FIPS PUB 198-1	HMAC-SHA-384	384	Message Authentication
2617	RSA	FIPS PUB 186-4	SHA-384	3072	Key Pair Generation
			SHA-384	3072	Signature Generation and Verification
3920	SHS	FIPS PUB 180-4	SHA-384	-	Message Digest
3921	SHS	FIPS PUB 180-4	SHA-1	-	Message Digest
3922	SHS	FIPS PUB 180-4	SHA-256	-	Message Digest
Vendor Affirmation	CKG	NIST SP 800-133	-	-	Key Generation Symmetric keys and generated seeds are produced using unmodified output from the approved DRBG.

The module implements the Allowed algorithms listed Table 4 below.

Table 4 – Allowed Algorithm Implementations

Algorithm	Caveat	Use
RSA key transport	Key establishment methodology provides 112 or 128 bits of encryption strength	Key wrapping
Diffie-Hellman	Key establishment methodology provides 112 or 128 bits of encryption strength	Key agreement
Elliptic Curve Diffie-Hellman	Key establishment methodology provides between 112 and 256 bits of encryption strength	Key agreement
NDRNG (/dev/urandom)	-	Seeding for the DRBG. The entropy source provides a min-entropy of 7.88 out of 8 bits.
MD5	-	TLS 1.0/1.1

[19] ECDSA – Elliptic Curve Digital Signature Algorithm

2.2.1 Physical Cryptographic Boundary

As a firmware module, OA has no physical characteristics; however, the physical boundary of the cryptographic module is defined by the hardware on which it runs.

The cryptographic module was tested and found compliant on the HPE BLc7000 Onboard Administrator with KVM Option (P/N[20] 456204-B21). The module firmware executes on an AMCC PowerPC (PPC) 440EPx embedded processor. The module's physical cryptographic boundary is the physical perimeter of the BLc7000 Onboard Administrator with KVM Option hardware. This boundary fully encloses the processors and other hardware components that store and protect the firmware module. Figure 1 below shows a front view of the hardware blade; Figure 2 presents a hardware block diagram of the blade.

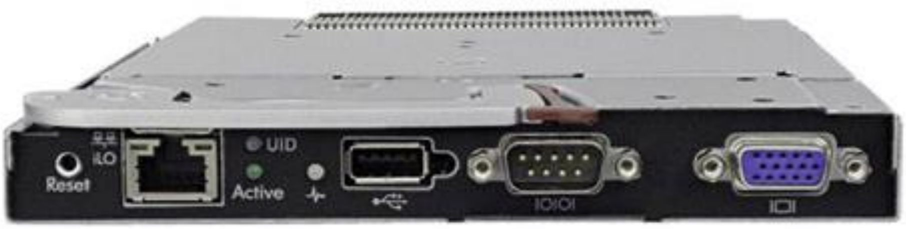
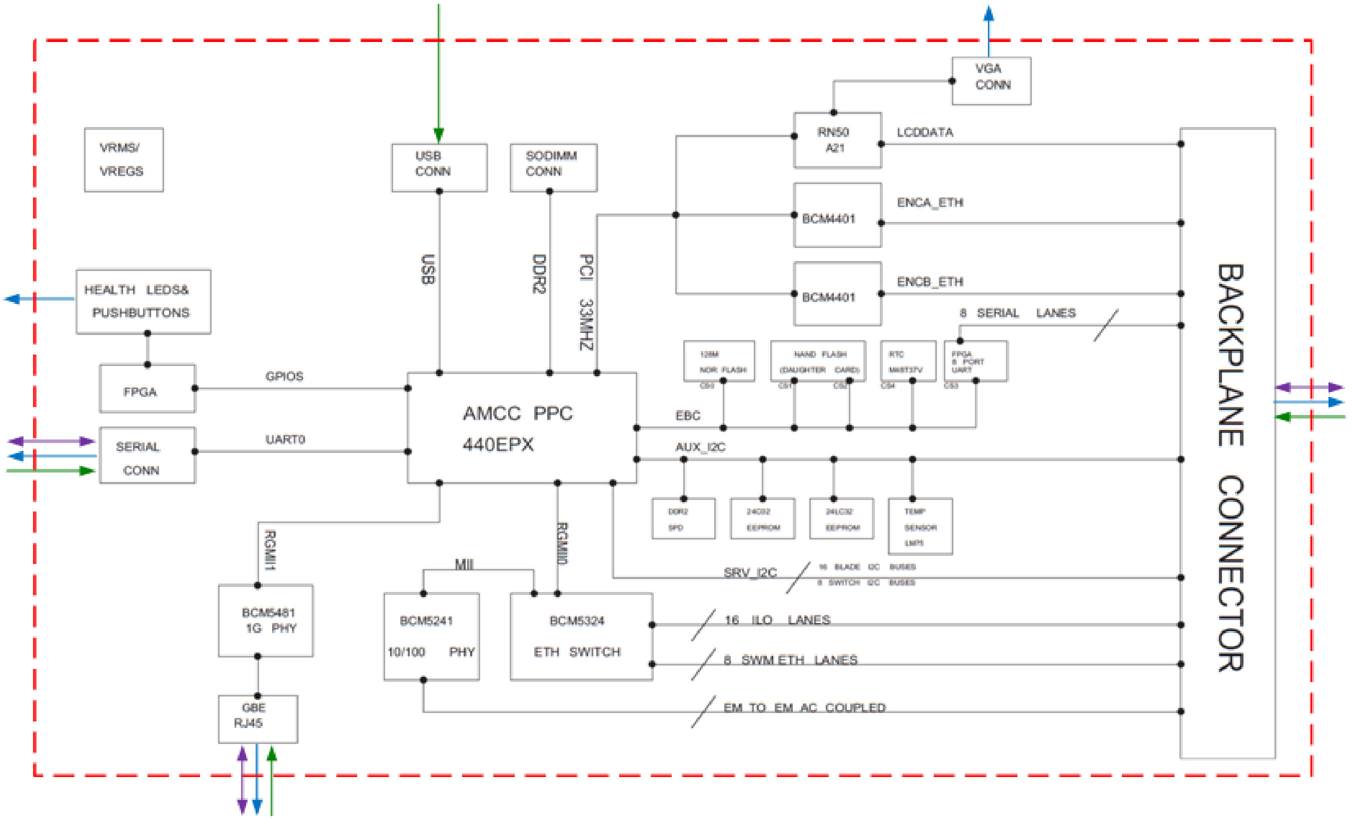


Figure 1 – BLc7000 Onboard Administrator with KVM Option (P/N 456204-B21)

[20] P/N – Part Number



LEGEND:

Data In/Out ⟷
Control input ←
Status output →
Crypto boundary – – –

KEY:

AUX – Auxiliary
CONN – Connector
DDR – Double Data Rate
ECB – External Peripheral Bus Controller
EEPROM – Electrically Erasable Programmable
Read-Only Memory
ETH – Ethernet
FPGA – Field-Programmable Gate Array
G – Gigabit
GBE – Gigabit Ethernet
I2C – Inter-Intergrated Circuit
MHZ – Megahertz
MII – Media Independent Interface
PCI – Peripheral Component Interconnect
PHY – Physical Layer
PPC – PowerPC
RJ45 – Registered Jack 45
SODIMM – Small Outline Dual Inline Memory Module
UART – Universal Asynchronous Receiver Transmitter

Figure 2 – Hardware Block Diagram for BLc7000 Onboard Administrator Blade

2.2.2 Logical Cryptographic Boundary

The logical cryptographic boundary is drawn around the firmware executing on the hardware blade's Central Processing Unit (CPU), while the physical cryptographic boundary of the module is drawn around the hardware blade. The boundary depicted in Figure 3 below.

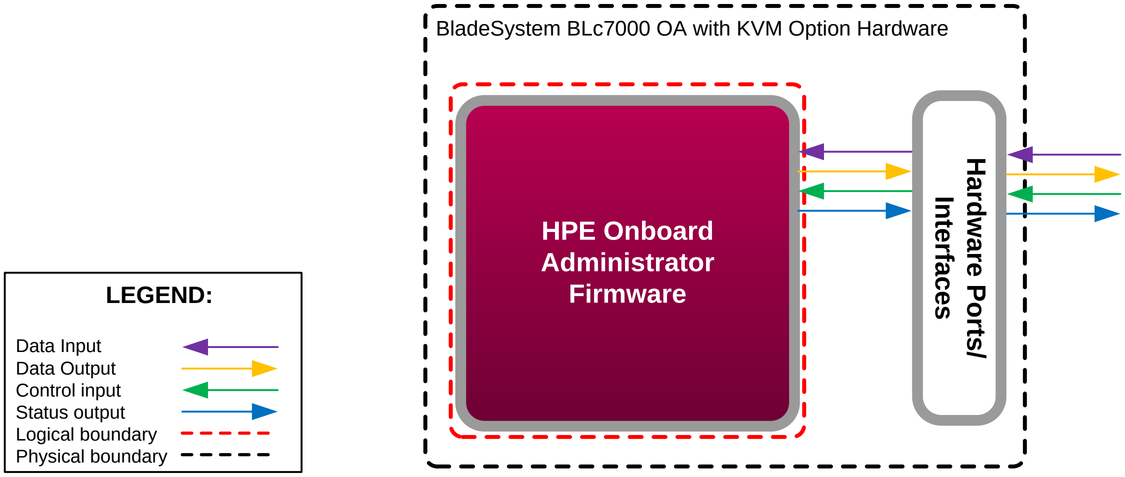

BladeSystem BLc7000 OA with KVM Option Hardware
HPE Onboard Administrator Firmware
Hardware Ports/ Interfaces
LEGEND:
Data Input
Data Output
Control input
Status output
Logical boundary
Physical boundary

Figure 3 – HPE Onboard Administrator Firmware Cryptographic Boundary

2.3 Module Interfaces

OA Firmware implements distinct module interfaces in its firmware design. Physically, the module ports and interfaces are those of the hardware blade that the firmware runs upon. Logically, the firmware is accessible via a CLI[21] (Serial or SSH) or GUI[22] (HTTPS) which allow it to receive requests and execute function calls for cryptographic and administrative services. In addition, the module provides support for SNMPv3 and LDAP over TLS. The module also provides other logical inputs and outputs such as menu controls, keyboard and mouse input, display output, and status signals. These interfaces can be categorized into the following logical interfaces defined by FIPS 140-2:

- Data Input Interface
- Data Output Interface
- Control Input Interface
- Status Output Interface

The module's physical and electrical characteristics, manual controls, and physical indicators are provided by the host platform. The module's hardware platform offers the following physical interfaces:

- Ethernet RJ45 connector
- Serial RS232 DB-9 connector with PC23 standard pinout
- Backplane connector
- Reset button
- USB 2.0 Type A connector
- Insight Display LCD and LCD Buttons
- VGA DB-15 connector with PC standard pinout
- Backplane connector
- LED indicators
- Power interface

[21] CLI – Command Line Inteface
[22] GUI – Graphical User Interface
[23] PC – Personal Computer

The module's operating system controls and directs all interactions between the operator and the module, and is responsible for mapping the blade's physical interfaces to the module's logical input/output mechanisms. The mapping of FIPS 140-2 logical interfaces in the firmware to the module's logical interfaces is described in Table 5.

Table 5 – FIPS 140-2 Logical Interface Mappings

FIPS 140-2 Interface	Physical Port/Interface	Logical Port/Interface
Data Input	• Ethernet RJ45 connector • Serial RS232 DB-9 connector with PC[24] standard pinout • Backplane connector	Application inputs via operator interfaces (GUI, CLI) and network interfaces
Data Output	• Ethernet RJ45 connector • Serial RS232 DB-9 connector with PC standard pinout • Backplane connector	Application outputs to operator interfaces (GUI, CLI) and network interfaces
Control Input	• Ethernet RJ45 connector • Serial RS232 DB-9 connector with PC standard pinout • Reset button • USB 2.0 Type A connector • Insight Display LCD Buttons • Backplane connector	Application management commands and command parameter inputs via operator interfaces (GUI, CLI)
Status Output	• Ethernet RJ45 connector • Serial RS232 DB-9 connector with PC standard pinout • VGA DB-15 connector with PC standard pinout • Backplane connector • LED indicators • Insight Display LCD	Application management command status/output returns
Power Interface	Power Interface	Not Applicable

2.4 Roles and Services

The sections below describe the module's roles and services.

2.4.1 Authorized Roles

There are two roles in the module (as required by FIPS 140-2) that operators may assume: a Crypto-Officer (CO) role and a User role. See the *HPE BladeSystem Onboard Administrator User Guide* and *HPE BladeSystem Onboard Administrator Command Line Interface User Guide* for more information about the roles and services provided by OA Firmware. Roles are explicitly assumed by authenticating to an account associated with a particular role.

- CO Role – The CO role can create User accounts, define permissions, change passwords, and take the module into or out of a FIPS mode of operation. The CO maps to the "Administrator" and "OA Administrator" account classifications, as defined in the *HPE BladeSystem Onboard Administrator User Guide* and *HPE BladeSystem Onboard Administrator Command Line Interface User Guide*.

- User Role – The User role can perform management operations for the BladeSystem c-Class Enclosure, as defined by their user permissions, via interfaces secured by the cryptographic configuration of the module. The User maps to the "OA operator", "operator", "OA user", and "user" account classifications, as defined

[24] PC – Personal Computer

in the *HPE BladeSystem Onboard Administrator User Guide* and *HPE BladeSystem Onboard Administrator Command Line Interface User Guide*.

Descriptions of the services available to the CO and User roles are provided in Table 6 below. The CO has access to all the services of the User.

2.4.2 Operator Services

Descriptions of the module's available services are listed in Table 6 below. Please note that the keys and Critical Security Parameters (CSPs) listed indicate the type of access required using the following notation:

- R – Read: The CSP is read.
- W – Write: The CSP is established, generated, modified, or zeroized.
- X – Execute: The CSP is used within an Approved or Allowed security function or authentication mechanism.

Table 6 – Module Services by Role

Service / Approved Mode	Role		Description	Input	Output	CSP and Type of Access
	CO	User				
Create/modify users (All modes)	✓		Create, edit, and delete users; define user accounts and assign permissions.	Command to create a new user with credentials/permissions.	User successfully created with established credentials/permissions.	None
Change CO credentials (All modes)	✓		Change the CO credentials (password or certificate) or permissions.	Command to change password, certificate, or permissions.	Change CO credential/permissions.	Operator password – W Operator certificate – W
Change user credentials (All modes)	✓	✓	Change the User password or certificate.	Command to change password or certificate.	Change User password or certificate.	Operator password – W Operator certificate – W
Access the GUI (FIPS Mode ON)	✓	✓	Access the GUI via HTTPS connection through web browser.	Command to begin HTTPS connection via web browser.	Connection is established and administration page appears.	TLS Session Authentication key – WX TLS Session Encryption key – WX TLS Pre-Master Secret – WX TLS Master Secret – WX RSA Public/Private Keypair – X DH Public/Private Components – X AES-GCM IV – WX

Service / Approved Mode	Role		Description	Input	Output	CSP and Type of Access
	CO	User				
Access the GUI (FIPS Mode TOP SECRET)	✓	✓	Access the GUI via HTTPS connection through web browser.	Command to begin HTTPS connection via web browser.	Connection is established and administration page appears.	TLS Session Authentication key – WX TLS Session Encryption key – WX TLS Pre-Master Secret – WX TLS Master Secret – WX RSA Public/Private Keypair – X DH Public/Private Components – X ECDSA Public/Private Keypair – X ECDH Public/Private Components – X AES-GCM IV – WX
Access the CLI (FIPS Mode ON)	✓	✓	Manage the module using the CLI accessed via SSH protocol over Ethernet, or directly via Serial interface.	Command to begin SSH session.	CLI session established.	SSH Session Authentication Key – WX SSH Session Encryption Key – WX SSH Shared Secret – WX RSA Public/Private Keypair – X ECDSA Public/Private Keypair – X ECDH Public/Private Components – X DH Public/Private Components – X AES-GCM IV – WX
Access the CLI (FIPS Mode TOP SECRET)	✓	✓	Manage the module using the CLI accessed via SSH protocol over Ethernet, or directly via Serial interface.	Command to begin SSH session.	CLI session established.	SSH Session Authentication Key – WX SSH Session Encryption Key – WX SSH Shared Secret – WX ECDSA Public/Private Keypair – X ECDH Public/Private Components – X AES-GCM IV – WX
Authenticate to the module (All modes)	✓	✓	Assume the CO or User role by supplying authentication credentials.	Username and password or certificate.	Status output.	Operator Password – X Operator Certificate – X
Access the SNMPv3 interface (FIPS Mode ON)	✓	✓	Manage the module remotely and provide non-security relevant information about the module's state and statistics.	None.	Status output.	SNMPv3 Privacy Key – RX SNMPv3 Authentication Key – RX
Zeroize keys (All modes)	✓		Overwrite existing keys and regenerate all cryptographic keys.	GENERATE KEY ALL command in the CLI.	All keys are zeroized and regenerated.	All keys – W

Service / Approved Mode	Role		Description	Input	Output	CSP and Type of Access
	CO	User				
Set FIPS mode (All modes)	✓		Enable/disable FIPS mode of operation. Calls the set factory defaults service.	CLI command: SET FIPS MODE ON/OFF/TOP_SECRET. GUI Interface: FIPS Mode ON" or "FIPS Mode Top -Secret". Requires reboot of module hardware.	Set Factory Defaults service is called. Keys zeroized, OA reboots. New TLS and SSH keys are generated. Module boots in FIPS Approved mode.	All keys – W
Show FIPS mode status (All modes)	✓		Display FIPS status of module.	CLI command: SHOW FIPS MODE. GUI Interface: If "FIPS Mode ON" or "FIPS Mode Top-Secret" is selected.	CLI: FIPS Mode is On or FIPS Mode is Top Secret. GUI: Status icon is displayed.	None
Perform self-tests on demand (All modes)	✓		Run self-tests on demand.	None.	Status output.	None
Generate certificate signing request (FIPS Mode ON)	✓		Generate an X.509 Certificate signing request.	Command to generate certificate signing request.	Generated certificate signing request.	RSA Public/Private Keypair – X
Generate certificate signing request (FIPS Mode TOP SECRET)	✓		Generate an X.509 Certificate signing request.	Command to generate certificate signing request.	Generated certificate signing request.	RSA Public/Private Keypair – X ECDSA Public/Private Keypair – X
Update firmware (All modes)	✓	✓	Update the module firmware.	Command to update firmware from the web GUI and the image to use.	Firmware is updated and the module is out of FIPS mode.	Firmware Load Test Key – X
Key encapsulation (All modes)	✓	✓	Perform key wrapping operation.	Data to encrypt and encryption key.	Encrypted data.	RSA Public Key – X

Service / Approved Mode	Role		Description	Input	Output	CSP and Type of Access
	CO	User				
Key unencapsulation (All modes)	✓	✓	Perform key unwrapping operation.	Data to decrypt and decryption key.	Decrypted plaintext data.	RSA Private Key – X
Generate digital signature (FIPS Mode ON)	✓	✓	Generate a signature.	Data to sign.	Digitally signed data.	RSA Public/Private Key – WX
Generate digital signature (FIPS Mode TOP SECRET)	✓	✓	Generate a signature.	Data to sign.	Digitally signed data.	RSA Public/Private Key – WX ECDSA Public/Private key – WX
Verify digital signature (FIPS Mode ON)	✓	✓	Verify the digital signature attached to data.	Data to verify.	Hash value of data to be verified.	RSA Public/Private key – WX
Verify digital signature (FIPS Mode TOP SECRET)	✓	✓	Verify the digital signature attached to data.	Data to verify.	Hash value of data to be verified.	RSA Public/Private Key – WX ECDSA Public/Private key – WX
Generate symmetric keys (FIPS Mode ON)	✓	✓	Calls the DRBG to generate symmetric keys.	DRBG parameters.	Key of requested size.	Entropy Input String – RX DRBG Key – X DRBG V Value – X DRBG Seed – RWX TLS Session Encryption key (AES-CBC, AES-GCM, TDES-CBC) – W SSH Session Encryption key (AES-CBC, AES-CTR, AES-GCM, TDES-CBC) – W
Generate symmetric keys (FIPS Mode TOP SECRET)	✓	✓	Calls the DRBG to generate symmetric keys.	DRBG parameters.	Key of requested size.	Entropy Input String – RX DRBG Key – X DRBG V Value – X DRBG Seed – RWX TLS Session Encryption key (AES-CBC, AES-GCM) – W SSH Session Encryption key (AES-GCM) – W
Generate asymmetric keys (FIPS Mode ON)	✓	✓	Call the DRBG for primes/keying material.	DRBG parameters.	Key or prime of requested size.	Entropy Input String – RX DRBG Key – X DRBG V Value – X DRBG Seed – RWX RSA Public/Private Key – W

Service / Approved Mode	Role		Description	Input	Output	CSP and Type of Access
	CO	User				
Generate asymmetric keys (FIPS Mode TOP SECRET)	✓	✓	Call the DRBG for primes/keying material.	DRBG parameters.	Key or prime of requested size.	Entropy Input String – RX DRBG Key – X DRBG V Value – X DRBG Seed – RWX RSA Public/Private key – W ECDSA Public/Private key – W

For more information on the non-security relevant services of the module, please refer to the *HPE BladeSystem Onboard Administrator User Guide* (https://h20566.www2.hpe.com/hpsc/doc/public/display?docId=c00705292) and *HPE BladeSystem Onboard Administrator Command Line Interface User Guide* (https://h20565.www2.hpe.com/hpsc/doc/public/display?docId=c00702815).

2.4.3 Authentication

The module implements role-based authentication using password-based and certificate-based mechanisms. Crypto Officer and User accounts each have a unique username and password or user certificate assigned to them. Role selection is accomplished explicitly by successfully authenticating to the Crypto Officer or User role using valid credentials that are associated with the desired role's account.

The password-based mechanism uses locally or remotely (e.g. LDAP[25]) stored username and password combination. For the local authentication mechanism, roles are assigned to a user account by the CO. Strong passwords are automatically enabled in an Approved mode of operation and cannot be disabled. When enabled, passwords must be a minimum of 8 characters in length and must contain at least one character from three of the four categories: uppercase, lowercase, numeric, and non-alphanumeric. For the remote LDAP authentication mechanism, similar password strength enforcement rules must be used.

The certificate-based mechanism employs user certificates (and optionally Common Access Cards (CAC)) issued by a trusted certificate authority. Roles can be assigned to a local user account or assigned through a CO configured mapping to an LDAP directory group. When certificate authentication is used, the authentication attempt must be made with a valid certificate issued by a trusted authority and containing a *Subject Name* or *Subject Alternate Name* matching an authorized local or remote user account.

Table 7 provides the strength of the authentication mechanisms used by the module.

[25] LDAP – Lightweight Directory Access Protocol

Table 7 – Authentication Mechanism Used by the Module

Authentication Type	Strength
Username/Password (local)	Once properly configured, the minimum length of the password is 8 characters, with 94 different case-sensitive alphanumeric characters and symbols possible for usage. Assuming the worst case of a minimum password length of 8 characters, with characters selected from three of the four categories (reducing the total character set to 62), the chance of a random attempt falsely succeeding is: 1: (62^8), or 1: 218,340,105,584,896 Which is less than 1:1,000,000 as required by FIPS 140-2. The fastest network connection supported by the module (for management) is 1 Gbps. Hence at most (1,000,000,000 bits × 60 seconds) 6 x 10^{10} bits of data can be transmitted to the module in one minute (assuming no overhead). Each password attempt is (8 bits x 8 characters) 64 bits in length, meaning (6 x 10^{10}/64) 9.38 x 10^8 password attempts can be made in one minute. Therefore, the probability that a random attempt will succeed or a false acceptance will occur in one minute is: 1: (62^8 possible passwords / 9.38 x 10^8 passwords per minute) 1: 232,896 Which is less than 1:100,000 within one minute as required by FIPS 140-2.
Username/Password (remote)	Assuming the same password complexity is enforced by the LDAP server, the same estimates apply to remote authentication as with local authentication.
Certificate/CAC authentication	Assuming a worst case with a 2048-bit RSA keypair used for certificate authentication yielding an equivalent 112 bits of strength, the chance of a random authentication attempt falsely succeeding is: 1: (2^{112}), or 1: 5.1922968585348276285304963292201e+33 Which is less than 1:1,000,000 as required by FIPS 140-2. The fastest network connection supported by the module (for management) is 1 Gbps. Hence at most (1,000,000,000 bits × 60 seconds) 6 x 10^{10} bits of data can be transmitted to the module in one minute (assuming no overhead). Each attempt is 112 bits in length, meaning (6 x 10^{10} bits/112) 5.36 x 10^8 attempts can be made in one minute. Therefore, the probability that a random attempt will succeed or a false acceptance will occur in one minute is: 1: (2^{112} possible keys / 5.36 x 10^8 keys per minute) 1: 9.69 x 10^{24} Which is less than 1:100,000 within one minute as required by FIPS 140-2.

2.5 Physical Security

As a multi-chip standalone firmware module, the module relies on the HPE BLc7000 Onboard Administrator blade (with KVM Option) installed in an HPE BladeSystem c7000 enclosure to provide the mechanisms necessary to meet

FIPS 140-2 level 1 physical security requirements. All components of the hardware are made of production-grade materials, and all integrated circuits are coated with commercial standard passivation.

Additionally, the HPE BladeSystem c7000 enclosure hardware including the BLc7000 OA hardware has been tested for and meets applicable Federal Communications Commission (FCC) Electromagnetic Interference and Electromagnetic Compatibility requirements for business use as defined in Subpart B of FCC Part 15.

2.6 Operational Environment

The operational environment requirements of FIPS 140-2 do not apply to the OA Firmware. The OS[26] included in the firmware does not allow the loading of new applications; therefore, the operational environment of the module is a non-modifiable operational environment.

[26] OS – Operating System

2.7 Cryptographic Key Management

The module supports the CSPs listed below in Table 8.

Table 8 – Cryptographic Keys, Cryptographic Key Components, and CSPs

CSP	CSP Type / Approved Mode	Generation / Input	Output	Storage	Zeroization	Use
SSH/TLS Session Authentication Key	**FIPS Mode On:** HMAC-SHA-1 HMAC-SHA-256 HMAC-SHA-512 AES-128 GCM AES-256 GCM **FIPS Mode Top Secret:** AES-256 GCM HMAC-SHA-384	Derived from SSH Shared Secret or TLS Pre-Master Secret	Never output from module	Plaintext in volatile RAM	End session, power cycle, host reboot, factory reset, or leaving a FIPS-Approved mode	SSH/TLS session authentication
SSH Session Encryption Key	**FIPS Mode ON:** AES-128 AES-192 AES-256 Triple-DES **FIPS Mode Top Secret:** AES-256 GCM	Derived from SSH Shared Secret	Never output from module	Plaintext in volatile RAM	End session, power cycle, host reboot, factory reset, or leaving a FIPS-Approved mode	Encryption/Decryption for SSH sessions
SSH Shared Secret	Shared secret	Established using Diffie-Hellman or Elliptic Curve Diffie-Hellman key agreement	Never output from module	Plaintext in volatile RAM	End session, power cycle, host reboot, factory reset, or leaving a FIPS-Approved mode	Used to derive SSH Session Authentication Key and SSH Session Encryption Key

CSP	CSP Type / Approved Mode	Generation / Input	Output	Storage	Zeroization	Use
TLS Session Encryption Key	**FIPS Mode ON:** AES-128 AES-256 AES-128 GCM AES-256 GCM Triple-DES **FIPS Mode Top Secret:** AES-256 GCM	Derived from TLS Pre-Master Secret	Never output from module	Plaintext in volatile RAM	End session, power cycle, host reboot, factory reset, or leaving a FIPS-Approved mode	Encryption/ Decryption for TLS sessions
TLS Pre-Master Secret	Pre-master secret for TLS	Established using Diffie Hellman key agreement, Elliptic Curve Diffie-Hellman key agreement, or RSA key transport	Never output from module	Plaintext in volatile RAM	End session, power cycle, host reboot, factory reset, or leaving a FIPS-Approved mode	Derivation of TLS Master Secret
TLS Master Secret	Master secret for TLS	Derived from TLS Pre-Master Secret	Never output from module	Plaintext in volatile RAM	End session, power cycle, host reboot, factory reset, or leaving a FIPS-Approved mode	Derivation of TLS Session Authentication Key and TLS Session Encryption Key

CSP	CSP Type / Approved Mode	Generation / Input	Output	Storage	Zeroization	Use
AES GCM IV[27]	96-bit IV	**TLS:** Internally generated deterministically in compliance with TLSv1.2 GCM cipher suites as specified in RFC 5288 and Section 8.2.1 of NIST SP 800-38D. When the nonce_explicit part of the IV exhausts the maximum number of possible values for a given session key, the module will trigger a handshake to establish a new encryption key according to RFC 5246. **SSH:** Internally generated randomly using approved DRBG.	Never output from the module.	Plaintext in volatile RAM	End session, power cycle	IV input to AES GCM function Supported TLSv1.2 GCM ciphersuites: TLS_RSA_WITH_AES_128_GCM_SHA256 TLS_RSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
RSA Private Key	**FIPS Mode ON:** RSA-2048 **FIPS Mode Top Secret:** RSA-3072	Internally generated – Generated by call during first boot	Never output from module	Plaintext in Flash memory	Factory reset, leaving a FIPS-Approved mode, or GENERATE KEY command	Signature generation, decryption, key establishment, certificate generation (TLS sessions), TLS and SSH authentication
RSA Public Key	**FIPS Mode ON:** RSA-2048 **FIPS Mode Top Secret:** RSA-3072	Internally generated – Generated by call during first boot	Output from module via Data Output interface in plaintext	Plaintext in Flash memory	Factory reset, leaving a FIPS-Approved mode, or GENERATE KEY command	Signature verification, encryption, key exchange with 2048-bit or 3072-bit only, certificate generation (TLS sessions), TLS and SSH authentication

[27] IV – Initialization Vector

CSP	CSP Type / Approved Mode	Generation / Input	Output	Storage	Zeroization	Use
ECDSA Private Key	**FIPS Mode Top Secret:** P-384	Internally generated	Never output from module	Plaintext in Flash memory	Factory reset, leaving a FIPS-Approved mode, or GENERATE KEY command	Key establishment (TLS, SSH sessions)
ECDSA Public Key	**FIPS Mode Top Secret:** P-384	Internally generated	Output from module via Data Output interface in plaintext	Plaintext in Flash memory	Factory reset, leaving a FIPS-Approved mode, or GENERATE KEY command	Key establishment (TLS, SSH sessions)
Entropy Input String	256-bit random value	Gathered from system entropy (/dev/urandom)	Never output from module	Plaintext in NVRAM[28]	Removing NVRAM battery, host reboot	Seed generation for the DRBG
DRBG Seed	384-bit random value	Internally generated using entropy input string	Never output from module	Plaintext in NVRAM	Removing NVRAM battery, host reboot	Random number generation using the DRBG
DRBG V Value	DRBG internal state value	Internally generated using entropy input string	Never output form module	Plaintext in volatile RAM	Uninstantiate function, host reboot	DRBG Internal state value
DRBG Key	DRBG key	Internally generated using entropy input string	Never output from module	Plaintext in volatile RAM	Uninstantiate function, host reboot	DRBG internal state value
DH Public Components	**FIPS Mode ON:** 2048-bit modulus **FIPS Mode Top Secret:** 3072-bit modulus	Internally generated	Output from module via Data Output interface in plaintext	Plaintext in volatile RAM	End session, power cycle, host reboot, factory reset, leaving a FIPS-Approved mode, or GENERATE KEY command	Key establishment (TLS, SSH sessions)
DH Private Components	**FIPS Mode ON:** 2048-bit modulus **FIPS Mode Top Secret:** 3072-bit modulus	Internally generated	Never output from module	Plaintext in volatile RAM	End session, power cycle, host reboot, factory reset, leaving a FIPS-Approved mode, or GENERATE KEY command	Key establishment (TLS, SSH sessions)
ECDH Public Components	**FIPS Mode ON:** P-256, P-384, P-512 **FIPS Mode Top Secret:** P-384	Internally generated	Output from module via Data Output interface in plaintext	Plaintext in volatile RAM	End session, power cycle, host reboot, factory reset, leaving a FIPS-Approved mode, or GENERATE KEY command	Key establishment (TLS, SSH sessions)

[28] NVRAM – Non-volatile Random Access Memory

CSP	CSP Type / Approved Mode	Generation / Input	Output	Storage	Zeroization	Use
ECDH Private Components	**FIPS Mode ON:** P-256, P-384, P-512 **FIPS Mode Top Secret:** P-384	Internally generated	Never output from module	Plaintext in volatile RAM	End session, power cycle, host reboot, factory reset, leaving a FIPS-Approved mode, or GENERATE KEY command	Key establishment (TLS, SSH sessions)
SNMPv3 Privacy Key	**FIPS Mode ON:** AES-128	Internally generated	Never output from module	Plaintext in volatile RAM	End session, power cycle, host reboot, factory reset, leaving a FIPS-Approved mode, or GENERATE KEY command	Encryption of SNMPv3 packets
SNMPv3 Authentication Key	**FIPS Mode ON:** HMAC-SHA-1-96	Internally generated	Never output from module	Plaintext in volatile memory	End session, power cycle, host reboot, factory reset, leaving a FIPS-Approved mode, or GENERATE KEY command	Authenticating SNMPv3 packets.
Operator Password	Minimum of eight characters of alphanumeric string	Initial CO password hardcoded, password changes input by operator over TLS or SSH	Never output from the module	Plaintext in Flash memory and in RAM	Zeroized when the password is updated with a new one or during factory reset	Operator authentication
Operator Certificate	Public key (RSA, ECDSA) associated with operator certificate	Input by CO via TLS or SSH	Never output from the module	Plaintext in Flash memory and in RAM	Zeroized when the certificate validation and user authentication process is complete	Operator authentication
Firmware Load Test Key	RSA 2048-bit public key	Hard-coded	Never output from the module	Embedded with module firmware	N/A	Firmware load test

2.8 Self-Tests

Once the module has been configured per section 3.1 below cryptographic self-tests are performed automatically and without operator intervention by the module when it is powered on. In addition, conditional tests are run when a random number or asymmetric key pair is created. The following sections list the self-tests performed by the module, their expected error status, and the error resolutions.

2.8.1 Power-Up Self-Tests

OA Firmware performs the following self-tests at power-up:

- uBoot CRC Firmware Integrity Test (CRC[29]-32)
- uBoot SHA-1 Firmware Integrity Test (SHA-1)
- Cryptographic Library Integrity Test (HMAC-SHA-1)
- Known Answer Tests (KATs)
  - AES ECB encryption KAT
  - AES ECB decryption KAT
  - AES GCM encryption KAT
  - AES GCM decryption KAT
  - Triple-DES ECB encryption KAT
  - Triple-DES ECB decryption KAT
  - RSA encrypt KAT
  - RSA decrypt KAT
  - RSA signature generation KAT
  - RSA signature verification KAT
  - ECDSA signature generation KAT
  - ECDSA signature verification KAT
  - SP 800-56A Primitive "Z" Computation KAT
  - HMAC SHA-1 KAT
  - HMAC SHA-224, HMAC SHA-256, HMAC SHA-384, and HMAC SHA-512 KATs
  - SHA-256 KAT
  - CTR_DRBG KAT

2.8.2 Conditional Self-Tests

OA Firmware performs the following conditional self-tests:

- Continuous Random Generator Test (CRNGT) for CTR_DRBG
- CRNGT for the NDRNG
- RSA Pairwise Consistency Test (PCT)
- ECDSA PCT
- Firmware Load Test

[29] CRC – Cyclic Redundancy Check

2.8.3 Critical Functions Self-Tests

OA Firmware implements the SP 800-90A HMAC_DRBG as its random number generator. The SP 800-90A specification requires that certain critical functions be tested conditionally to ensure the security of the DRBG. Therefore, the following critical function tests are implemented by the cryptographic modules:

- SP 800-90A CTR_DRBG Instantiate Test
- SP 800-90A CTR_DRBG Generate Test
- SP 800-90A CTR_DRBG Reseed Test
- SP 800-90A CTR_DRBG Uninstantiate Test

2.9 Mitigation of Other Attacks

This section is not applicable. The modules do not claim to mitigate any attacks beyond the FIPS 140-2 Level 1 requirements for this validation.

3. Secure Operation

The OA Firmware cryptographic module meets Level 1 requirements for FIPS 140-2. The sections below describe how to place and keep the module in a FIPS-Approved mode of operation.

3.1 Initial Setup

The module must be properly initialized in order to be considered to be in a FIPS-Approved mode of operation. Initialization and other configuration and management operations can be accomplished using:

- a CLI via the serial or Ethernet interface, utilizing getty
- a Web GUI via Ethernet interface, utilizing HTTPS (TLS)

To initialize the modules, the CO must:

1. Initialize the entropy
2. Select the operational mode

3.1.1 Entropy Initialization

The FIPS-Approved modes require specific levels of entropy[30] for the random number generation functions. To ensure that a brand-new appliance has the appropriate levels of entropy available, and before performing the initial configuration of the device, the CO should power on the module and allow it to fully boot up. Then, a reboot must be performed. This can be accomplished using the module's CLI or GUI as follows:

- Via the CLI – The CO must enter "RESTART OA", which will cause a reboot of the module.

- Via the GUI – The CO must navigate to the "Enclosure Information" screen, select "Active Onboard Administrator", select the "Virtual Buttons" tab, and then click the "Reset" button. This will reboot the module

Once the module has completed the boot-up cycle for the second time, the CO must configure the cryptographic module.

3.1.2 Operational Mode Selection

The module supports two FIPS-Approved modes:

- FIPS Mode ON
- FIPS Mode TOP-SECRET

When the OA is operating in "FIPS Mode ON", certificates must have a minimum RSA key length of 2048 bits, and the signature hash algorithm must be SHA-224, SHA-256, SHA-384, or SHA-512. In "FIPS Mode TOP-SECRET", certificates must have a minimum RSA key length of 3072 bits or ECDSA 384 bits, and the signature hash algorithm must be SHA-384.

[30] The module comes preloaded with at least 128 bits of entropy from the factory.

The CO is responsible for ensuring that the module is configured to operate in an Approved mode. To do this, a CO must use the proper credentials to log in to the CLI over SSH or the GUI through the management Ethernet interface.

- Via the CLI – The CO must first check that the OA is not in VC mode, by using the "show vcmode" command. If it returns "Virtual Connect Mode: Enabled", then the CO must use the "clear vcmode" command. The CO must then input the "SET FIPS MODE ON" or "SET FIPS MODE TOP_SECRET" command into the CLI and supply a new OA Administrator password.

- Via the GUI – The CO must navigate to "Enclosure Settings" within the "Enclosure Information" collapsible drop-down menu. Next, the CO must navigate the "Network Access" page, and then select the "FIPS" tab. If there is a VC module connected to the BladeSystem enclosure and a VC domain exists, it may be necessary to clear the VC domain, using the "Clear VC Mode" button. This will take the enclosure out of VC mode and clear all VC settings. Once this is complete, the CO must select the radio button labeled "FIPS MODE ON" or "FIPS MODE Top-Secret" and input a new OA Administrator password.

After this is completed, the OA will reboot and initialize self-tests in order to operate in a FIPS-Approved mode. The module is non-compliant until it is configured as per the instructions above.

3.2 Crypto Officer Guidance

The Crypto Officer is responsible for ensuring that the module is operating in a FIPS-Approved mode of operation. The module is non-compliant unless managed according to the instructions in the following sections.

3.2.1 Secure Management

When configured according to the Crypto Officer guidance in this Security Policy, the module only runs in its Approved modes of operation. The Crypto Officer shall configure the module via the CLI or Web GUI.

The module provides a KVM interface for accessing server consoles as well as the Insight Display LCD which provides manual enclosure controls. The enclosure KVM and Insight Display LCD are locked when the module has been configured to operate in one of the Approved modes as described in section 3.1.2 and shall remain locked for the duration of the module's operation.

3.2.2 Monitoring Status

The CO is responsible for ensuring that the module is running in FIPS-Approved mode of operation. The CO can check the module's FIPS-Approved status in the following ways:

- CLI – The "SHOW FIPS MODE" command will return "FIPS Mode is On" or "FIPS Mode is Top Secret" if the module is currently operating in FIPS mode. Additionally, when in a FIPS-Approved mode, the CLI prompt will have a "[FIPS]" or "[FIPS TSEC]" prefix.

- GUI – The "FIPS Mode ON" or "FIPS Mode TOP-SECRET" radio button will be selected on the "FIPS" tab of the "Network Access" page, discussed above, if the module is operating in FIPS mode. Additionally, after logging in when the module is in a FIPS-Approved mode, the header of the web page will show an icon which contains the text “FIPS” and either a key or a lock icon. Hovering over the text of this icon will display the current FIPS mode of the module: “FIPS Mode ON Enabled” or “FIPS Mode Top-Secret Enabled”.

3.2.3 Zeroization

The CO can force zeroization of the module’s stored CSPs via the management interfaces. Ephemeral keys can be zeroized by power-cycling the module.

Stored keys require the CO to perform a factory reset; to call the GENERATE KEY ALL command from the CLI; or to transition out of either FIPS-Approved mode. Any of these three procedures will overwrite all stored certificates and keys, requiring another set to be generated before the module can resume cryptographic services.

3.3 User Guidance

The User is neither authorized nor able to modify the FIPS-Approved configuration of the module. Users may only utilize the services denoted by “User” as listed in Table 6. Although the User does not have any ability to modify the configuration of the module, they should report to the CO if any irregular activity is observed.

3.4 Additional Usage Policies

This sections notes additional policies below that must be followed by module operators:

- Passwords that are created by module operators shall be at least 8 characters in length and may contain any combination of uppercase and lowercase letters [A-z, a-z]; numbers [0-9]; and special characters (not including space).

3.5 Non-Approved Mode of Operation

When configured according to the Crypto Officer’s guidance found herein, the module does not support a non-Approved mode of operation. The module is considered non-compliant unless configured and managed according to the sections above.

4. Acronyms

Table 9 provides definitions for the acronyms used in this document.

Table 9 – Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
AUX	Auxiliary
CAC	Common Access Card
CBC	Cipher Block Chaining
CCM	Counter with CBC-MAC
CFB	Cipher Feedback
CLI	Command Line Interface
CMAC	Cipher-based Message Authentication Code
CMVP	Cryptographic Module Validation Program
CO	Cryptographic Officer
CONN	Connector
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
CRNGT	Continuous Random Generator Test
CSE	Communications Security Establishment Canada
CKG	Cryptographic Key Generation
CSP	Critical Security Parameter
CTR	Counter
CVL	Component Validation List
DDR	Double Data Rate
DES	Data Encryption Standard
DH	Diffie-Hellman
DRBG	Deterministic Random Bit Generator
DSA	Digital Signature Algorithm
EBC	External Peripheral Bus Controller
ECB	Electronic Code Book
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
EEPROM	Electrically Erasable Programmable Read-Only Memory
EMC	Electromagnetic Compatibility

EMI	Electromagnetic Interference
ETH	Ethernet
FFC	Finite Field Cryptography
FIPS	Federal Information Processing Standard
FPGA	Field-Programmable Gate Array
G	Gigabit
GBE	Gigabit Ethernet
GCM	Galois/Counter Mode
GUI	Graphical User Interface
HMAC	(keyed-) Hash Message Authentication Code
HTTPS	Hypertext Transfer Protocol Secured
I2C	Inter-Integrated Circuit
IP	Internet Protocol
IV	Initialization Vector
KAS	Key Agreement Scheme
KAT	Known Answer Test
KDF	Key Derivation Function
KVM	Keyboard, Video, Mouse
LCD	Liquid Crystal Display
LDAP	Lightweight Directory Authentication Protocol
LED	Light Emitting Diode
MD5	Message Digest v5
MHZ	Megahertz
MII	Media Independent Interface
NDRNG	Non-deterministic Random Number Generator
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
NVRAM	Non-volatile Random Access Memory
OFB	Output Feedback
OS	Operating System
PC	Personal Computer
PCI	Peripheral Component Interconnect
PCT	Pairwise Consistency Test
PHY	Physical Layer
PIN	Personal Identification Number
PPC	PowerPC
RAM	Random Access Memory

RJ45	Registered Jack 45
RNG	Random Number Generator
RSA	Rivest Shamir and Adleman
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOAP	Simple Object Access Protocol
SODIMM	Small Outline Dual Inline Memory Module
SP	Special Publication
SSH	Secure Shell
SSL	Secure Socket Layer
TECB	Triple DES Electronic Codebook
TCBC	Triple DES Cipher Block Chaining
TLS	Transport Layer Security
UART	Universal Asynchronous Receiver Transmitter
USB	Universal Serial Bus
VGA	Video Graphics Array

Prepared by:
Corsec Security, Inc.

13921 Park Center Road, Suite 460
Herndon, VA 20171
United States of America

Phone: +1 703 267 6050
Email: info@corsec.com
http://www.corsec.com