Hewlett Packard Enterprise Development LP

HP BladeSystem Onboard Administrator Firmware

Firmware Version: 4.40

FIPS 140-2 Non-Proprietary Security Policy

FIPS Security Level: 1
Document Version: 1.0

Prepared for:

Hewlett Packard Enterprise Development LP
11445 Compaq Center Dr. W.
Houston, TX 77070
United States of America

Phone: +1 (281) 370-0670
http://www.hpe.com

Prepared by:

Corsec Security, Inc.

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

Phone: +1 (703) 267-6050
http://www.corsec.com

Table of Contents

Table of Figures

List of Tables

© 2016 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

1 Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the HP BladeSystem Onboard Administrator Firmware (Firmware Version: 4.40) from Hewlett Packard Enterprise Development LP This Security Policy describes how the HP BladeSystem Onboard Administrator Firmware meets the security requirements of Federal Information Processing Standards (FIPS) Publication 140-2, which details the U.S. 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. The HP BladeSystem Onboard Administrator Firmware is referred to in this document as the Onboard Administrator, OA[1], cryptographic module, or the module, and the Hewlett Packard Enterprise Development LP is referred to as HP.

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. More information is available on the module from the following sources:

- The HP website (www.hp.com) contains information on the full line of products from HP.
- The CMVP website (http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm) contains contact information for individuals to answer technical or sales-related questions for the module.

1.3 Document Organization

The Security Policy document is one document in a FIPS 140-2 Submission Package. In addition to this document, the Submission Package contains:

- Vendor Evidence document
- Finite State Model document
- Other supporting documentation as additional references

This Security Policy and the other validation submission documentation were produced by Corsec Security, Inc. under contract to HP. With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Submission Package is proprietary to HP and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact HP.

[1] OA – Onboard Administrator

© 2016 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

2 HP BladeSystem Onboard Administrator Firmware

2.1 Overview

The HP BladeSystem is a blade server enclosure designed to maximize power while minimizing costs. The enclosure holds the server blades and supplies them with power, cooling, networking, and data storage, resulting in a reduction in power redistribution units, cabling, switches, and other clutter.

The HP BladeSystem Onboard Administrator Firmware is the enclosure management and the firmware base used to support the HP BladeSystem c-Class Enclosure and all the managed devices contained within the enclosure. The HP BladeSystem Onboard Administrator Firmware is designed to manage all power flow and access permissions for every blade within the enclosure. This involves IP[2] addressing for the server blade's management interface, power management for the server blades, fans, and other modules, utilizing Integrated Lights-Out (iLO).

HP BladeSystem Onboard Administrator Firmware provides a single access point to perform basic management tasks on server blades and switches within the enclosure. HP BladeSystem Onboard Administrator Firmware 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.

HP recommends that the administrator read the specific *HP BladeSystem Onboard Administrator User Guide* for enclosure-specific information before proceeding with Onboard Administrator setup. This user guide provides information on the initial setup and operation of the HP BladeSystem Onboard Administrator. It also covers use of the Onboard Administrator GUI[3] and the use of the enclosure Insight Display. The Onboard Administrator Command Line Interface Guide covers the use of the CLI [4].

The HP BladeSystem Onboard Administrator Firmware provides several features designed to simplify management of c-Class blades and interconnects. The BladeSystem c7000 and c3000 enclosures can be configured with redundant OA modules to provide uninterrupted manageability of the entire enclosure and blades in the event of a failure of the primary OA module or network outage.

The HP BladeSystem Onboard Administrator Firmware is validated at the following FIPS 140-2 Section levels:

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	1
4	Finite State Model	1
5	Physical Security	1
6	Operational Environment	N/A[5]
7	Cryptographic Key Management	1
8	EMI/EMC[6]	1

[2] IP – Internet Protocol
[3] GUI – Graphical User Interface
[4] CLI – Command-Line Interface
[5] N/A – Not applicable
[6] EMI/EMC – Electromagnetic Interference / Electromagnetic Compatibility

© 2016 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Section	Section Title	Level
9	Self-tests	1
10	Design Assurance	1
11	Mitigation of Other Attacks	N/A
14	Cryptographic Module Security Policy	1

2.2 Module Specification

The HP BladeSystem Onboard Administrator Firmware is a firmware module with a multiple-chip standalone embodiment. The overall security level of the module is 1. The cryptographic boundary of the HP BladeSystem Onboard Administrator Firmware is defined by all the firmware that runs on the HP BladeSystem Onboard Administrator blade, operating within the c3000 and c7000 BladeSystem c-Class enclosures. The physical cryptographic boundary of the module is drawn around the hardware blade (red dotted line in Figure 2 below), from this point forward referred to as the 'host appliance', that it runs on. The logical cryptographic boundary is drawn around the module code that runs entirely on the host appliance's Central Processing Unit (CPU), and is depicted in Figure 1 below.

The HP BladeSystem Onboard Administrator Firmware module provides many communication pathways for an administration of the BladeSystem enclosure. The module's cryptographic functions are utilized for securing management traffic being sent and received by the module.

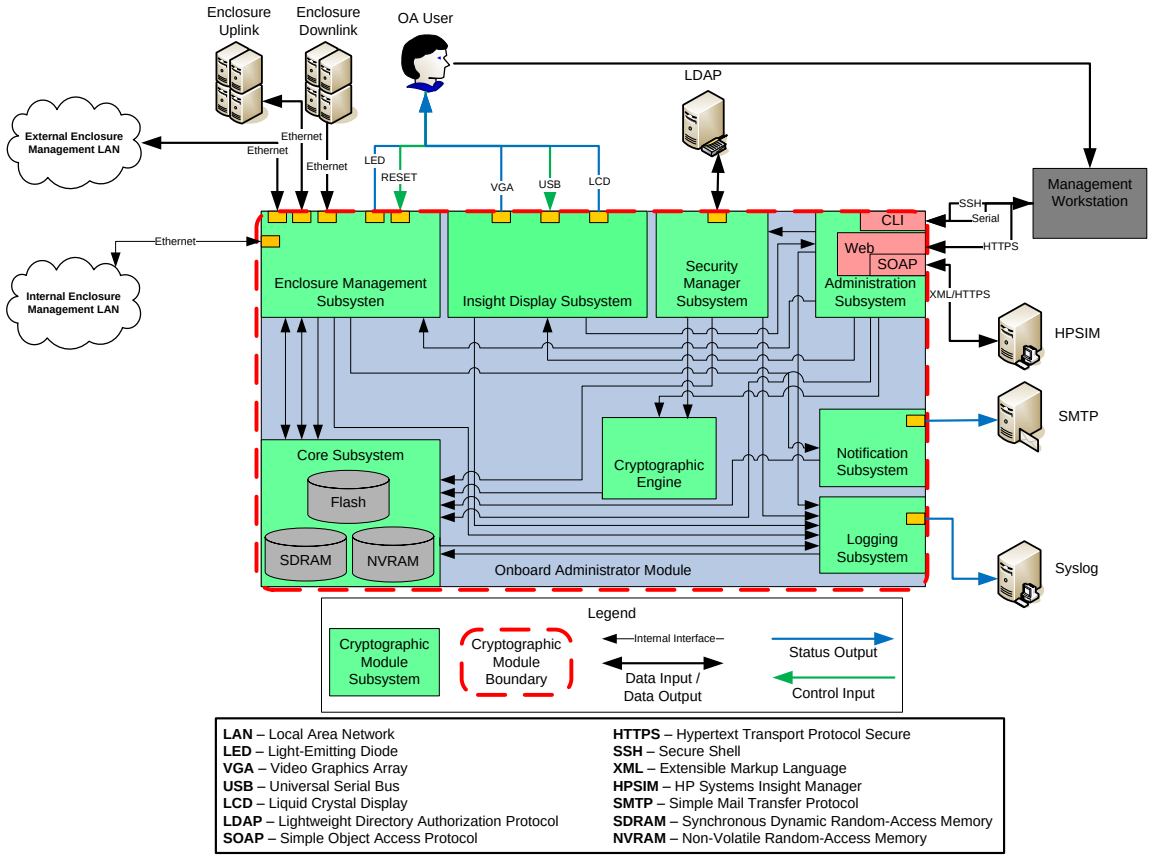

Figure 1 – HP BladeSystem Onboard Administrator Firmware Cryptographic Boundary

© 2016 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Figure 1 shows the systems at work within the Onboard Administrator firmware:

- Security Manager Subsystem – Performs user authentication and account management, and also provides integration into existing LDAP[7] directories.
- Administration Subsystem – Exposes logical interfaces accessible via HTTPS[8], and SOAP[9] that allow management of the OA. This shows an interface with HPSIM[10], over SOAP. HPSIM is a management application that communicates with the OA, iLO, and HP Virtual Connect module in the c-Class enclosure.
- Cryptographic Engine – Performs all cryptographic functionality offered by OA, including encryption of management traffic.
- Enclosure Management Subsystem – Monitors and controls enclosure components and provides status and information on installed devices.
- Insight Display/KVM[11] Subsystem – Enables initial configuration through a small LCD[12] interface on the enclosure, as well as provides KVM access to server blade consoles.
- Logging Subsystem – Facilitates the generation and storage of system event logs to provide administrators with an audit trail of user activity.
- Core Subsystem – Provides a secure, reliable platform on which the other OA subsystems operate, including the operating system, storage, and working memory.
- Notification Subsystem – Processes enclosure alerts and enables notification via SMTP[13] and SNMPv3.

This firmware is designed to run on an HP BladeSystem Onboard Administrator appliance for use in HP BladeSystem c-Class Enclosures. The module will run on the PowerPC (PPC) 440EPX processor. This processor executes the module, which is the OA firmware image, stored in flash memory. There are three forms of Onboard Administrator hardware appliances that support this processor.

The cryptographic module was tested and found compliant on the following platforms:

PowerPC 440EPx:

- c7000 DDR[14]2 Onboard Administrator with KVM
- c3000 Tray with Embedded DDR2 Onboard Administrator
- c3000 Dual DDR2 Onboard Administrator

These will be referred to, collectively, as the "host appliance".

[7] LDAP – Lightweight Directory Authentication Protocol
[8] HTTPS – Hypertext Transfer Protocol Secure
[9] SOAP – Simple Object Access Protocol
[10] HPSIM – HP Systems Insight Manager
[11] KVM – Keyboard, Video, Mouse
[12] LCD – Liquid Crystal Display
[13] SMTP – Simple Mail Transfer Protocol
[14] DDR – Double Data Rate

© 2016 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

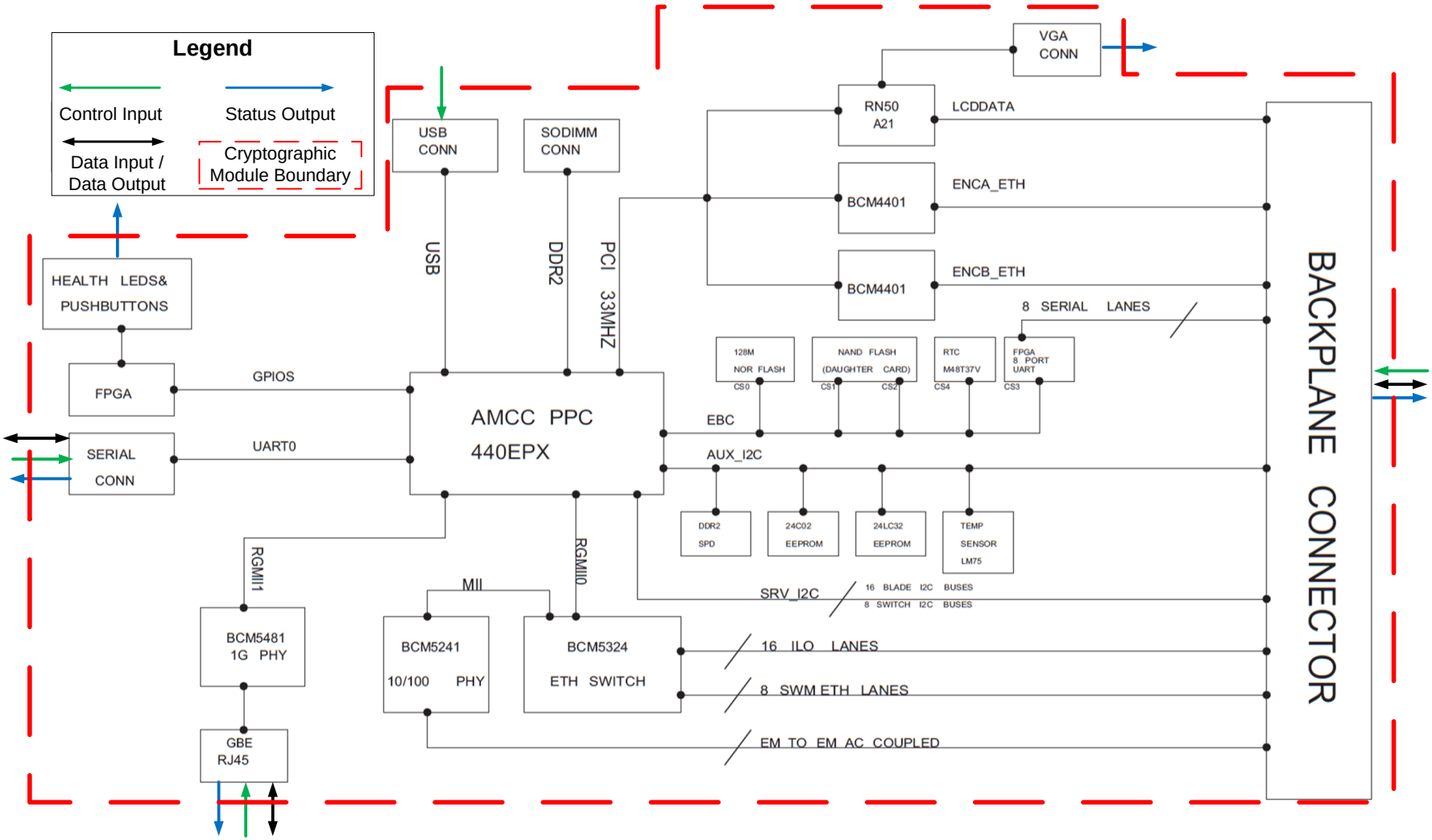

Figure 2 – Hardware Block Diagram for 440EPx Processor

© 2016 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

2.3 Module Interfaces

The OA implements distinct module interfaces in its firmware design. Physically, the module ports and interfaces are considered to be those of the host platform that the firmware runs upon. However, the firmware communicates through a CLI or GUI, which allows it to receive requests and execute function calls for cryptographic and administrative services. The CLI, GUI, and the physical ports/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

These logical interfaces are mapped to the host appliance's physical interfaces, as described in Table 2.

Figure 3 through Figure 5 below show the host appliances and their physical interfaces.

Figure 3 – BladeSystem c7000 Onboard Administrator with KVM

Figure 4 – BladeSystem c3000 Tray with Embedded DDR2 Onboard Administrator

Figure 5 – BladeSystem c3000 Dual DDR2 Onboard Administrator

All of the physical interfaces of the appliance are separated into logical interfaces defined by FIPS 140-2, as described in the following table:

© 2016 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Table 2 – FIPS 140-2 Logical Interface Mappings

FIPS 140-2 Logical Interface	Physical Port/Interface	HP BladeSystem Onboard Administrator Firmware Port/Interface
Data Input	• Ethernet RJ45[15] connector • Serial RS232 DB-9 connector with PC[16] standard pinout • Backplane connector	• TLS[17], SSH[18], and plaintext sessions (HTTPS, SOAP, LDAP, NTP[19])
Data Output	• Ethernet RJ45 connector • Serial RS232 DB-9 connector with PC standard pinout • Backplane connector	• TLS, SSH, and plaintext sessions (HTTPS, SMTP, LDAP, SOAP)
Control Input	• Reset button • Ethernet RJ45 connector • Serial RS232 DB-9 connector with PC standard pinout • USB 2.0 Type A connector • Insight Display LCD Buttons • Backplane connector	• CLI commands • Web GUI interface • Keyboard/Mouse input
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	• Video output from VGA/LCD • CLI output • Web GUI interface • External Syslog • SMTP
Power Interface	Power Interface	Not Applicable

* Only on the c7000 OA

The OA connects to the BladeSystem Enclosure backplane providing connection pathways to all of the enclosure modules and subsystems in order to provide administration.

2.4 Roles and Services

The module supports role-based authentication. 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 *Onboard Administrator User Guide and Command Line Interface User Guide* for more information about the roles and services provided by the Onboard Administrator.

[15] RJ45 – Registered Jack 45
[16] PC – Personal Computer
[17] TLS – Transport Layer Security
[18] SSH – Secure Shell
[19] NTP – Network Time Protocol

© 2016 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

2.4.1 Crypto-Officer Role

The Crypto-Officer role has the ability to create User accounts, define permissions, change passwords, and take the module into or out of a FIPS mode of operation. The Crypto-Officer maps to the "Administrator" and "OA Administrator" account classifications, as defined in the *Onboard Administrator Command Line Interface User Guide*. Descriptions of the services available to the Crypto-Officer role are provided in Table 3, below. The Crypto-Officer has access to all of the services of the User. Please note that the keys and CSPs[20] listed in the table 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 3 – Crypto-Officer Services

Service	Description	Input	Output	CSP and Type of Access
Create/modify Users	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	Change the Crypto-Officer password or permissions	Command to change password/permissions	Change CO password/permissions	Password – W
Access the GUI	Access the GUI via HTTPS connection through web browser	Command to begin HTTPS connection via web browser	Connection established and administration page appears	Session key – X Authentication key – X RSA[21] public/private keypair – X DH[22] public/private components – X
Access the CLI	Manage the module using the CLI accessed via SSH protocol over Ethernet, or directly via Serial interface	Command to begin SSH session	Session established	Crypto-Officer credentials – X Session key – X Authentication key – X RSA public/private keypair – X DH public/private components – X

[20] CSP – Critical Security Parameter
[21] RSA – Rivest, Shamir, and Adleman
[22] DH – Diffie-Hellman

© 2016 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Service	Description	Input	Output	CSP and Type of Access
Access the SNMPv3	Manage the module remotely and provide non-security relevant information about the module's state and statistics	None	Status output	SNMPv3 Privacy Key – R/W/X SNMPv3 Authentication Key – R/W/X
Set Factory Defaults	Unable to be called directly in FIPS mode. Triggered by entering or leaving FIPS mode. Zeroizes all keys, certificates, and users. Resets Administrator password to factory setting	Command to set factory default	Set Factory Defaults	All keys – W
Zeroize Keys	Entering the GENERATE KEY ALL command in the module's CLI forces the module to overwrite existing keys and regenerate all cryptographic keys	Execute the GENERATE KEY ALL command in the module's CLI	All keys are zeroized and regenerated	All keys – W
Set FIPS Mode	Enable/disable FIPS mode of operation. Calls the Set Factory Defaults service	CLI command: SET FIPS MODE ON/OFF GUI Interface: check or uncheck "FIPS Mode ON" checkbox 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 mode	None
Check FIPS Mode Status	Display FIPS status of module	CLI command: SHOW FIPS MODE GUI Interface: If "FIPS Mode ON" checkbox is checked, module is in FIPS mode	CLI: FIPS Mode is On GUI: Checkbox is checked	None
Perform Self-Tests on demand	Run self-tests on demand	None	Status	All keys – W

© 2016 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Service	Description	Input	Output	CSP and Type of Access
Certificate Generation	Generate an X.509 Certificate signing request	Command to generate certificate	Generated certificate	RSA public/private key – X

2.4.2 User Role

The User role has the ability to 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 in the *Onboard Administrator Command Line Interface User* Guide. Descriptions of the services available to the User role are provided in the Table 4 below.

Table 4 – User Services

Service	Description	Input	Output	CSP and Type of Access
Update Firmware	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	None
Change User Credentials	Change the User password	Command to change password	Change User password	Password – W
Access the GUI	Access the GUI via HTTPS connection through web browser	Command to begin HTTPS connection via web browser	Connection established and administration page appears	Session key – X Authentication key – X RSA public/private keypair – X DH public/private components – X
Access the CLI	Manage the module using the CLI accessed via SSH protocol over Ethernet, or directly via Serial interface	Command to begin session	Session established	Session key – X Authentication key – X RSA public/private keypair – X DH public/private components – X
Access the SNMPv3	Manage the module remotely and provide non-security relevant information about the module's state and statistics	None	Status output	SNMPv3 Privacy Key – R/W/X SNMPv3 Authentication Key – R/W/X

© 2016 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Service	Description	Input	Output	CSP and Type of Access
Key Wrapping	Perform key wrapping operation	Data to encrypt and encryption key	Encrypted data	RSA public key – X
Key Unwrapping	Perform key unwrapping operation	Data to decrypt and decryption key	Decrypted plaintext data	RSA private key – X
Signature Generation	Generate a signature	Data to sign	Digitally signed data	RSA public/private key – WX
Signature Verification	Verify the digital signature attached to data	Data to verify	Hash value of data to be verified	RSA public/private key – WX
Generate Symmetric Keys	Calls the DRBG[23] to generate symmetric keys	DRBG parameters	Key of requested size	Entropy Input String – RX DRBG Seed – WRX TLS Session key – X SSH Session Encryption key – X
Generate Asymmetric Keys	Call the DRBG for primes/keying material	DRBG parameters	Key or prime of requested size	RSA keypair –W

For more information on the non-security relevant services of the module, please refer to the HP BladeSystem Onboard Administrator User Guide (*http://h20628.www2.hp.com/km-ext/kmcsdirect/emr_na-c00705292-43.pdf*).

2.5 Physical Security

The HP BladeSystem Onboard Administrator Firmware is a multiple-chip standalone cryptographic module. The module consists of production-grade components that include standard passivation techniques.

2.6 Operational Environment

As a firmware module, the operational environment requirements of FIPS 140-2 do not apply to the HP BladeSystem Onboard Administrator Firmware. The OS[24] included in the firmware does not allow the loading of new applicationgs; therefore, the operational environment of the module is a non-modifiable operational environment.

2.7 Cryptographic Key Management

The module implements the FIPS-Approved algorithms listed in Table 5 below.

[23] DRBG – Deterministic Random Bit Generator

[24] OS – Operating System

© 2016 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Table 5 – FIPS-Approved Algorithm Implementations

Algorithm	Certificate Number
Symmetric Key Algorithm	
AES encryption/decryption in CBC[25], CTR[26], ECB modes (128, 192, 256-bit key)	3333
AES GCM[27] encryption/decryption/generation/verification (128, 192, 256-bit)	3333
Triple-DES[28] encryption/decryption in CBC, ECB modes (Keying options 1 and 2)	1903
Asymmetric Key Algorithm	
RSA (FIPS 186-4) key generation (2048-bit), signature generation (2048-bit), signature verification (2048-bits)	1712
Secure Hashing Algorithm (SHA)	
SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	2767
SHA-1 (Integrity Test)	2766
SHA-256	2768
Message Authentication Code (MAC) Function	
HMAC[29] using SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512	2124
Deterministic Random Bit Generation (DRBG)	
SP[30] 800-90A based CTR_DRBG (AES), no derivation function	780
Component Validation List (CVL)*	
Section 4.2, TLS – Key Derivation Function (KDF)	487
Section 5.2, SSH – KDF	487
Section 5.4, SNMP[31]v3 – KDF	487

***** The TLS, SSH and SNMP v3 protocols have not been reviewed or tested by the CAVP or the CMVP. Only the Key Derivation Functions, that are being implemented and used by these protocols have been tested by the CAVP.

NOTE: The following security functions have been deemed "deprecated" or "restricted" by NIST. Please refer to NIST Special Publication 800-131A for further details.

- The use of two-key Triple DES for encryption is **restricted** after December 31, 2010.
- After December 31, 2013, key lengths providing less than 112 bits of security strength shall not be used in the Approved mode of operation to generate keys or digital signatures.
- For additional information on the risks associated with the use of a particular algorithm or given key length please consult the transition tables available at the CMVP Web site (http://csrc.nist.gov/groups/STM/cmvp/).

Additionally, the module utilizes the following non-Approved algorithm implementations that are allowed to be used in Approved mode of operation:

[25] CBC – Cipher-Block Chaining
[26] CTR – Counter
[27] GCM – Galois/Counter Mode
[28] DES – Data Encryption Standard
[29] HMAC – (Keyed) Hash Message Authentication Code
[30] SP – Special Publication
[31] SNMP – Simple Network Management Protocol

© 2016 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

- Diffie-Hellman (key agreement; key establishment methodology provides 112 bits of encryption strength)
- MD5[32] (for TLS use)
- RSA key wrapping (key wrapping; key establishment methodology provides 112 bits of encryption strength)
- /dev/urandom – a non-Approved NDRNG[33] used for entropy gathering

[32] MD5 – Message Digest Algorithm
[33] NDRNG – Non-Deterministic Random Number Generator

© 2016 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

The module supports the critical security parameters (CSPs) listed below in Table 6.

Table 6 – List of Cryptographic Keys, Cryptographic Key Components, and CSPs

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
SSH/TLS Session Authentication Key	HMAC SHA-1	Internally generated	Never output from module	Plaintext in volatile memory	End session, power cycle, host reboot, factory reset, leaving FIPS mode, or GENERATE KEY command	Authenticate SSH or TLS session
SSH Session Encryption Key	AES 128-, 192-, 256-bit key Triple-DES 168-bit key	Internally generated	Never output from module	Plaintext in volatile memory	End session, power cycle, host reboot, factory reset, leaving FIPS mode, or GENERATE KEY command	Encryption/Decryption for SSH sessions
TLS Session Key	AES 128-, 192-, 256-bit key Triple-DES 168-bit key	Internally generated	Never output from module	Plaintext in volatile memory	End session, power cycle, host reboot, factory reset, leaving FIPS mode, or GENERATE KEY command	Encryption/ Decryption forTLS sessions
RSA Private Key	RSA 2048-bit Key	Internally generated – Generated by call during first boot	Never output from module	Stored in Flash memory	Factory reset, leaving FIPS mode, or GENERATE KEY command	Signature generation, decryption, key exchange, certificate generation (TLS sessions), TLS and SSH authentication

© 2016 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
RSA Public Key	RSA 2048-bit Key	Internally generated – Generated by call during first boot	Output from module in plaintext	Stored in Flash memory	Factory reset, leaving FIPS mode, or GENERATE KEY command	Signature verification, encryption, key exchange with 2048-bit only, certificate generation (TLS sessions), TLS and SSH authentication
Entropy Input String	256-bit random value	Gathered from system entropy (/dev/urandom)	Never output from module	Stored in NVRAM	Removing NVRAM battery, host reboot	Generate seed and finally random number using the DRBG
DRBG Seed	384-bit random value	Internally generated using entropy input string	Never output from module	Stored in NVRAM	Removing NVRAM battery, host reboot	Generate random number using the DRBG
DH Public Components	Public components of DH protocol (2048-bit key)	Internally generated	Output from module via Data Output interface in plaintext	Plaintext in volatile memory	End session, power cycle, host reboot, factory reset, leaving FIPS mode, or GENERATE KEY command	Key exchange (TLS, SSH sessions)
DH Private Components	Private components of DH protocol (256-bit key)	Internally generated	Never output from module	Plaintext in volatile memory	End session, power cycle, host reboot, factory reset, leaving FIPS mode, or GENERATE KEY command	Key exchange (TLS, SSH sessions)
SNMPv3 Privacy Key	AES 128-, 192-, 256-bit or Triple-DES 168-bit	Internally generated	Never output from module	Plaintext in volatile memory	End session, power cycle, host reboot, factory reset, leaving FIPS mode, or GENERATE KEY command	Encrypting SNMPv3 packets.

© 2016 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
SNMPv3 Authentication Key	HMAC-SHA-1-96	Internally generated	Never output from module	Plaintext in volatile memory	End session, power cycle, host reboot, factory reset, leaving FIPS mode, or GENERATE KEY command	Authenticating SNMPv3 packets.
Operator password	Minimum of eight characters of alphanumeric string	Initial CO password hardcoded, password changes entered into module over TLS or SSH	Initially login password provided to the CO, changed password never exits the module	Hashed on Flash memory and in RAM	Zeroized when the password is updated with a new one	Authenticating the Operator

© 2016 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

2.8 Self-Tests

2.8.1 Power-Up Self-Tests

The HP BladeSystem Onboard Administrator Firmware performs the following self-tests at power-up:

- uBoot CRC Firmware Integrity Test (CRC[34]-32)
- uBoot SHA-1 Firmware Integrity Test (SHA-1)
- Cryptographic Library Integrity Tests (HMAC SHA-1 and SHA-256)
- Known Answer Tests (KATs)
    - AES ECB mode encryption KAT
    - AES ECB mode decryption KAT
    - AES GCM mode encryption KAT
    - AES GCM mode decryption KAT
    - Triple-DES ECB mode encryption KAT
    - Triple-DES ECB mode decryption KAT
    - RSA signature generation KAT
    - RSA signature verification KAT
    - HMAC SHA-1 KAT
    - HMAC SHA-224, HMAC SHA-256, HMAC SHA-384, and HMAC SHA-512 KATs
    - SHA-256 KAT
    - SP 800-90A based CTR_DRBG KAT

2.8.2 Conditional Self-Tests

The HP BladeSystem Onboard Administrator Firmware performs the following conditional self-tests:

- Continuous Random Generator Test (CRNGT) for SP 800-90A based CTR_DRBG
- CRNGT for the NDRNG
- RSA Pairwise Consistency Test

2.8.3 Critical Function Tests

The HP BladeSystem Onboard Administrator 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 Critical Function Test
- SP 800-90A CTR _DRBG Generate Critical Function Test
- SP 800-90A CTR _DRBG Reseed Critical Function Test
- SP 800-90A CTR _DRBG Uninstantiate Critical Function Test

2.9 Mitigation of Other Attacks

The module is not designed to mitigate one or more specific attacks beyond the FIPS 140-2 Level 1 requirements for this validation.

[34] CRC – Cyclic Redundancy Check

© 2016 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

3 Secure Operation

The HP BladeSystem Onboard Administrator Firmware meets Level 1 requirements for FIPS 140-2. The sections below describe how to place and keep the module in FIPS-approved mode of operation.

3.1 Initial Setup

The module must be properly initialized in order to be considered to be in FIPS-Approved mode of operation. Once configured for FIPS mode, the module only operates in FIPS-Approved mode of operation. The FIPS mode requires specific levels of entropy[35] in the random number generation functions. In order to ensure that the brand new appliance has the appropriate levels of entropy available, and before performing the initial configuration of the device, the Crypto-Officer should power on the module and allow it to fully boot up. Then on the command line interface, the Crypto-Officer should enter "RESTART OA" which will cause a reboot of the device. The reboot can also be performed using the GUI by navigating to the "Enclosure Information", then to the "Active Onboard Administrator", then selecting the "Virtual Buttons" tab, and clicking the "Reset" button. Once the module has completed the boot up cycle for the second time the Crypto-Officer must configure the HP BladeSystem c-Class Enclosure.

The Crypto-Officer is responsible for making sure that the module is configured to operate in FIPS mode. In order to do this, a Crypto-Officer must log into either the CLI over SSH or the GUI through an Ethernet interface, with the proper credentials for Crypto-Officer administration.

In the GUI, the Crypto-Officer must navigate to "Enclosure Settings" within the "Enclosure Information" collapsible drop-down menu. Within that, the CO must select the "Network Access" page, and then select the "FIPS" tab. If there is a Virtual Connect (VC) module connected to the BladeSystem enclosure and VC domain exists, it may be necessary to clear VC domian, 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 Crypto-Officer must check the radio button labeled "FIPS MODE ON" and input a new OA Administrator password. This new password must contain at least eight characters. There must be at least one character of each of four character types: uppercase, lowercase, numeric, and non-alphanumeric.

If setting FIPS mode via the CLI, the Crypto-Officer must first check that the OA is not in Virtual Connect mode, by using the "show vcmode" command. If it returns "Virtual Connect Mode: Enabled", then the Crypto-Officer must use the "clear vcmode" command. The Crypto-Officer must then input the "SET FIPS MODE ON" command into the CLI, and supply a new OA Administrator password, following the same conventions outlined above.

After this is completed, the OA will reboot and initialize self-tests in order to operate in FIPS mode.

If a redundant OA is to be used, then it must be properly connected to the enclosure. The Crypto-Officer must first power-on the OA module. If this is the first power-on of the module, or if it has undergone a factory reset, it will begin to generate keys and certificates. The active OA module will pass a hash of the password in an unencrypted form to the redundant OA.

3.2 Secure Management

This section provides guidance which ensures that the module is always operated in the FIPS mode of operation. It will generally include services and activities allotted to the Crypto-Officer. An example is provided below.

The Crypto-Officer is responsible for making sure the module is running in FIPS-Approved mode of operation.

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

© 2016 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

The Crypto-Officer can check the module's FIPS mode status in several ways:

- CLI - The "show fips mode" command will return "FIPS Mode is On" if the module is currently operating in FIPS mode. Additionally, when in FIPS mode, the CLI prompt will have a "[FIPS]" prefix.

- GUI - The FIPS Mode ON 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 FIPS mode, the header of the web page will show an icon which contains the text "FIPS". Mouse-over text of this icon will display the current FIPS mode of the module: "FIPS Mode ON Enabled".

3.2.1 Management

The module may be managed through a CLI via the Serial or Ethernet interface, utilizing getty, or a Web GUI via Ethernet interface, utilizing HTTPS (TLS). Through these interfaces, a Crypto-Officer can configure and enable the FIPS mode. The Crypto-Officer can also gain access to OA controls over the BladeSystem enclosure via a KVM interface, which connects via the optional KVM Module in the enclosure. Access through these interfaces is controlled by role-based authentication.

The KVM and Insight Display LCD are locked, by default, in FIPS mode. However, the Crypto-Officer can unlock these interfaces through the Web GUI. Unlocking these interfaces requires the configuration of a PIN code that must be used to access these management interfaces. This PIN code, set by the Crypto-Officer, must be 1 to 6 characters long. The characters supported are upper and lower-case letters, and numbers.

Note that only TLS is supported by the module, when operating in FIPS mode. Other versions of SSL (v3.0 and under) are unsupported.

The OA can communicate with HP iLO modules. The iLO modules, to be used with the OA, must be configured to use AES encryption for communication traffic.

3.2.2 Zeroization

The Crypto-Officer is able to force zeroization of the module CSPs, both stored and ephemeral, via the management interface. Ephemeral keys can be zeroized by power-cycling the module. Stored keys require the Crypto-Officer to perform a factory reset, to call the GENERATE KEY ALL command from the CLI, or to transition out of FIPS mode. This 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 listed in Table 4. Although the User does not have any ability to modify the configuration of the module, they should report to the Crypto-Officer if any irregular activity is observed.

© 2016 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

4 Acronyms

Table 7 in this section defines the acronyms.

Table 7 – Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
CBC	Cipher Block Chaining
CLI	Command-Line Interface
CMVP	Cryptographic Module Validation Program
CO	Crypto-Officer
CPU	Central Processing Unit
CSE	Communications Security Establishment
CSP	Critical Security Parameter
CRNGT	Continuous Random Number Generator Test
CRC	Cyclic Redundancy Check
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
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FIPS	Federal Information Processing Standard
GCM	Galois/Counter Mode
GUI	Graphical User Interface
HMAC	(Keyed-) Hash Message Authentication Code
HP	Hewlett-Packard
HPSIM	HP Systems Insight Manager
HTTPS	Hypertext Transfer Protocol Secure
iLO	Integrated Lights-Out
IP	Internet Protocol
KAS	Key Agreement Scheme
KAT	Known Answer Test

© 2016 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Acronym	Definition
KDF	Key Derivation Function
KVM	Keyboard-Video-Mouse
LAN	Local Area Network
LCD	Liquid-Crystal Display
LDAP	Lightweight Directory Access Protocol
LED	Light-Emitting Diode
MAC	Message Authentication Code
MD5	Message Digest 5
N/A	Not Applicable
NDRNG	Non-Deterministic Random Number Generator
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
NVRAM	Non-Volatile Random Access Memory
OA	Onboard Administrator
OFB	Output Feedback
OS	Operating System
PC	Personal Computer
PKCS	Public-Key Cryptography Standards
PPC	PowerPC
RJ45	Registered Jack 45
RSA	Rivest Shamir and Adleman
SDRAM	Synchronous Dynamic RandomAccess Memory
SHA	Secure Hash Algorithm
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOAP	Simple Object Access Protocol
SP	Special Publication
SSH	Secure Shell
SSL	Secure Socket Layer
TCP	Transmission Control Protocol
TDES	Triple-Data Encryption Standard
TLS	Transport Layer Security
Triple-DES	Triple- Data Encryption Standard
USB	Universal Serial Bus
VC	Virtual Connect

© 2016 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Acronym	Definition
VGA	Video Graphics Array
XML	Extensible Markup Language

© 2016 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

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