Hewlett-Packard Development Company, L.P.

HP BladeSystem Onboard Administrator Firmware

Firmware Version: 3.71

FIPS 140-2 Non-Proprietary Security Policy

FIPS Security Level: 1
Document Version: 1.2

Prepared for:

Hewlett-Packard Development Company, L.P.
11445 Compaq Center Dr W
Houston, TX 77070
United States of America

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

Prepared by:

Corsec Security, Inc.
13135 Lee Jackson Memorial Hwy, Suite 220
Fairfax, VA 22033
United States of America

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

Table of Contents

Table of Figures

List of Tables

1 Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the Hewlett-Packard Development Company, L.P. (HP) HP BladeSystem Onboard Administrator Firmware 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 Canada (CSEC) 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], crypto-module, or 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. 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

2 HP BladeSystem Onboard Administrator Firmware

2.1 Overview

The HP BladeSystem is designed to maximize power while minimizing costs, saving up to 56% of the total cost of ownership compared to traditional infrastructures. Since all server blades share power, network, and storage infrastructure, there can be a drastic reduction in power redistribution units, cabling, switches, and other clutter, leading to an efficient, comprehensive server infrastructure in one enclosure.

The HP BladeSystem Onboard Administrator Firmware fulfills a critical function in the infrastructure of the BladeSystem. It is designed to administrate all power flow and access permissions for every unit within the enclosure. This involves IP addressing for the server blade's management interface, power management for the server blades, fans, and other modules, utilizing Integrated Lights-Out (iLO).

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.

Onboard Administrator provides a single point from which to perform basic management tasks on server blades and switches within the enclosure. Onboard Administrator 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[2] and the use of the enclosure Insight Display. The Onboard Administrator Command Line Interface Guide covers the use of the CLI [3].

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.

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

[2] GUI – Graphical User Interface

[3] CLI – Command-Line Interface

.

Section	Section Title	Level
7	Cryptographic Key Management	1
8	EMI/EMC[4]	1
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

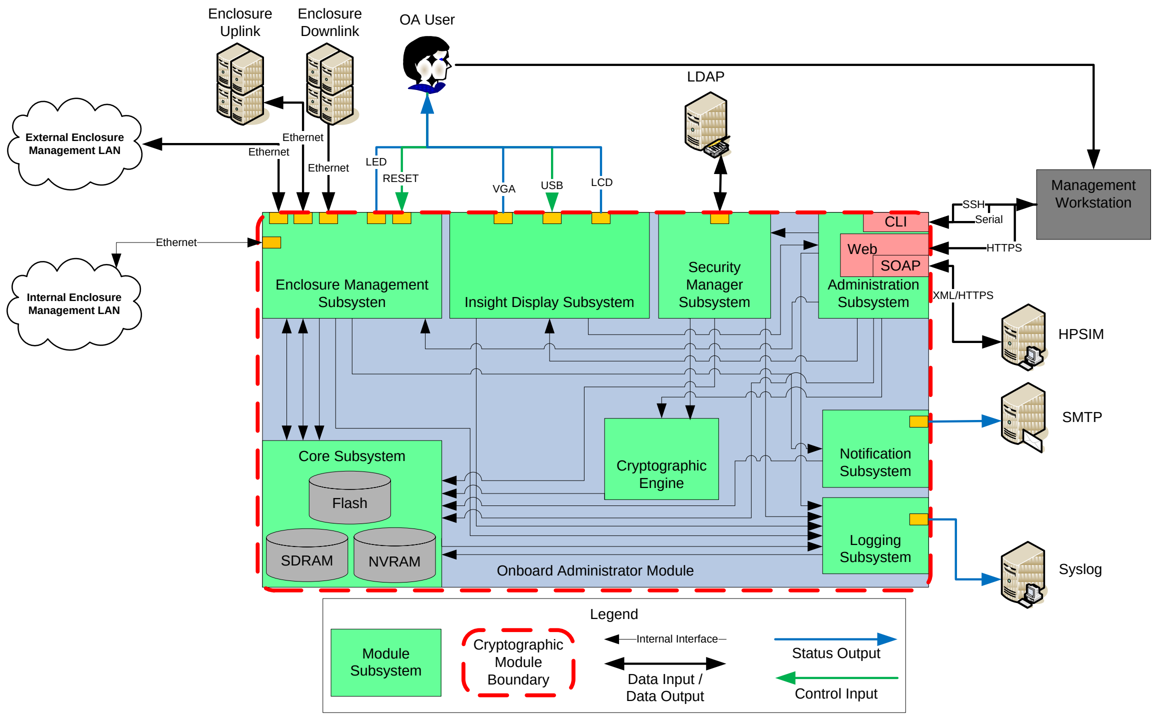
The HP BladeSystem Onboard Administrator Firmware is a firmware module with a multi-chip standalone embodiment. The overall security level of the module is 1. The cryptographic boundary of the HP BladeSystem Onboard Administrator Firmware is defined by all the firmware that runs on the BladeSystem Onboard Administrator blade, operating within the c3000 and c7000 BladeSystem c-Class enclosures. The physical cryptographic boundary of the module is the hardware blade, 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 CPU[5].

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

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

[5] CPU – Central Processing Unit

.



LAN – Local Area Network	**HTTPS** – Hypertext Transport Protocol Secure
LED – Light-Emitting Diode	**SSH** – Secure Shell
VGA – Video Graphics Array	**XML** – Extensible Markup Language
USB – Universal Serial Bus	**HPSIM** – HP Systems Insight Manager
LCD – Liquid Crystal Display	**SMTP** – Simple Mail Transfer Protocol
LDAP – Lightweight Directory Authorization Protocol	**SDRAM** – Synchronous Dynamic Random-Access Memory
SOAP – Simple Object Access Protocol	**NVRAM** – Non-Volatile Random-Access Memory

Figure 1 – HP BladeSystem Onboard Administrator Firmware Cryptographic Boundary

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

- OA Security Manager Subsystem – Performs user authentication and account management, and also provides integration into existing LDAP[6] directories.

- OA Administration Subsystem **–** Exposes logical interfaces accessible via HTTPS, and SOAP that allow management of the OA. This shows an interface with HPSIM, over SOAP. HPSIM is a management application that communicates with the OA, iLO, and HP Virtual Connect module in the c-Class enclosure.

- OA Cryptographic Engine **–** Performs all cryptographic functionality offered by OA, including encryption of management traffic.

- OA Enclosure Management Subsystem – Monitors and controls enclosure components and provides status and information on installed devices.

- OA Insight Display/KVM[7] Subsystem – Enables initial configuration through a small LCD interface on the enclosure, as well as provides KVM access to server blade consoles.

- OA Logging Subsystem – Facilitates the generation and storage of system event logs to provide administrators with an audit trail of user activity.

[6] LDAP – Lightweight Directory Authentication Protocol
[7] KVM – Keyboard, Video, Mouse

.

- OA Core Subsystem – Provides a secure, reliable platform on which the other OA subsystems operate, including the operating system, storage, and working memory.

- OA Notification Subsystem – Processes enclosure alerts and enables notification via SMTP[8]

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[9]2 Onboard Administrator with KVM option
- c3000 Tray with Embedded DDR2 Onboard Administrator
- c3000 Dual DDR2 Onboard Administrator

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

[8] SMTP – Simple Mail Transfer Protocol

[9] DDR – Double Data Rate

.

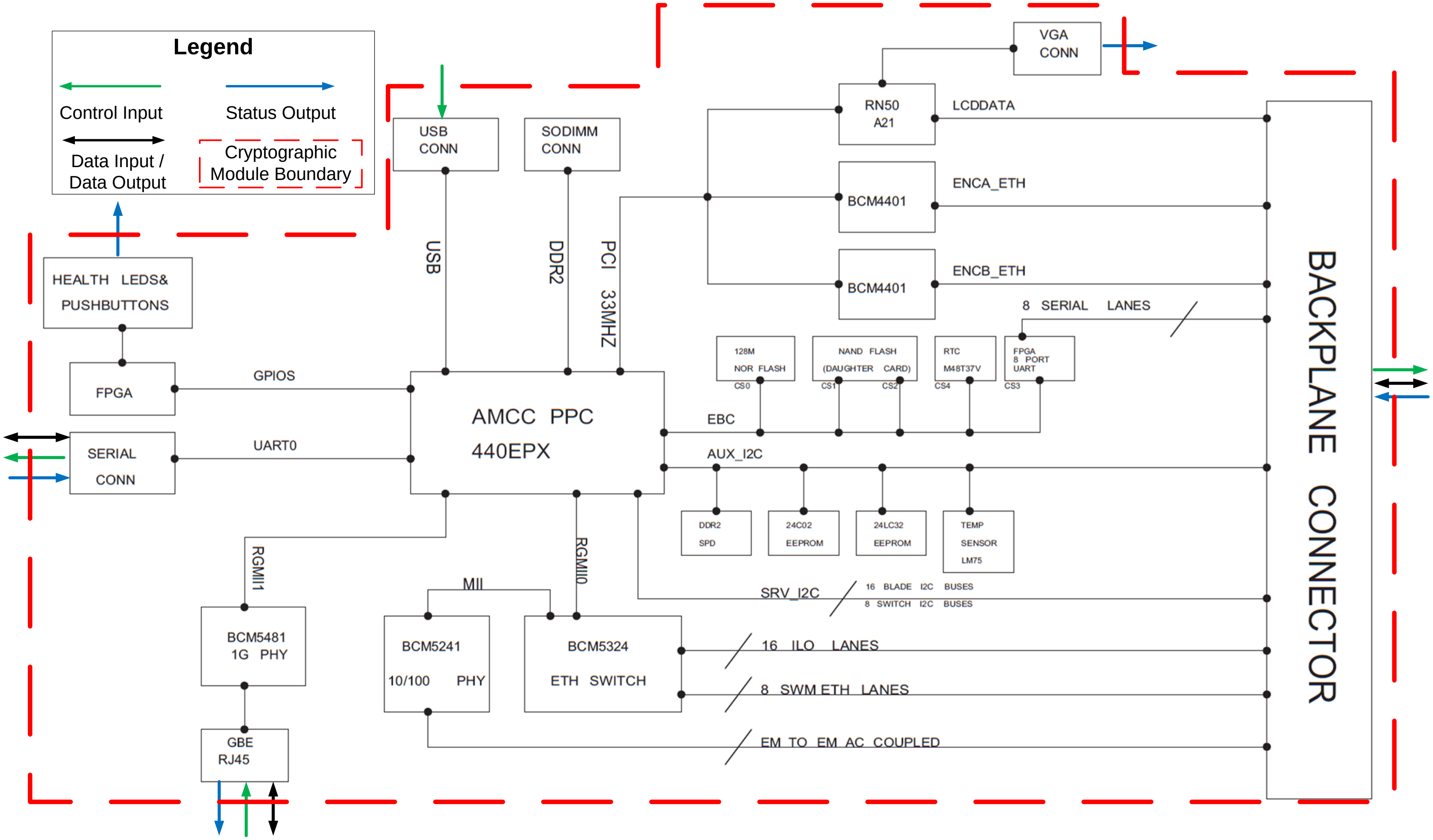


Figure 2 – Hardware Block Diagram for 440EPx Processor

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 (as defined by FIPS 140-2) map to the host appliance's physical interfaces, as described in Table 2.

Figure 3 through Figure 5 show the host appliance's physical interfaces.

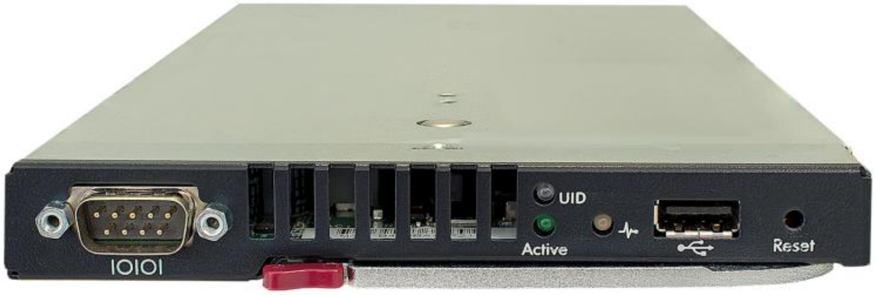


Figure 3 – BladeSystem c7000 Onboard Administrator with KVM

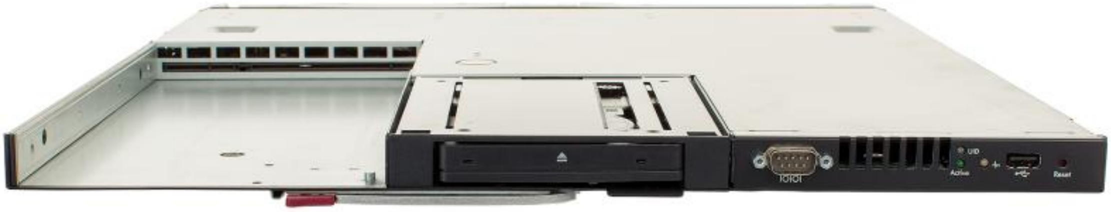


Figure 4 – BladeSystem c3000 Tray with Embedded DDR2 Onboard Administrator

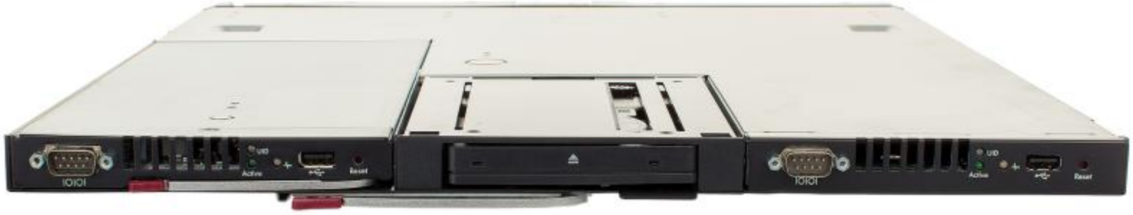


Figure 5 – BladeSystem c3000 Dual DDR2 Onboard Administrator

.

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

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 connector • Serial RS232 DB-9 connector with PC standard pinout • Backplane connector	• TLS[10], and plaintext sessions (HTTPS, SOAP, LDAP, NTP[11])
Data Output	• Ethernet RJ45 connector • Serial RS232 DB-9 connector with PC standard pinout • Backplane connector	• TLS, and plaintext sessions (HTTPS, SMTP, LDAP, SOAP)
Control Input	• Reset button • Ethernet RJ45 connector • Serial RS232 DB-9 connector with PC[12] 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 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.

[10] TLS – Transport Layer Security
[11] NTP – Network Time Protocol
[12] PC – Personal Computer

.

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”, “OA Administrator”, and “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[13] 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	CSP and Type of Access
Create/modify Users	Create, edit, and delete users; define user accounts and assign permissions	
Change CO[14] credentials	Change the Crypto-Officer password or permissions	
Access the GUI	Access the GUI via HTTPS connection through web browser	Session key – X RSA public/private keypair – X
Access the CLI	Manage the module using the CLI via Serial interfaces	
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 default Administrator password to factory setting.	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	All keys – W
Set FIPS Mode	Enable/disable FIPS mode of operation. Calls the Set Factory Defaults service.	
Check FIPS Mode Status	Display FIPS status of module	N/A

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

[13] CSP – Critical Security Parameter

[14] CO – Crypto-Officer

.

in the *Onboard Administrator Command Line Interface User* Guide. Descriptions of the services available to the User role are provided in the table below.

Table 4 – User Services

Service	Description	CSP and Type of Access
Update firmware	Update the module firmware	
Change User credentials	Change the User password	
Access the GUI	Access the GUI via HTTPS connection through web browser.	Session key –X RSA public/private keypair – X
Access the CLI	Manage the module using the CLI via Serial interfaces	
Symmetric Encryption	Perform symmetric encryption operation on data	Session key – X
Symmetric Decryption	Perform symmetric decryption operation on data	Session key – X
Key Wrapping	Perform key wrapping operation	RSA[15] public key – X
Key Unwrapping	Perform key unwrapping operation	RSA private key – X
Signature Generation	Generate a signature	RSA private key – X
Signature Verification	Verify the digital signature attached to data	RSA public key – X
Certificate Generation	Generate an X.509 Certificate signing request	RSA public/private keypair – X
Generate Symmetric Keys	Call the RNG[16] to generate symmetric keys	ANSI[17] X9.31 Seed – X ANSI X9.31 Seed Key – X AES[18] Key – W TDES Key – W
Generate Asymmetric Keys	Call RNG for primes/keying material	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-c00705292-39.pdf*).

2.4.3 Non-Approved Services

The module may also offer non-Approved services as listed in Table 5 below. To provide these services, the module utilizes the following functions and protocol whose use, in Approved mode of operation, is restricted by the Crypto Officer as documented in Section 3 of this Security Policy document:

[15] RSA – Rivest, Shamir, Adleman
[16] RNG – Random Number Generator
[17] ANSI – American National Standards Institute
[18] AES – Advanced Encryption Standard

.

- MD5 (for non-TLS)
- RSA (1024-bit) (signature generation and key wrapping)
- SHA – 160 (for signature generation)
- Diffie-Hellman (1024-bit)
- DSA (1024-bit)
- SSH (Secure Shell)
- RC4

Table 5 – Non-Approved Services

Service	Description	Non-Approved Cryptographic Function
Symmetric encryption/decryption	Perform RC4 symmetric encryption/decryption operations.	RC4
Key Wrapping	Perform key wrapping operation with RSA with public key sizes smaller than 2048-bits.	RSA
Key Unwrapping	Perform key unwrapping operation with RSA with public key sizes smaller than 2048-bits.	RSA
Certificate Generation	Perform certificate generation functions with RSA public key sizes smaller than 2048-bits or that use SHA-1 for hashing.	RSA, SHA
Signature Generation	Perform digital signature generation functions with RSA or DSA public key sizes smaller than 2048-bits or that use SHA-1 for hashing.	RSA, DSA, SHA
Generate Asymmetric Keys	Perform RSA or DSA key generation functions with public key sizes smaller than 2048-bits.	RSA, DSA
Key Establishment	Perform key establishement functions with public key sizes smaller than 2048-bits.	Diffie-Hellman
Hashing	For non-TLS uses	MD5
CLI Services	Access using SSH	DSA, Diffie-Hellman

2.5 Physical Security

The HP BladeSystem Onboard Administrator Firmware is a multi-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.

2.7 Cryptographic Key Management

The module implements the FIPS-Approved algorithms listed in Table 6 below.

.

Table 6 – FIPS-Approved Algorithm Implementations

Algorithm	Certificate Number
Symmetric Key Algorithm	
AES – CBC[19], CTR[20] mode for 128-, 192-, and 256-bit key sizes AES – OFB[21] mode for 128-bit key size	#2289
Triple-DES[22] – CBC mode for keying options 1 and 2	#1439
Asymmetric Key Algorithm	
RSA (PKCS[23]#1, X9.31) key pair generation (2048-bit), signature generation (2048-bit), signature verification(1024-, 2048-bit)	#1178
Secure Hashing Algorithm (SHA)	
SHA[24]-1, SHA-224, SHA-256, SHA-384, SHA-512	#1973
SHA-1 (Integrity Test)	#1972
Message Authentication Code (MAC) Function	
HMAC[25] SHA-1	#1406
Pseudo Random Number Generator (PRNG)	
ANSI x9.31 Appendix A.4.2 Pseudo Random Number Generator	#1140

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.
- As of January 1, 2014, the use of the RNGs specified in FIPS 186-2, [X9.31] and ANS [X9.62] are deprecated from 2011 through December 31, 2015, and disallowed after 2015.
- 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-FIPS-approved algorithm implementations that are allowed to be used in Approved mode of operation:

- Diffie-Hellman key exchange (2048-bit)
  - Caveat: Diffie Hellman (key agreement; key establishment methodology) provides 112 bits of encryption strength, for 2048-bit public keys. Diffie-Hellman provides higher bits of encryption strength with higher key sizes; non-compliant with less than 112 bits of encryption strength. After December 31, 2013, |n| ≤ 223 bits shall not be used in a key agreement scheme. Please see NIST Special Publication 800-131A for further details.
- MD5 (for TLS use)
- HMAC SHA-1-96
- RSA key wrapping/unwrapping

[19] CBC – Cipher Block Chaining
[20] CTR – Counter
[21] OFB – Output Feedback
[22] DES – Data Encryption Standard
[23] PKCS – Public-Key Cryptography Standards
[24] SHA – Secure Hashing Algorithm
[25] HMAC – (Keyed-) Hash Message Authentication Code

.

  - Caveat: RSA (key wrapping; key establishment methodology) provides 112 bits of encryption strength, for 2048-bit keys. RSA provides higher bits of encryption strength with higher key sizes; non-compliant with less than 112 bits of encryption strength.
- /dev/urandom
  - Non-Approved NDRNG[26] used for entropy gathering

[26] Non-Deterministic Random Number Generator

.

The module supports the critical security parameters (CSPs) listed below in Table 7.

Table 7 – List of Cryptographic Keys, Cryptographic Key Components, and CSPs

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
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 TLS session
TLS Session Key	AES 128-, 192-, 256-bit key Triple-DES 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, key exchange, certificate generation (TLS sessions)
RSA Public Key	RSA 1024, 2048-bit Key	Internally generated – Generated by call during first boot	Output from module	Stored in Flash memory	Factory reset, leaving FIPS mode, or GENERATE KEY command	Signature verification, key exchange with 2048-bit only, certificate generation (TLS sessions)
ANSI X9.31 PRNG Seed	128-bit random value	Gathered from system entropy (/dev/urandom)	Never output from module	Stored in NVRAM	Removing NVRAM battery, host reboot	Signature Generation, Key Generation
ANSI X9.31 PRNG Seed Key	128-bit random value	Gathered from system entropy (/dev/urandom)	Never output from module	Stored in NVRAM	Removing NVRAM battery, host reboot	Signature Generation, Key Generation

.

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
DH Public Components	Public components of DH protocol (2048-bit key)	Internally generated	Output from module via Data Output interface	Plaintext in volatile memory	End session,power cycle, host reboot, factory reset, leaving FIPS mode, or GENERATE KEY command	Key exchange (TLS 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 sessions)
Firmware Update Signing Key	RSA 1024-bit signature with SHA-256	Hard-coded in plaintext	Never output from module	Stored in Flash memory	Never zeroized	Signature verification of OA Firmware updates

.

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[27]-32)
- uBoot SHA-1 Firmware Integrity Test (SHA-1)
- Cryptographic Library Integrity Test (HMAC SHA-1)
- Known Answer Tests (KATs)
    - AES encrypt KAT
    - AES decrypt KAT
    - Triple-DES encrypt KAT
    - Triple-DES decrypt KAT
    - RSA signature generation KAT
    - RSA signature verification KAT
    - HMAC SHA-1 KAT
    - X9.31 RNG KAT

2.8.2 Conditional Self-Tests

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

- ANSI X9.31 PRNG Continuous Self-Test
- RSA pairwise consistency check
- NDRNG Continuous Random Number Generator 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.

[27] CRC – Cyclic Redundancy Check

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, along with a specific hardware configuration, in order to be considered to be in FIPS-Approved mode of operation. Once configuredr for FIPS mode, the module only operates in FIPS-Approved mode of operation. The FIPS mode requires specific levels of entropy[28] in the random number generation functions. In order to ensure that the brand new appliance has the appropriate levels of entropy available, 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 enter “RESTART OA” which will cause a reboot. The reboot can also be performed from the GUI by navigating to “Enclosure Information”, then “Active Onboard Administrator”, 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 through a serial interface 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, it may be necessary to clear VC mode, 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 should provide guidance which ensures that the module is always operated in a secure/FIPS compliant configuration. It will generally include services and activities allotted to the Crypto-Officer. An example is provided below.

[28] Note: The module comes preloaded with atleast 128 bits of entropy from the factory.

The Crypto-Officer is responsible for making sure the module is running in FIPS-Approved mode of operation. The following algorithms, key sizes, protocols, and services listed in Table 5 cannot be used in FIPS-Approved mode of operation:

- MD5 (for non-TLS)
- RSA (1024-bit) (signature generation and key wrapping)
- SHA – 160 (for signature generation)
- Diffie-Hellman (1024-bit)
- DSA
- SSH (Secure Shell)
- RC4

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 Serial interface, utilizing getty, or a Web GUI via Ethernet interface, utilizing HTTPS (SSL[29]). Through these interfaces, a Crypto-Officer can configure and enable the FIPS mode of operation. 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 6 characters long. The characters supported are upper and lower-case letters, numbers, and some symbols.

Note that only TLS is supported by the module, when operating in FIPS mode. Other versions of SSL (v3.0 and under) are unsupported. Likewise, SNMP[30] is disabled in FIPS mode.

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 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.

[29] SSL – Secure Socket Layer

[30] SNMP – Simple Network Management Protocol

.

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.

4 Acronyms

This section defines the acronyms.

Table 8 – 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
CSEC	Communications Security Establishment Canada
CSP	Critical Security Parameter
CRC	Cyclic Redundancy Check
CTR	Counter
DDR	Double Data Rate
DES	Data Encryption Standard
DH	Diffie-Hellman
DSA	Digital Signature Algorithm
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FIPS	Federal Information Processing Standard
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
KAT	Known Answer Test
KVM	Keyboard-Video-Mouse
LCD	Liquid-Crystal Display
LDAP	Lightweight Directory Access Protocol
LED	Light-Emitting Diode
NIST	National Institute of Standards and Technology

.

Acronym	Definition
NTP	Network Time Protocol
NVLAP	National Voluntary Laboratory Accreditation Program
OA	Onboard Administrator
OFB	Output Feedback
PC	Personal Computer
PKCS	Public-Key Cryptography Standards
PPC	PowerPC
PRNG	Pseudo-Random Number Generator
RNG	Random Number Generator
RSA	Rivest Shamir and Adleman
SHA	Secure Hash Algorithm
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOAP	Simple Object Access Protocol
SSH	Secure Shell
SSL	Secure Socket Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
USB	Universal Serial Bus
VC	Virtual Connect
VGA	Video Graphics Array
VSS	Visual Source Safe

Prepared by:
Corsec Security, Inc.

13135 Lee Jackson Memorial Highway, Suite 220
Fairfax, VA 22033
United States of America

Phone: (703) 267-6050
Email: info@corsec.com
http://www.corsec.com