Hewlett-Packard Development Company, L.P.

iLO 3 Cryptographic Module

Firmware Version: 1.50

Hardware Version: ASIC (GLP: 531510-003) with Flash Memory (41050DL00-233-G), NVRAM (420102C00-244-G), and DDR3 SDRAM (42020BJ00-216-G);
ASIC (GXE: 438893-503) with Flash Memory (41050DL00-233-G), NVRAM (420102C00-244-G), and DDR2 SDRAM (459715-002)

FIPS 140-2 Non-Proprietary Security Policy

FIPS Security Level: 1
Document Version: 1.8

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 Highway, Suite 220
Fairfax, VA 22033
United States of America

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

Table of Contents

1 INTRODUCTION 3
1.1 PURPOSE 3
1.2 REFERENCES 3
1.3 DOCUMENT ORGANIZATION 3

2 ILO 3 CRYPTOGRAPHIC MODULE 4
2.1 OVERVIEW 4
2.2 MODULE SPECIFICATION 7
2.3 MODULE INTERFACES 8
2.4 ROLES AND SERVICES 9
2.4.1 Crypto Officer Role 10
2.4.2 User Role 11
2.4.3 Additional Services 12
2.5 PHYSICAL SECURITY 12
2.6 OPERATIONAL ENVIRONMENT 12
2.7 CRYPTOGRAPHIC KEY MANAGEMENT 12
2.8 EMI/EMC 17
2.9 SELF-TESTS 17
2.9.1 Power-Up Self-Tests 17
2.9.2 Conditional Self-Tests 17
2.10 MITIGATION OF OTHER ATTACKS 17

3 SECURE OPERATION 18
3.1 CRYPTO OFFICER GUIDANCE 18
3.1.1 Initialization 18
3.1.2 Secure Management 19
3.1.3 Loading TLS Keys 19
3.2 USER GUIDANCE 20

4 ACRONYMS 21

Table of Figures

FIGURE 1 – ILO 3 ASIC 4

List of Tables

TABLE 1 – COMPARISON OF HP ILO 3 ADVANCED AND STANDARD FEATURES 5
TABLE 2 – SECURITY LEVEL PER FIPS 140-2 SECTION 7
TABLE 3 – FIPS 140-2 LOGICAL INTERFACE MAPPINGS 8
TABLE 4 – CRYPTO OFFICER SERVICES 10
TABLE 5 – USER SERVICES 11
TABLE 6 – FIPS-APPROVED ALGORITHM IMPLEMENTATIONS IN HARDWARE 12
TABLE 7 – FIPS-APPROVED ALGORITHM IMPLEMENTATIONS IN FIRMWARE 13
TABLE 8 – FIPS NON-APPROVED ALGORITHM IMPLEMENTATIONS 14
TABLE 9 – FIPS NON-COMPLIANT ALGORITHM IMPLEMENTATIONS 14
TABLE 10 – LIST OF CRYPTOGRAPHIC KEYS, CRYPTOGRAPHIC KEY COMPONENTS, AND CSPS 15
TABLE 11 – ACRONYMS 21

1 Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the iLO 3 Cryptographic Module from Hewlett-Packard Development Company, L.P., or HP. This Security Policy describes how the iLO 3 Cryptographic Module 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 iLO 3 Cryptographic Module is referred to in this document as iLO, the cryptographic 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 (http://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.

2 iLO 3 Cryptographic Module

2.1 Overview

HP Integrated Lights-Out (iLO), an ASIC[1] also referred to as the GLP or GXE, and its supporting hardware, are incorporated directly onto the motherboards of HP BladeSystem blade servers and storage blades. iLO is an autonomous management subsystem embedded directly on the server. HP iLO management processors for HP ProLiant Gen7 servers virtualize system controls to help simplify server setup, engage health monitoring, provide power and thermal control, and promote remote administration of HP ProLiant ML, DL, SL, and BL servers. iLO is also the foundation of BladeSystem High Availability (HA) embedded server and fault management. iLO provides system administrators with secure remote management capabilities regardless of the server status or location. iLO is available whenever the blade server is connected to a power source, even if the server main power switch is in the Off position.

Remote access is the key to maximizing efficiency of administration and troubleshooting for enterprise servers. BladeSystem blade servers are designed so that administrative functions that are performed locally can also be performed remotely. iLO enables remote access to the operating system console, control over the server power and hardware reset functionality, and works with the server to enable remote network booting through a variety of methods. Figure 1 shows an iLO ASIC chip.

Figure 1 – iLO 3 ASIC

The iLO ASIC is an independent microprocessor running an embedded real-time operating system. The architecture ensures that the majority of iLO functionality is available, regardless of the state of the host operating system. The HP Lights-Out Online Configuration Utility is available for Windows and Linux operating systems. iLO adds support for Microsoft device driver support, improved .NET framework support, and HP SIM[2] SSO[3] support. iLO drivers and agents are available for the following network operating systems: Microsoft® Windows® Server 2008 R2/2008/2003/2003 web edition and Microsoft small business server 2003 for the HP ProLiant server ML300 series. iLO drivers and agents are also

[1] ASIC – Application-Specific Integrated Circuit
[2] SIM – System Insight Manager
[3] SSO – Single Sign-On

available for Red Hat Enterprise Linux 5 (32-bit x86), RedHat Enterprise Linux 5 (AMD64/EM64T), SUSE[4] Linux Enterprise Server 10, and SUSE Linux Enterprise Server 11 Operating Systems (OS).

iLO functions out-of-the-box without additional software installation. It functions regardless of the servers' state of operation, and uses a local account database or directory service to authenticate and authorize its users. iLO can be accessed from any location via a web browser and works hand-in-hand with HP Systems Insight Manager, Insight Control, and Insight Dynamics, helping customers unleash the value of the ProLiant platform and deliver the highest possible quality of IT[5] service to the business.

Advanced features of iLO, available via licensing, include (but are not limited to) the following: graphical remote console, multi-user collaboration, power and thermal optimization, health monitoring, virtual media, and console video recording and playback. The advanced features offer sophisticated remote administration of servers in dynamic data center and remote locations. A comparison of standard and advanced functionality is shown in Table 1.

Table 1 – Comparison of HP iLO 3 Advanced and Standard Features

Feature	HP iLO 3 Advanced for Blade Systems	HP iLO 3 Standard for Blade Systems	HP iLO 3 Advanced	HP iLO 3 Standard
iLO Remote Administration				
Virtual Keyboard, Video, Mouse (KVM)	Full text and graphic modes (pre-OS & OS)	Full text and graphic modes (pre-OS)	Full text and graphic modes (pre-OS & OS)	Full text and graphic modes (pre-OS)
Global Team Collaboration (Virtual KVM)	Up to 6 Server Administrators		Up to 6 Server Administrators	
Console Record and Replay	✓		✓	
Virtual Power	✓	✓	✓	✓
Virtual Media	✓	Browser Only	✓	
Virtual Folders	✓		✓	
Remote Serial Console[6]	SSH[7] Only	SSH Only	SSH Only	SSH Only
Virtual Unit Indicator Display	✓	✓	✓	✓
Simplified Server Setup				
ROM[8]-Based Setup Utility (RBSU)	✓	✓	✓	✓
Option ROM Configuration for Arrays (ORCA)	✓	✓	✓	✓

[4] SUSE – It was originally a German acronym for "Software und System Entwicklung", meaning "Software and systems development
[5] IT – Information Technology
[6] Remote Serial Console feature only available while operating in the non-Approved mode of operation
[7] SSH – Secure Shell
[8] ROM – Read-Only Memory

.

Feature	HP iLO 3 Advanced for Blade Systems	HP iLO 3 Standard for Blade Systems	HP iLO 3 Advanced	HP iLO 3 Standard
Power Management & Control				
Present Power Reading	✓	✓	✓	✓
Power Usage Reporting	✓		✓	
Ambient Temperature Reporting	✓	✓	✓	✓
Dynamic Power Capping	✓		✓	
Power Supply High-Efficiency Mode	✓	✓	✓	✓
Sea of Sensors	✓	✓	✓	✓
Embedded System Health				
Power On Self Test (POST) and Failure Sequence Replay	✓		✓	
iLO and Server Integrated Management Log	✓	✓	✓	✓
Advanced Server Management (ASM)	✓	✓	✓	✓
Alert Administrator (SNMP[9] Passthrough)	✓	✓	✓	✓
System Health & Configuration Display	✓	✓	✓	✓
Access Security				
Directory Services Authentication	✓		✓	
Locally Stored Accounts	✓	✓	✓	✓
Interfaces				
Browser	✓	✓	✓	✓
Command Line	✓	✓	✓	✓
Extensible Markup Language (XML)/Perl Scripting	✓	✓	✓	✓
Integrated Remote Console for Windows Clients	✓	✓	✓	✓
Java Applet Client for Windows and Linux Clients	✓	✓	✓	✓

[9] SNMP - Simple Network Management Protocol

.

Feature	HP iLO 3 Advanced for Blade Systems	HP iLO 3 Standard for Blade Systems	HP iLO 3 Advanced	HP iLO 3 Standard
Security Protocols				
Transport Layer Security (TLS)	✓	✓	✓	✓
Secure Shell (SSH) [10]	✓	✓	✓	✓
RC4/AES[11] (Virtual KVM) [12]	✓	✓	✓	✓
Network Connectivity				
Dedicated Network Interface Controller (NIC)	✓	✓	✓	✓
Shared Network Port	✓	✓	✓	✓

HP iLO 3 Cryptographic Module is validated at the FIPS 140-2 section levels listed in Table 2.

Table 2 – 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
7	Cryptographic Key Management	1
8	EMI/EMC[13]	1
9	Self-tests	1
10	Design Assurance	1
11	Mitigation of Other Attacks	N/A[14]
14	Cryptographic Module Security Policy	1

2.2 Module Specification

iLO is a hardware module with a multiple-chip embedded embodiment. The overall security level of the module is 1. The cryptographic boundary of the module is defined by:

- iLO ASIC (GLP: 531510-003), deployed with:

[10] Feature only available while operating in the non-Approved mode of operation
[11] AES - Advanced Encryption Standard
[12] Feature only available while operating in the non-Approved mode of operation
[13] EMI/EMC – Electromagnetic Interference / Electromagnetic Compatibility
[14] N/A – Not Applicable

- Flash Memory chip (41050DL00-233-G)
- Battery-backed NVRAM[15] (420102C00-244-G)
- DDR3[16] SDRAM[17] (42020BJ00-216-G)
- The traces between these components

- iLO ASIC (GXE: 438893-503), deployed with:
  - Flash Memory chip(41050DL00-233-G)
  - Battery-backed NVRAM (420102C00-244-G)
  - DDR2 SDRAM (459715-002)
  - The traces between these components

The module includes the iLO firmware. With the exception of power and ground pins, all data pins on the Flash and RAM[18] chips lead directly to the iLO processor and do not cross the module boundary.

HP affirms that all HP server blades that run the iLO GXE and GLP ASICs specified in this module will perform the same as this module regardless of the specific SDRAM, NVRAM, or flash memory chips used. All HP hardware components must meet HP's rigorous part requirements and demonstrate the HP required functionality.

2.3 Module Interfaces

iLO offers a WebUI[19] (accessible over TLS[20]) management interface. The module's design separates the physical ports into five logically distinct categories. They are:

- Data Input
- Data Output
- Control Input
- Status Output
- Power

The iLO processor provides several power and ground interfaces to the module, as do the Flash and RAM chips. The physical ports and interfaces of the module comprise the individual pins on the iLO processor as described by logical interfaces in Table 3. All of these interfaces are also separated into logical interfaces defined by FIPS 140-2 in Table 3 below.

Table 3 – FIPS 140-2 Logical Interface Mappings

Physical Port/Interface	Quantity	FIPS 140-2 Interface
LPC[21]/PCIe[22]	1	• Data Input • Data Output
USB 2.0[23]	1	• Data In • Data Out • Control In • Status Out

[15] NVRAM – Non-Volatile Random Access Memory
[16] DDR3 – Double Data Rate v3
[17] SDRAM – Synchronous Dynamic Random Access Memory
[18] RAM – Random Access Memory
[19] WebUI – Web User Interface
[20] TLS – Transmission Layer Security
[21] LPC – Low Pin Count
[22] PCIe – Peripheral Component Interconnect Express

.

Physical Port/Interface	Quantity	FIPS 140-2 Interface
PECI[24]	1	• Data Input • Data Output
VGA[25]/DVI[26] (GLP/GXE)	1	• Data Out • Status Out
Clock In	2	• Data In
GPIO[27]	2	• Control In • Status Out
PS/2[28]	2	• Data In • Control In
GMII[29]/MII[30] (Primary Ethernet)	1	• Data In • Data Out • Control In • Status Out
RMII[31]/MII (Secondary Ethernet)	1	• Data In • Data Out • Control In • Status Out
UART[32]	2	• Control In • Status Out
PWM[33]	8	• Data Out
SPI[34]	1	• Data In • Data Out
Power	4	• Power In

2.4 Roles and Services

The module supports two roles that operators may assume: a Crypto Officer (CO) role and a User role.

[23] USB – Universal Serial Bus
[24] PECI – Platform Environmental Control Interface
[25] VGA – Video Graphics Array
[26] DVI – Digital Visual Interface
[27] GPIO – General Purpose Input Output
[28] PS/2 – Personal System/2
[29] GMII – Gigabit Media Independent Interface
[30] MII – Media Independent Interface
[31] RMII – Reduced Media Independent Interface
[32] UART – Universal Asynchronous Receiver/Transmitter
[33] PWM – Power Management
[34] SPI – Serial peripheral Interface

.

2.4.1 Crypto Officer Role

The Crypto Officer role has the ability to configure the iLO. This role is assigned when the first operator logs into the system using the default username and password. Only the Crypto Officer can create other users and provision the iLO to operate in FIPS-Approved mode. Crypto Officer services are provided via the supported secure protocols, specifically Transport Layer Security (TLS). Descriptions of the services available to the Crypto Officer are provided in Table 4. Please note that the keys and CSPs listed in the table indicate the type of access required using the following notation:

- R – Read: The CSP[35] 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 4 – Crypto Officer Services

Service	Description	Input	Output	CSP and Type of Access
Authenticate	CO logs into iLO	Command and parameters	Command response / Status output	Password – R/X
Add, remove, modify or assign users and roles	Creating, editing and deleting users; Define user accounts and assign permissions	Command and parameters	Command response / Status output	Password – W/R/X
View system information	View and monitor system information, event logs, power settings, etc	Command	Command response / Status output	None
Configure the module and host server	Configure and manage the module and host system parameters such as Remote console, Virtual media, power management, network management and host server	Command and parameters	Command response / Status output	Password – R/X
Activate or deactivate licensed features	Enable advanced features including graphical remote console, multi-user collaboration, power and thermal optimization, health monitoring, virtual media, and console video recording and playback	Command and parameters	Command response / Status output	Password – R/X
Set FIPS mode	Set the FIPS mode flag	Command	Command response / Status output	Password – R/X
Zeroize keys and CSPs	Zeroize all the keys and CSPs stored within iLO	Command	Command response / Status output	All – R/W/X

[35] CSP – Critical Security Parameter

.

Service	Description	Input	Output	CSP and Type of Access
Administer TLS certificates	Add, Remove, View, or Modify root and specific certificates for HTTPS connections *See Section 3.1.3 for details	Command	Command response / Status output	Password – R/X RSA[36] private/public keys – R/W
Show status	Facilitates the user to check whether the module is in FIPS-Approved mode or not	Command	Command response / Status output	Password – R/X
Perform self-tests	Perform Power-up Self Tests on demand	Reset or Power Cycle	Status output	None
Manage the module via WebUI	Login to the module via WebUI using TLS protocol to perform CO services	Command	Command response / Status output	Password – R/X RSAPublic key – R/X RSA Private key – R/W/X TLS Session key – R/W/X TLS Authentication Key – R/W/X
Firmware Upgrade	Loads new firmware and performs an integrity test using an RSA digital signature verification.	Command	Status output	Firmware Upgrade Authentication Key – R/X

2.4.2 User Role

The User role has the ability to monitor the module configurations and the host system. Descriptions of the services available to the User role are provided in the Table 5.

Table 5 – User Services

Service	Description	Input	Output	CSP and Type of Access
Authenticate	User logs into module	Command and parameters	Command response / Status output	Password – R/X
Change Password	Change the user's password	Command and parameters	Command response / Status output	Password – R/W/X
View system information	View and monitor system information, event logs, power settings, etc	Command	Command response / Status output	None
View network statistics	View and monitor network information and statistics	Command	Command response / Status output	Password – R/X

[36] RSA – Rivest, Shamir and Adleman

.

Service	Description	Input	Output	CSP and Type of Access
Show status	Facilitates the user to check whether the module is in FIPS-Approved mode or not	Command	Command response / Status output	Password – R/X
Perform self-tests	Perform Power-up Self Tests on demand	Reset or Power Cycle	Status output	None
Use the module via WebUI	Login to the module via WebUI using TLS protocol to perform user services	Command	Command response / Status output	Password – R/X RSA Public key – R/X RSA Private key – R/X TLS Session key – R/X TLS Authentication Key – R/X

2.4.3 Additional Services

The module offers additional services to both the CO and User, which are not relevant to the secure operation of the module. All services provided by the modules are listed in the *HP ProLiant Integrated Lights-Out 3 v1.05 User Guide; June 2010 (Third Edition)*. The User Guide is supplied with the shipment of the iLO modules or may be freely obtained at http://h20000.www2.hp.com/bizsupport/TechSupport/Home.jsp.

2.5 Physical Security

iLO 3 Cryptographic Module is a multiple-chip embedded cryptographic module. The module consists of production-grade components that include standard passivation techniques.

2.6 Operational Environment

The iLO 3 Cryptographic Module does not provide a general-purpose operating system (OS) to the user. The operating system is not modifiable by the operator and only the module's signed image can be executed.

2.7 Cryptographic Key Management

The module uses the FIPS-validated algorithm implementations in hardware as listed in Table 6.

Table 6 – FIPS-Approved Algorithm Implementations in Hardware

Algorithm	Certificate Number
Advanced Encryption Standard (AES) in OFB[37] mode (128-bit)	#2297 & #2298

Additionally, the module uses FIPS-Approved algorithms implemented in firmware as listed in Table 7.

[37] OFB – Output Feedback

Table 7 – FIPS-Approved Algorithm Implementations in Firmware

Algorithm	Certificate Number
Advanced Encryption Standard (AES) in CBC[38] mode (128-bit, 256-bit)	#2294, #2295, & #2296
Triple Data Encryption Standard (Triple-DES) in CBC mode (3-key)	#1443, #1444, #1445
RSA PKCS#1.5 Signature Verification (Mod 1024*, 2048)	#1183
RSA Signature Verification (Mod 4096)	#1182
DSA FIPS 186-2 Signature Verification (Mod 1024)*	#720
SHA[39]-1** and SHA-512	#1977, #1978, #1979
HMAC SHA-1	#1410

*Note: The use of RSA Mod (1024) and DSA Mod (1024) for Digital Signature Verification purpose is allowed for legacy-use.

**Note: The use of SHA-1 for the purpose of Digital Signature Generation is non-compliant. The use of SHA-1 for the purpose of Digital Signature Verification is allowed for legacy-use. Any other use of SHA-1 for non-digital signature generation applications is acceptable and approved.

Caveat: Additional information concerning RSA, DSA, or SHA-1, and specific guidance on transitions to the use of stronger cryptographic keys and more robust algorithms is contained in NIST Special Publication 800-131A.

The module utilizes the following key establishment methodology and key derivation functions, allowed for use in the FIPS-Approved mode:

- Diffie-Hellman (key agreement; key establishment methodology provides between 112 to 128-bits of encryption strength; non-compliant less than 112-bits of encryption strength). After December 31, 2013, $|n| \leq 223$ bits shall not be used in a key agreement scheme. Please see NIST Special Publication 800-131A for further details.
- TLS v1.0/v1.1 KDF[40]

The module utilizes the following non-FIPS-approved protocol and algorithm implementations that are allowed for use in a FIPS-Approved mode of operation:

- TLS
- MD5 (used in the TLS handshake)

The module implements the non-FIPS-Approved algorithms listed in Table 8. These algorithms are available in Non-FIPS-Approved mode of operation.

[38] CBC – Cipher Block Chaining
[39] SHA – Secure Hash Algorithm
[40] KDF – Key Derivation Function

.

Table 8 – FIPS non-Approved Algorithm Implementations

Algorithm	Non-Compliant Service(s)
RC2	Encryption and Decryption
RC4	Encryption and Decryption
HMAC-MD5	Message Authentication
DES	Encryption and Decryption

Additionally, the module implements the non-compliant, FIPS-Approved algorithms listed in Table 9. These implementations have not been validated. As such, these algorithms shall not be used in the FIPS-Approved mode of operation.

Table 9 – FIPS Non-Compliant Algorithm Implementations

Algorithm	Non-Compliant Service(s)
Triple-DES (2-key)	Encryption and Decryption
RSA Key Generation (Mod 2048 to 4096)	Asymmetric Key Generation, Certificate Signing Requests (CSRs)
RSA PKCS #1 Signature Generation (Mod 1024, 2048)	Signature Generation
RSA wrap and unwrap	Data wrapping and unwrapping
DSA Key Generation (Mod 1024, 2048)	Asymmetric Key Generation
DSA Signature Generation (Mod 1024, 2048)	Signature Generation
Non-Compliant DH (1024, 1536-bit)	Key Establishment
SHA-1	Signature Generation
FIPS 186-2 RNG	Random Number Generation

.

The module supports the critical security parameters (CSPs) listed below in Table 10.

Table 10 – List of Cryptographic Keys, Cryptographic Key Components, and CSPs

CSP	CSP Type	Generation/Input	Output	Storage	Zeroization	Use
RSA public key	1024, 2048-bit key	Imported via key loader utility (See section 3.1.3)	The module's public key component exits the module in plaintext	Flash (plaintext)	Exiting FIPS-Approved mode	Used for PKI authentication, TLS authentication, and RSA signature verification
RSA private key	2048-bit key	Imported via key loader utility (See section 3.1.3)	Never exits the module	Flash (plaintext)	Exiting FIPS-Approved mode	Used for PKI authentication and TLS authentication
DSA public key	1024-bit key	Imported via key loader utility (See section 3.1.3)	The module's public key component exits the module in plaintext	Flash (plaintext)	Exiting FIPS-Approved mode	Used for PKI authentication, TLS authentication, and DSA signature verification
Diffie-Hellman public key component	2048, 3072 bits	Derived internally via TLS Pseudo-Random Function	The module's Public key component exits the module in plaintext.	NVRAM (plaintext)	Exiting the session/reboot/power off	Used for key agreement during TLS sessions (deriving TLS Session and Authentication Key)
Diffie-Hellman private key component	224, and 256 bits	Derived internally via TLS Pseudo-Random Function	Never exits the module	NVRAM (plaintext)	Exiting the session/reboot/power off	Used for key agreement during TLS sessions (deriving TLS Session and Authentication Key)
TLS Pre-Master Secret	Shared Secret (384, 1024, 2048-bits)	Imported in encrypted form	Never exits the module	SDRAM (plaintext)	Exiting FIPS-Approved mode and Exiting the session/reboot/power off	Used to derive the TLS Master Secret as part of TLS Pseudo-Random Function
TLS Master Secret	Shared Secret (384-bits)	Derived internally via TLS Pseudo-Random Function	Never exits the module	SDRAM (plaintext)	Exiting FIPS-Approved mode and Exiting the session/reboot/power off	Used to derive the TLS Session and Authentication Key as part of TLS Pseudo-Random Function

.

CSP	CSP Type	Generation/Input	Output	Storage	Zeroization	Use
TLS Session Key***	TDES or AES	Derived internally via TLS Pseudo-Random Function	Never exits the module	NVRAM (plaintext)	Exiting FIPS-Approved mode and Exiting the session/reboot/power off	It is used for encrypting or decrypting the data traffic during the TLS session
TLS Authentication Key***	HMAC SHA-1	Derived internally via TLS Pseudo-Random Function	Never exits the module	NVRAM (plaintext)	Exiting FIPS-Approved mode and Exiting the session/reboot/power off	It is used for data integrity and authentication during TLS sessions
Password	Crypto Officer and User passwords	Entered by Crypto Officer or User	Never exits the module	Flash, NVRAM (plaintext)	Exiting FIPS-Approved mode	Used for authenticating the Crypto Officer or User
Firmware Upgrade Authentication Key	Hardcoded RSA 2048-bit key	Embedded in pre-boot image	Never exits the module	Image in Flash memory	The Flash location is write protected in hardware at the factory (i.e. not writeable by end user) and is not zeroized.	Used to verify RSA signature of items loaded through Firmware Upgrade utility

*** The vendor makes no conformance claims to any key derivation functions specified in SP800-135rev1. References to the key derivation functions addressed in SP 800-135rev1 including SSH, and TLS are only listed to clarify the key types supported by the module. Keys related to SSH, and TLS are only used in the Approved mode under the general umbrella of a non-Approved Diffie-Hellman scheme, with no assurance claims to the underlying key derivation functions.

2.8 EMI/EMC

The module was tested and found to be conformant to the EMI/EMC requirements specified by 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class A (i.e., for business use).

2.9 Self-Tests

This section explains the required self-test that the module implements.

2.9.1 Power-Up Self-Tests

iLO performs the following Power-Up Self-Tests:

- Firmware integrity check using 4096-bit RSA with SHA-512 (kernel and Dynamic Download signature verification)
- Known Answer Tests (KATs) in hardware
  - AES KAT
- KATs in Firmware
  - AES Encrypt and Decrypt KATs
  - Triple-DES Encrypt and Decrypt KATs
  - RSA Verify KAT
  - DSA Verify KAT
  - SHA-1 KAT
  - SHA-512 KAT
  - HMAC SHA-1 KAT

2.9.2 Conditional Self-Tests

iLO performs the Firmware Image Load Test using RSA-2048 with SHA-1 or SHA-512 (signature verification).

Upon failure of the firmware load test, the module enters an error state and the module will log the error messages. When the iLO enters the error state, the module operations are halted and it exits FIPS-Approved mode, all the keys and CSPs are zeroized, no further traffic is processed, and the module reboots. The module cannot perform any cryptographic operations while in the error state. All data output interfaces are inhibited when the error state exists.

2.10 Mitigation of Other Attacks

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

3 Secure Operation

The iLO 3 Cryptographic Module meet 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 Crypto Officer Guidance

The following sections provide the necessary step-by-step instructions for the secure installation of iLO card, as well as the steps necessary to configure the module for a FIPS Approved mode of operation.

3.1.1 Initialization

It is the Crypto Officer's responsibility to configure the module into the FIPS-Approved mode. iLO contains a distinct FIPS-Approved mode of operation that can be set through the configuration of a single parameter.

Once the host computer is properly installed within the blade chassis, iLO will execute in non-FIPS-Approved mode by default. iLO can be configured to operate in FIPS-Approved mode; it is expected that iLO will be configured for FIPS-Approved mode only once during initial host computer installation. Exiting the FIPS-Approved mode will factory reset the module and zeroize all the keys, CSPs, and user accounts.

The following steps outline the procedure for configuring iLO to run in FIPS-Approved mode:

- Access the iLO over the Ethernet port via WebUI (locally or over TLS)
- Use the default username and password provided on the server tag along with the iLO blade to log on.
- Under the "Administration" menu click on "Security" sub-menu. Under the "Security" sub-menu navigate to the "Encryption" tab.
- Under the Encryption Enforcement Settings, select the "FIPS Mode" check box and click on "Apply".
- iLO will wipe the memories, reinitialize (zeroizing all existing keying material), and reboot.
- Follow the steps outlined in Section 3.1.3 to load new TLS keys
- Access the iLO again, using the first two steps outlined above.
- Accept the new certificate.
- Under the "Administration" menu, click on the "User Administration" sub-menu. Check the box next to "Administrator", the only current Local User, and click the "Edit" button. Enter a new password in the "Password" text box. Reenter the password, to confirm, in the "Password Confirm" text box. Click the "Update User" button at the bottom of the page.
- Under the "Administration" menu, click on the "Management" sub-menu. The "SNMP Settings" tab contains SNMP configuration data. In the "Insight Management Integration" area, change the value of "Level of Data Returned" to "Disabled (No Response to Request)". Click "Apply". This disables SNMP.
- Under the "Administration" menu, click on the "Access Settings" sub-menu. Uncheck the checkbox for "Enable IPMI/DCMI over LAN on Port 623". Click "Apply". This disables IPMI.
- The module is now in FIPS-Approved mode.

Once the module is configured in a FIPS-Approved mode of operation, it is not possible to set this parameter back, directly. The module will remain configured for the FIPS-Approved mode until the host system is flashed with a new firmware image, or the module automatically performs a factory reset (which zeroizes all CSPs) as the result of a module error.

3.1.2 Secure Management

The module has a non-modifiable OS. A CO shall change the default password after first login. When a module is powered on for the first time, a CO must configure the module for FIPS mode by following the steps mentioned in Section 3.1.1. Additionally, the following usage policies apply:

- SNMP shall be disabled while the module is running in the FIPS-Approved mode of operation.
- The CO shall use the SPI interface for local administration.
- The CO shall not enter the DSA or RSA public keys manually while the module is operating in the FIPS-Approved mode.
- The CO shall import all keys being used by the module. The CO must ensure that all imported keys are generated using FIPS Approved methods. (See section 3.1.3)
- The CO shall not administer the module remotely using the SSH/CLI[41] via the Remote Serial Console.
- The CO shall not administer the module remotely using the virtual KVM interface.
- Remote administration must only be performed over the WebUI (HTTPS) interface.

Once a module is provisioned into FIPS mode, the module will operate and remain in FIPS-Approved mode of operation unless the module enters an error state and performs a factory reset. The Crypto-Officer can also exit FIPS-Approved mode on demand by either installing a new firmware image or restoring the module to factory default.

In order to check the module's FIPS mode status, the Crypto-Officer can check the "iLO Event Log" page, under the "Information" header. In the "Description" column of the event log, the text "FIPS Mode Enabled." should appear at the time when the iLO was powered on or the status was changed to enable it.

To operate the module in a FIPS-approved mode, the Crypto-Officer shall only make use of the algorithms specified in Table 6 and Table 7 of Section 2.7. The use of other algorithms in a FIPS-approved mode is not allowed.

3.1.3 Loading TLS Keys

During the initial set-up of the module and on the occasion when the TLS certificate expires, the Crypto Officer will be responsible for replacing the TLS certificate and keys stored on the module. Before following the instructions provided below, the CO shall generate a self-signed X.509 certificate on the module's host device. The certificate and associated private and public keys shall be saved with the ".DER" file extension.

3.1.3.1 Loading the Key Loader Utility

Prior to adding the certificate and keys onto the module, a key loader utility (keyloader.bin) must be loaded onto the iLO host device. The key loader utility can be obtained from ftp://ftp.hp.com/pub/softlib2/software1/pubsw-windows/p1468032246/v93851. The CO shall follow these steps every time in order to load the key loader utility onto the module:

1. Access and log on to the module's WebUI
2. Select and upload the "keyloader.bin" file via the "Firmware Update" service
   NOTE: This **does not** actually update the firmware. The file will only reside in SDRAM.
3. Click the "Upload" button to complete the loading of the Key Loader
4. Log out of the WebUI

3.1.3.2 Loading the TLS Certificate and Keys

Prior to loading the TLS certificate and keys onto the module, the CO shall install the "certloader.exe" program onto iLO host device. The program can be obtained from ftp://ftp.hp.com/pub/softlib2/software1/pubsw-windows/p1468032246/v93851. The CO shall follow these steps in order to load the TLS certificate and private and public key-pair onto the module:

[41] CLI – Command-Line Interface

1. Access the Operating System[42] of the iLO host device or directly attached GPC to the iLO host device
2. Run the certloader.exe program from the iLO host device or directly attached GPC to the iLO host device
3. Select the .DER file that contains the new TLS certificate and the .DER file that contains the new private and public key-pair
4. Click the "Download to iLO" button

3.2 User Guidance

The User does not have the ability to configure sensitive information on the module, with the exception of their password. The User must be diligent to pick strong passwords, and must not reveal their password to anyone. Additionally, the User should be careful to protect any secret/private keys in their possession.

[42] Operating System must be the Windows Operating System and shall have the iLO driver and .NET Framework 4.0 installed

.

4 Acronyms

Table 11 in this section describes the acronyms.

Table 11 – Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
API	Application Programming Interface
ASM	Advanced Server Management
ASIC	Application Specific Integrated Circuit
CA	Certificate Authority
CBC	Cipher Block Chaining
CBIT	Conditional Built In Test
CLI	Command Line Interface
CMVP	Cryptographic Module Validation Program
CO	Crypto Officer
CRNGT	Continuous Random Number Generator Test
CSEC	Communications Security Establishment Canada
CSP	Critical Security Parameter
CSR	Certificate Signing Request
DDR	Double Data Rate
DH	Diffie Hellman
DSA	Digital Signature Algorithm
ECC	Error-Correcting Code
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FIPS	Federal Information Processing Standard
GMII	Gigabit Media Independent Interface
GPC	General Purpose Computer
GPIO	General Purpose Input Output
HA	High Availability
HB	High Brightness
HMAC	(Keyed-) Hash Message Authentication Code
HP	Hewlett Packard
I^2C	Inter-Integrated Circuit

.

Acronym	Definition
iLO	Integrated Lights Out
IPMI	Intelligent Platform Management Interface
IT	Information Technology
JTAG	Joint Test Action Group
KAT	Known Answer Test
KVM	Keyboard, Video, Mouse
LPC	Low Pin Count
MB	Megabyte
MII	Media Independent Interface
NDRNG	Non-Deterministic Random Number Generator
NIC	Network Interface Card
NIST	National Institute of Standards and Technology
NVLAP	National Voluntary Laboratory Accreditation Program
NVRAM	Non-Volatile Random Access Memory
OFB	Output Feedback
ORCA	Option ROM Configuration for Arrays
OS	Operating System
PBIT	Power up Built In Test
PCIe	Peripheral Component Interconnect Express
PECI	Platform Environmental Control Interface
PKI	Public Key Infrastructure
POST	Power On Self Test
PRNG	Pseudo Random Number Generator
PS/2	Personal System/2
PWM	Power Management
RAM	Random Access Memory
RBSU	ROM-Based Set-up Utility
RMII	Reduced Media Independent Interface
RNG	Random Number Generator
ROM	Read-Only Memory
RSA	Rivest Shamir and Adleman
SD	Secure Digital
SDRAM	Synchronous Dynamic Random Access Memory
SHA	Secure Hash Algorithm

.

Acronym	Definition
SIM	System Insight Manager
SNMP	Simple Network Management Protocol
SPI	Serial Peripheral Interface
SSH	Secure Shell
SSO	Single Sign On
TCP	Transmission Control Protocol
TDES	Triple Data Encryption Standard
TLS	Transmission Layer Security
UART	Universal Asynchronous Receiver/Transmitter
USB	Universal Serial Bus
VGA	Video Graphics Array
WebUI	Web User Interface
XML	Extensible Markup Language

Prepared by:
Corsec Security, Inc.

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

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