Hewlett Packard Enterprise

iLO 5 Cryptographic Module

FIPS 140-2 Non-Proprietary Security Policy

Hardware Version: ASIC (GXP: 815393-001) with Flash Memory (1819-1208), NVRAM (1819-1209), and DDR3 SDRAM (2660-0461); Firmware Version: 2.45

Prepared for:

Hewlett Packard Enterprise

Hewlett Packard Enterprise Development LP
11445 Compaq Center Dr. W.

Houston, TX 77070
United States of America

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

Prepared by:

intertek acumen security

Acumen Security, LLC.

2400 Research Blvd.
Suite 395
Rockville, MD 20850
United States of America

Phone: +1 703 375 9820
www.acumensecurity.net

Table of Contents

List of Tables

©2024 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

List of Figures

©2024 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 iLO 5 Cryptographic Module from Hewlett Packard Enterprise Development LP (HPE). This Security Policy describes how the iLO 5 Cryptographic Module meets the security requirements of Federal Information Processing Standards (FIPS) Publication 140-2, which details the U.S.[1] and Canadian government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the National Institute of Standards and Technology (NIST) and the Canadian Centre for Cyber Security (CCCS) 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 security policy was prepared as part of the Level 1 FIPS 140-2 validation of the module. The iLO 5 Cryptographic Module is referred to in this document as iLO 5, 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 HPE website (www.hpe.com) contains information on the full line of products from HPE.
- The CMVP website (https://csrc.nist.gov/Projects/cryptographic-module-validation-program/validated-modules/Search) contains contact information for individuals responsible for answer technical or sales-related questions for the module.

[1] U.S. – United States

©2024 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

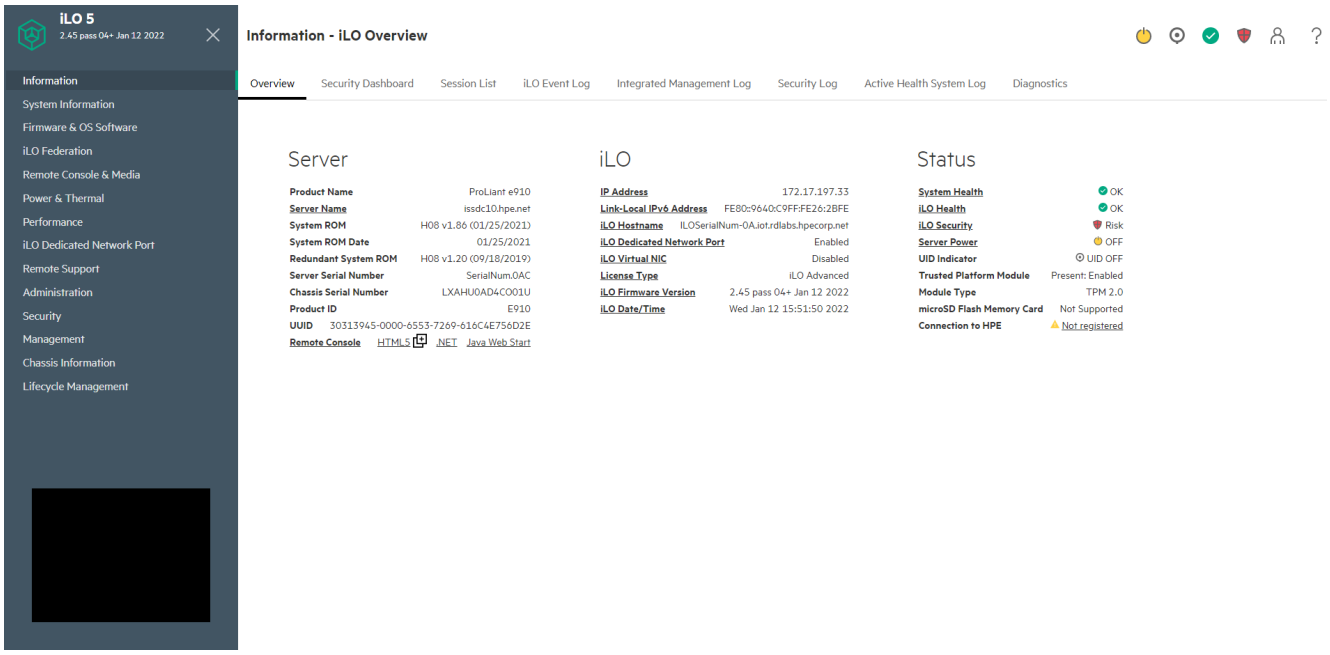
2. iLO 5

2.1 Overview

HPE's Integrated Lights-Out (iLO) is a proprietary embedded server management technology that provides out-of-band management functionality. HPE's fifth generation of iLO (iLO 5) is the foundation of HPE's Gen10 and Gen10 Plus series enterprise server consisting of HPE ProLiant servers and HPE Synergy systems. The HPE iLO 5 built into HPE ProLiant Gen10 and Gen10 Plus servers is an autonomous, secure management component embedded directly on the server motherboard. iLO 5 helps simplify initial server setup, power optimization, thermal optimization, and remote server administration. It also provides server health monitoring with the HPE Active Health System (AHS) and provides system administrators with true Agentless Management using SNMP[2] alerts from iLO 5, regardless of the state of the host server. The Embedded Remote Support (ERS) options allow Gen10 and Gen10 Plus servers to use their Insight Remote Support (IRS) server's registration from iLO 5, regardless of the operating system software and without the need for additional host software, drivers, or agents. The HPE AHS monitors and records changes in the server hardware and system configuration. iLO 5 provides system administrators with secure remote management capabilities regardless of the server status or location, and it is available whenever the server is connected to a power source, even if the server main power switch is in the Off position. Figure 1 below shows a screenshot of the iLO 5 management interface.

Figure 1 – HPE iLO 5 (Example Management Screen)

iLO 5 is supported on the following server platforms:



[2] SNMP – Simple Network Management Protocol

©2024 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

- HPE ProLiant Gen10 and Gen10 Plus DL Rack Servers
- HPE ProLiant Gen10 BL BladeSystem Servers
- HPE ProLiant Server Blade
- HPE ProLiant Gen10 and Gen10 Plus XL Scalable Servers
- HPE ProLiant Gen10 ML Servers
- HPE ProLiant MicroServer Gen10 and Gen10 Plus Servers
- HPE Edgeline Servers (ProLiant m750, ProLiant e910, and ProLiant e910t)
- HPE Synergy Gen10 and Gen10 Plus Compute Module
- HPE Apollo Gen10 and Gen10 Plus Servers

HPE enterprise servers are designed so that administrative functions that are performed locally can also be performed remotely. iLO 5 enables remote access to the operating system console, control over the server power, and hardware reset functionality. It also works with the server to enable remote network booting through a variety of methods.

The iLO 5 architecture ensures the availability of the majority of iLO 5 functionality, regardless of the state of the host operating system. The HPE Lights-Out Online Configuration Utility is available for Windows and Linux operating systems and VMware ESXi. Additionally, iLO 5 provides Microsoft device driver support, improved .NET framework support, and HPE SSO[3] support.

iLO 5 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 5 can be accessed from any location via a web browser and works hand-in-hand with HPE Systems Insight Manager, Insight Control, Insight Dynamics, HPE OneView and iLO Amplifier Pack.

Advanced features of iLO 5, 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 list of advanced functionality is shown in Table 1.

Table 1 – iLO 5 Features

Feature	iLO 5 Advanced
Virtual Keyboard, Video, Mouse (KVM[4])	Full text and graphic modes (pre-OS[5] & OS)
Global Team Collaboration (Virtual KVM)	Up to 6 Server Administrators
Console Record and Replay	✓
Virtual Power	✓
Virtual Media	✓
Virtual Folders	✓
Remote Serial Console	SSH[6] Only
Virtual Unit Indicator Display	✓
Email-based Alerting	✓
Drive Key Managers (i.e. ESKM[7])	✓

[3] SSO – Single Sign-On
[4] KVM – Keyboard, Video, Mouse
[5] OS – Operating System
[6] SSH – Secure Shell
[7] ESKM – Enterprise Secure Key Manager

©2024 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Feature	iLO 5 Advanced
ROM[8]-Based Setup Utility (RBSU)	✓
Present Power Reading	✓
Power Usage Reporting	✓
Ambient Temperature Reporting	✓
Dynamic Power Capping	✓
Power Supply High-Efficiency Mode	✓
Sea of Sensors	✓
Power-On Self-Test (POST) and Failure Sequence Replay	✓
iLO and Server Integrated Management Log	✓
Advanced Server Management	✓
Alert Administrator (SNMP Pass through)	✓
System Health & Configuration Display	✓
Directory Services Authentication	✓
Locally Stored Accounts	✓
Smartcard (CAC[9]/PIV[10]) Authentication	✓
Browser	✓
Command Line	✓
Extensible Markup Language (XML[11])/Perl Scripting	✓
Integrated Remote Console for Windows Clients	✓
Java Applet Client for Windows and Linux Clients	✓
RESTful[12] scripting	✓
Transport Layer Security (TLS)	✓
Secure Shell	✓
AES[13] (Virtual KVM)	✓
Dedicated Network Interface Controller (NIC)	✓
Shared Network Port	✓
iLO Federation Discovery	✓
iLO Federation Discovery Group License Activation	✓
iLO Federation Management	✓
Scan iLO and BIOS for malware	✓

[8] ROM – Read-Only Memory
[9] CAC – Common Access Card
[10] PIV – Personal Identification Verification
[11] XML – Extensible Markup Language
[12] REST – Representational State Transfer
[13] AES – Advanced Encryption Standard

©2024 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Feature	iLO 5 Advanced
High security modes (HIGH SECURITY, FIPS and CNSA[14])	✓
Firmware Verification	✓
Automatic Secure Recovery	✓

More details on these features are available in the iLO Licensing Guide.

iLO 5 is deployed in the form of an ASIC[15], a system-on-a-chip with an independent Cortex A9 processor running an embedded real-time operating system. iLO 5 ASICs for HPE enterprise Gen10 and Gen10 Plus servers virtualize system controls to help simplify server setup, engage health monitoring, provide power and thermal control, and promote remote administration of HPE Synergy, HPE ProLiant DL, XL, BL servers and HPE Edgeline servers. Figure 2 shows an iLO 5 ASIC.

Figure 2 – iLO 5 ASIC

The HPE iLO 5 Cryptographic Module includes the iLO 5 ASIC and its associated memory components incorporated directly onto the motherboards of HPE servers.

The iLO 5 is validated at the FIPS 140-2 Section levels shown 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[16]	1
9	Self-tests	1
10	Design Assurance	1
11	Mitigation of Other Attacks	N/A

[14] CNSA – Commercial National Security Algorithm
[15] ASIC – Application-Specific Integrated Circuit
[16] EMI/EMC – Electromagnetic Interference / Electromagnetic Compatibility

©2024 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

2.2 Module Specification

The iLO 5 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 surrounds the iLO 5 ASIC, Flash memory, battery-backed NVRAM[17], and DDR3[18] SDRAM[19] (see Table 3 for the part number of these components).

Table 3 – Module Components Part Numbers

Module Component	Part Number
ASIC	815393-001[20]
Flash Memory (16MB[21])	1819-1208
Battery-Backed NVRAM	1819-1209
DDR3 SDRAM	2660-0461

The module also includes the iLO 5 firmware and the circuit traces between the module's physical components. With the exception of power and ground pins, all data pins on the Flash and RAM[22] chips lead directly to the iLO 5 ASIC and do not cross the module boundary. The cryptographic boundary of the module and the relationship among the various internal components of the module are depicted in Figure 3 below.

[17] NVRAM – Non-Volatile Random Access Memory
[18] DDR3 – Double Data Rate v3
[19] SDRAM – Synchronous Dynamic Random Access Memory
[20] Some of these parts may be labelled 815393-001-B1; however, they are identical to those labelled 815393-001. Only the silkscreen is different.
[21] MB – Megabyte
[22] RAM – Random Access Memory

©2024 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

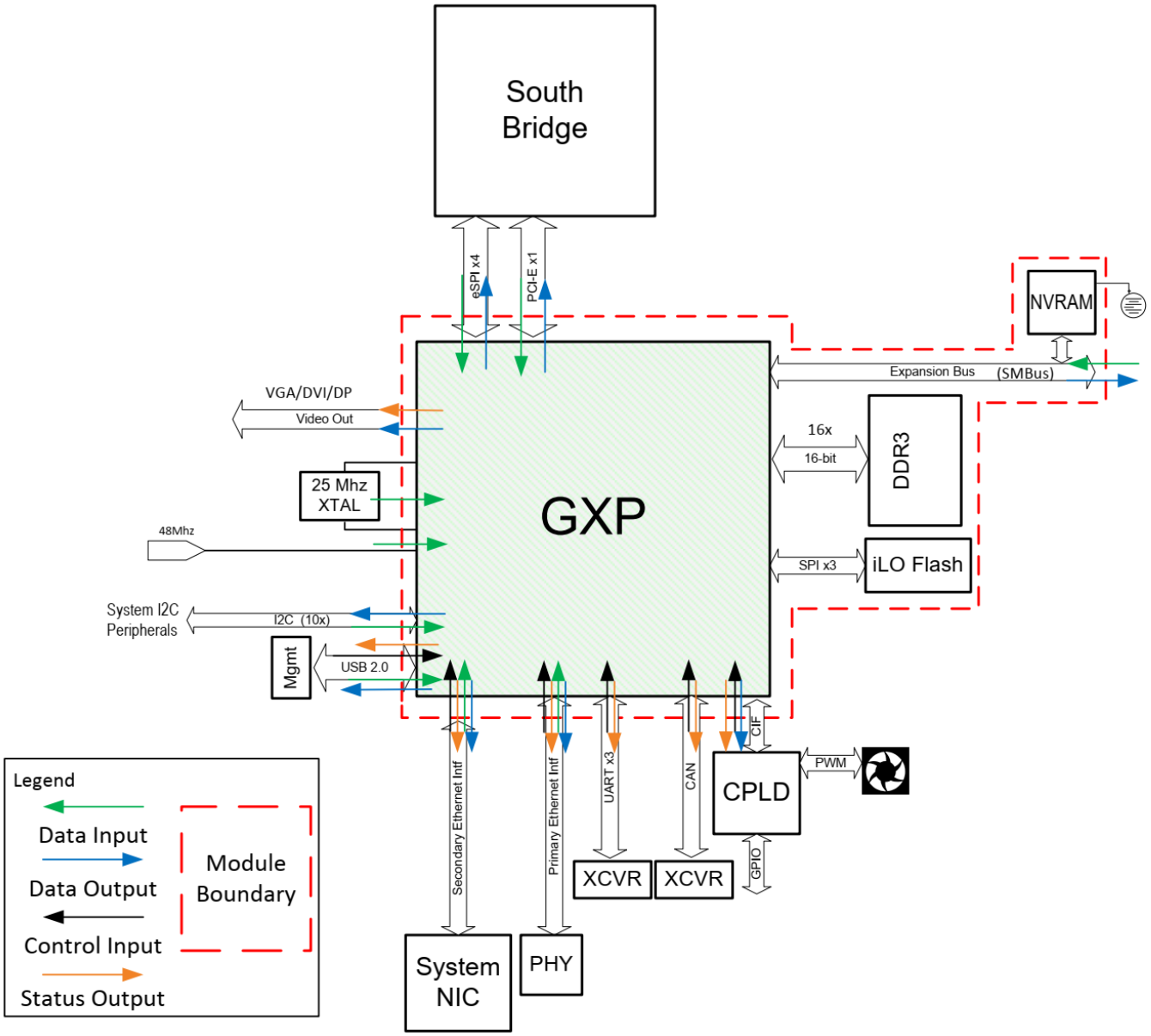


Figure 3 – iLO 5 Block Diagram

The cryptographic module was tested and found compliant using the specific part numbers shown in Table 3. However, HPE affirms that the GXP ASIC specified in this module will perform the same in all HPE servers regardless of the specific SDRAM, NVRAM, or flash memory chips used. All HPE hardware components must meet HPE's rigorous part requirements and demonstrate the HPE-required functionality.

The module uses the FIPS-Approved algorithm implementations in hardware as listed in Table 4.

©2024 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Table 4 – Hardware Algorithm Certificate Numbers

Algorithm	Certificate Number
AES Encryption/Decryption in OFB[23] mode (128-bit)	4467
AES GCM[24] Encryption/Decryption and Message Authentication with 128-, 256-bit keys	4467
AES Encryption/Decryption in CBC[25] mode (128, 256-bit)	4467
SHA[26]-384, SHA-512	3679

Additionally, the module uses FIPS-Approved algorithms implemented in firmware as listed in Table 5.

Note: Not all algorithms/modes tested for CAVP certificate #2273 are used and only those that are listed in Table 5 are used.

Table 5 – Firmware Algorithm Certificate Numbers

Algorithm	Certificate Number
AES Encryption/Decryption in CBC, OFB, CTR[27] modes (128, 256-bit)	A2273
AES GCM Encryption/Decryption/Generation/Verification (128, 256-bit)	A2273
RSA[28] (FIPS 186-4) Key Generation (2048, 3072-bit), Signature Generation (2048, 3072-bit), Signature Verification (2048, 3072, 4096-bit)	A2273
RSA (FIPS 186-2) Signature Verification (1024, 1536, 2048, 3072, 4096-bit)	A2273
DSA[29] (FIPS 186-4) Key Generation (2048, 3072-bit), Signature Generation (2048, 3072-bit), Signature Verification (2048, 3072-bit)	A2273
ECDSA[30] (FIPS 186-4) PKG/PKV/SigGen/SigVer for P-256 and P-384 curves	A2273
SHA[31]-1[32], SHA-256, SHA-384, SHA-512	A2273
HMAC[33] SHA-256, SHA-384, SHA-512	A2273
NIST SP[34] 800-90A based CTR_DRBG[35] (with 128-bit AES), no derivation function	A2273
CVL (SP 800-135[36] (TLS – KDF[37] and SSH – KDF))	A2273
KAS[38]-SSC[39](SP 800-56Arev3) ECC: ephemeralUnified (P-256, P-384) FFC: dhEphem (MODP -2048,	A2273

[23] OFB – Output Feedback
[24][24] GCM – Galois Counter Mode
[25] CBC – Cipher-Block Chaining
[26] SHA – Secure Hash Algorithm
[27] CTR – Counter
[28] RSA – Rivest, Shamir, and Adleman
[29] DSA – Digital Signature Algorithm
[30] ECDSA – Elliptical Curve Digital Signature Algorithm
[31] SHA – Secure Hash Algorithm
[32] Note: Additional information concerning RSA, DSA, and SHA-1, and specific guidance on transitions to the use of stronger cryptographic keys and more robust algorithms, is contained in NIST Special Publication 800-131Arev2.
[33] HMAC – (Keyed) Hash Messaged Authentication Code
[34] SP – Special Publication
[35] DRBG – Deterministic Random Bit Generator
[36] No parts of the TLS and SSH protocols, other than the KDF, have been tested by CAVP and CMVP.
[37] KDF – Key Derivation Function
[38] KAS – Key Agreement Scheme
[39] SSC – Shared Secret Computation

©2024 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Algorithm	Certificate Number
ffdhe2048, MODP-3072, ffdhe3072)	
KBKDF[40] based on HMAC SHA-512 – KDF (SP 800-108)	A2273
ENT (NP[41]) (SP 800-90B) Generated entropy: 256-bits	
CKG[42] (SP 800-133rev2)	vendor affirmed

KTS (AES Cert. #A2273 and HMAC Cert. #A2273; key establishment methodology provides between 128 and 256 bits of encryption strength).

The module claims KAS for both KAS-FFC & KAS-ECC as per the IG D.8 scenario X1 path(2) with the following caveats:

KAS (KAS-SSC Cert. #A2273, CVL Cert. #A2273; key establishment methodology provides between 128 and 192 bits of encryption strength).

KAS (KAS-SSC Cert. #A2273, CVL Cert. #A2273; key establishment methodology provides between 112 and 128 bits of encryption strength)

The KAS-FFC and KAS-ECC strengths are as follows:

KAS-ECC-SSC: 128 and 192 bits of encryption strength

KAS-FFC-SSC: 112 and 128 bits of encryption strength

Note: Additional information concerning RSA, DSA, and SHA-1, and specific guidance on transitions to the use of stronger cryptographic keys and more robust algorithms, is contained in NIST Special Publication 800-131Arev2.

Note: The module satisfies the requirements of FIPS 140-2 I.G 7.19 for full conformance to SP 800-90B.

When the module generates symmetric keys or seeds used for generating asymmetric keys, unmodified DRBG output is used as the symmetric key or as the seed for generating the asymmetric keys.

The module utilizes the following non-Approved algorithm implementations that are allowed for use in an Approved mode of operation:

- RSA (key wrapping; key establishment methodology provides between 112 and 128 bits of encryption strength)
  * PKCS#1-v1.5 padding is performed as shown in Section 8.1 of RFC 2313. The module supports PKCS#1 v1.5, which is allowed per IG D.9.

[40] KBKDF – Key Based Key Derivation Function

[41] Non-Physical Noise Source

[42] CKG – Cryptographic Key Generation

©2024 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

2.3 Module Interfaces

iLO 5 offers a WebUI[46] (accessible over TLS) and a Command Line Interface (CLI) (accessible over SSH) management interfaces. The module's design separates the physical ports into five logically distinct categories:

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

The iLO 5 ASIC 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 5 ASIC as described by logical interfaces in Table 6. All of these interfaces are also separated into logical interfaces defined by FIPS 140-2 in Table 6 below.

Table 6 – FIPS 140-2 Logical Interface Mappings

Physical Port/Interface	Quantity	FIPS 140-2 Interface
PCIe[47]	1	• Data Input • Data Output
CAN[48]	1	• Control Input • Status Output
eSPI[49]	4	• Data Input • Data Output
USB 2.0[50]	1	• Data Input • Data Output • Control Input • Status Output
SMBus[51]	1	• Data Input • Data Output
VGA[52]/DVI[53]/DP[54]	1	• Data Output • Status Output
Clock In	2	• Data Input

[46] WebUI – Web User Interface
[47] PCIe – Peripheral Component Interconnect Express
[48] CAN – Controller Area Network
[49] eSPI – Enhanced Serial Peripheral Interface
[50] USB – Universal Serial Bus
[51] SMBus – System Management Bus
[52] VGA – Video Graphics Array
[53] DVI – Digital Visual Interface
[54] DP – Display Port

©2024 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Physical Port/Interface	Quantity	FIPS 140-2 Interface
GPIO[55]	2	• Control Input • Status Output
I2C[56]	10	• Data Input • Data Output
GMII[57]/MII[58] (Primary Ethernet)	1	• Data Input • Data Output • Control Input • Status Output
RMII[59]/MII (Secondary Ethernet)	1	• Data Input • Data Output • Control Input • Status Output
UART[60]	3	• Control Input • Status Output
CIF[61]	1	• Data Output • Control Input • Status Output
SPI[62]	3	• Data Input • Data Output
Power	4	• Power Input

[55] GPIO – General Purpose Input Output
[56] I2C – Inter-Integrated Circuit
[57] GMII – Gigabit Media Independent Interface
[58] MII – Media Independent Interface
[59] RMII – Reduced Media Independent Interface
[60] UART – Universal Asynchronous Receiver/Transmitter
[61] CIF – Common Interface Format
[62] SPI – Serial Peripheral Interface

©2024 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

2.4 Roles and Services

The module supports two roles (as required by FIPS 140-2) that operators may assume: a Crypto Officer (CO) role and a User role. Roles are assumed explicitly by using a username and password or based on certificate-based credentials on a CAC/PIV card.

Please note that the keys and Critical Security Parameters (CSPs) 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.

2.4.1 Crypto Officer Role

The CO role has the ability to configure the module. This role is assigned when the first operator logs into the system using the default username and password. Only the CO can create other users and provision the iLO 5 to operate in FIPS-Approved mode. CO services are provided via the supported secure protocols, specifically Transport Layer Security (TLS) and SSH. Descriptions of the services available to the CO role are provided in Table 7 below.

Table 7 – Crypto Officer Services

Service	Description	CSP and Type of Access
Authenticate	Authenticate CO to module	Password – R/X
Add, remove, modify or assign users and roles	Create, edit, and delete users; Define user accounts and assign permissions	Password – R/W/X
View system information	View and monitor system information, event logs, power settings, etc.	Password – R/X
View network statistics (WebUI only)	View and monitor network information and statistics	Password – R/X
Configure the module and host server	Configure and manage the module and host system parameters such as Remote console[65], virtual media, power management, network management and host server	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	Password – R/X
Set FIPS mode	Set the FIPS mode flag	Password – R/X
Zeroize keys and CSPs	Zeroize all the keys and CSPs stored within iLO	All – W

[65] Note: Remote console can be configured and managed via WebUI only.

©2024 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Service	Description	CSP and Type of Access
Administer TLS certificates (WebUI only)	Add, remove, or view root and specific certificates for HTTPS[66] connections	Password – R/X RSA private/public keys – R/W/X ECDSA private/public keys – R/W/X
Show status	Indicate whether the module is in FIPS-Approved mode	Password – R/X
Perform self-tests	Perform power-up self-tests on demand	Entropy Input String – R/X DRBG Seed – R/W/X DRBG Key – R/W/X DRBG V Value – R/W/X
Access the module via SSH/CLI	Login to the module via CLI using SSH protocol to perform CO services	Password – R/X DSA Public key – R/W/X SSH Session key – R/W/X SSH Authentication Key – R/W/X RSA Public key – R/X RSA Private key – R/X ECDSA Public key – R/X ECDSA Private key – R/X Diffie-Hellman public key component – R/W/X Diffie-Hellman Private key component – R/W/X EC Diffie-Hellman public key component – R/W/X EC Diffie-Hellman Private key component – R/W/XAES GCM key – R/W/X AES GCM IV – R/W/X AES GCM key – R/W/X
Access the module via TLS/WebUI	Login to the module via WebUI using TLS protocol to perform CO services	Password – R/X RSA Public key – R/X RSA Private key – R/X ECDSA Public key – R/X ECDSA Private key – R/X Diffie-Hellman public key component – R/W/X Diffie-Hellman Private key component – R/W/X EC Diffie-Hellman public key component – R/W/X EC Diffie-Hellman Private key component – R/W/X TLS Pre-Master Secret – R/W/X TLS Master Secret – R/W/X TLS Session key – R/W/X TLS Authentication Key – R/W/X AES GCM key – R/W/X AES GCM IV – R/W/X KBKDF Secret Value – R/W/X
Access the module using CAC/PIV cards	Login to the module using CAC/PIV cards via certificate-based authentication over TLS protocol to perform CO services	RSA Public key – R/X RSA Private key – R/X ECDSA Public key – R/X ECDSA Private key – R/X Diffie-Hellman public key component – R/W/X Diffie-Hellman Private key component – R/W/X EC Diffie-Hellman public key component – R/W/X

[66] HTTPS – Hypertext Transfer Protocol Secure

©2024 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Service	Description	CSP and Type of Access
		EC Diffie-Hellman Private key component – R/W/X TLS Pre-Master Secret – R/W/X TLS Master Secret – R/W/X TLS Session key – R/W/X TLS Authentication Key – R/W/X AES GCM key – R/W/X AES GCM IV – R/W/X
Firmware Upgrade	Load new firmware and perform an integrity test using an RSA digital signature verification	Firmware Upgrade Authentication Key – R/X
Manage System Recovery Set	Create and manage a System Recovery Set from components stored in the iLO Repository.	Password – 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 Table 8 below.

Table 8 – User Services

Service	Description	CSP and Type of Access
Authenticate	User logs into module	Password – R/X
Change Password	Change the user's password	Password – R/W/X
View system information	View and monitor system information, event logs, power settings, etc.	None
View network statistics (WebUI only)	View and monitor network information and statistics	Password – R/X
Show status	Indicate whether the module is in FIPS-Approved mode	Password – R/X
Perform self-tests	Perform Power-up Self Tests on demand	Entropy Input String – RX DRBG Seed – RWX DRBG Key – R/W/X DRBG V Value – R/W/X
Access the module via CLI	Login to the module via CLI using SSH protocol to perform user services	Password – R/X DSA Public key – R/W/X SSH Session key – R/W/X SSH Authentication Key – R/W/X RSA Public key – R/X RSA Private key – R/X ECDSA Public key – R/X ECDSA Private key – R/X Diffie-Hellman public key component – R/W/X Diffie-Hellman Private key component – R/W/X EC Diffie-Hellman public key component – R/W/X EC Diffie-Hellman Private key component – R/W/X AES GCM key – R/W/X AES GCM IV – R/W/X

©2024 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Service	Description	CSP and Type of Access
Access the module via WebUI	Login to the module via WebUI using TLS protocol to perform user services	Password – R/X RSA Public key – R/X RSA Private key – R/X ECDSA Public key – R/X ECDSA Private key – R/X TLS Pre-Master Secret – R/W/X TLS Master Secret – R/W/X TLS Session key – R/W/X TLS Authentication Key – R/W/X AES GCM key – R/W/X AES GCM IV – R/W/X Diffie-Hellman public key component – R/W/X Diffie-Hellman Private key component – R/W/X EC Diffie-Hellman public key component – RW/X EC Diffie-Hellman Private key component – R/W/X KBKDF Secret Value – R/W/X
Access the module using CAC/PIV cards	Login to the module using CAC/PIV cards via certificate based authentication over TLS protocol to perform user services	RSA Public key – R/X RSA Private key – R/X ECDSA Public key – R/X ECDSA Private key – R/X TLS Pre-Master Secret – R/W/X TLS Master Secret – R/W/X TLS Session key – R/W/X TLS Authentication Key – R/W/X AES GCM key – R/W/X AES GCM IV – R/W/X Diffie-Hellman public key component – R/W/X Diffie-Hellman Private key component – R/W/X EC Diffie-Hellman public key component – R/W/X EC Diffie-Hellman Private key component – R/W/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 HPE iLO 5 User Guide*; April 2021, Edition: 1*. The User Guide is supplied with the shipment of the iLO 5 modules or may be freely obtained at the following webpage:

https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=a00105236en_us.

2.5 Physical Security

The iLO 5 is a multiple-chip embedded cryptographic module. The module consists of production-grade components that include standard passivation techniques.

2.6 Operational Environment

The module employs a non-modifiable operating environment. The module's firmware (Firmware version: 2.45)

©2024 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

is executed by the module's Cortex A9 processor. The module does not have a general-purpose operating system. The module also runs Green Hills Integrity 11.2.4 operating system, which is not possible to modify.

©2024 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

2.7 Cryptographic Key Management

The module supports the CSPs listed below in Table 9.

Table 9 – List of Cryptographic Keys, Cryptographic Key Components, and CSPs

CSP	CSP Type	Generation / Input	Output	Storage	Zeroization	Use
RSA public key	2048 and 3072-bit key	Internally generated or imported in plaintext	Exits the module in plaintext in the form of a certificate	NVRAM (plaintext)	Exiting FIPS-Approved mode	Used for PKI[69] authentication, TLS authentication, RSA signature verification, and certificate generation
RSA private key	2048 and 3072-bit key	Internally generated using NIST SP 800-90A CTR DRBG	Never exits the module	NVRAM (plaintext)	Exiting FIPS-Approved mode	Used for PKI authentication, TLS authentication, signature generation, and certificate generation
DSA public key	2048 and 3072-bit key	Imported in plaintext	Exits the module in plaintext	NVRAM (plaintext)	Exiting FIPS-Approved mode	Used for SSH user authentication.
ECDSA public key	NIST defined P-256 and P-384 curves	Internally generated or imported in plaintext	Exits the module in plaintext	NVRAM (plaintext)	Exiting FIPS-Approved mode	Used for PKI authentication, TLS authentication, signature verification, and certificate generation
ECDSA private key	NIST defined P-256 and P-384 curves	Internally generated using NIST SP 800-90A CTR DRBG	Never exits the module	NVRAM (plaintext)	Exiting FIPS-Approved mode	Used for PKI authentication, TLS authentication, signature verification, and certificate generation
Diffie-Hellman public key component	2048, 3072-bit	Internally generated or imported in plaintext	Exits the module in plaintext	DDR3 RAM (plaintext)	Session termination, rebooting, or power cycling	Used for key agreement during TLS and SSH sessions (deriving TLS and SSH session and authentication keys)

[69] PKI – Public Key Infrastructure

©2024 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

CSP	CSP Type	Generation / Input	Output	Storage	Zeroization	Use
Diffie-Hellman private key component	224, 256-bit	Internally generated using NIST SP 800-90A CTR DRBG	Never exits the module	DDR3 RAM (plaintext)	Session termination, rebooting, or power cycling	Used for key agreement during TLS and SSH sessions (deriving TLS and SSH session and authentication keys)
EC Diffie-Hellman public key component	NIST defined P-256 and P-384 curves	Internally generated or imported in plaintext	Exits the module in plaintext	DDR3 RAM (plaintext)	Session termination, rebooting, or power cycling	Used for key agreement during TLS and SSH sessions (deriving TLS and SSH session and authentication keys)
EC Diffie-Hellman private key component	NIST defined P-256 and P-384 curves	Internally generated using NIST SP 800-90A CTR DRBG	Never exits the module	DDR3 RAM (plaintext)	Session termination, rebooting, or power cycling	Used for key agreement during TLS and SSH sessions (deriving TLS and SSH session and authentication keys)
TLS Pre-Master Secret	Shared Secret (384, 1024, 2048-bit)	Imported in encrypted form with the server's RSA public key (for RSA key transport only)	Never exits the module	DDR3 RAM (plaintext)	Exiting FIPS-Approved mode, session termination, rebooting, or power cycling	Used to derive the TLS Master Secret as part of TLS Pseudo-Random Function
TLS Master Secret	Shared Secret (384-bit)	Internally generated via TLS Pseudo-Random Function	Never exits the module	DDR3 RAM (plaintext)	Exiting FIPS-Approved mode, session termination, rebooting, or power cycling	Used to derive the TLS Session and Authentication Keys as part of TLS Pseudo-Random Function
TLS Session Key	AES 128, 256-bit	Established internally using TLS KDF	Never exits the module	DDR3 RAM (plaintext)	Exiting FIPS-Approved mode, session termination, rebooting, or power cycling	Used for encrypting or decrypting the data traffic during the TLS session
TLS Authentication Key	HMAC with SHA-256, SHA-384, SHA-512	Generated internally using NIST SP 800-90A CTR DRBG	Never exits the module	DDR3 RAM (plaintext)	Exiting FIPS-Approved mode, session termination, rebooting, or power cycling	Used for data integrity and authentication during TLS sessions

©2024 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

CSP	CSP Type	Generation / Input	Output	Storage	Zeroization	Use
KBKDF Secret Value	Secret Key derived using SP 800-108 KBKDF	Established internally using KBKDF	Never exits the module	DDR3 RAM (plaintext)	Exiting FIPS-Approved mode, session termination, rebooting, or power cycling	Used for deriving additional keys using SP 800-108 KBKDF during Remote Console sessions
SSH Session Key	AES 256-bit	Generated internally using NIST SP 800-90A CTR DRBG	Never exits the module	DDR3 RAM (plaintext)	Exiting FIPS-Approved mode, session termination, rebooting, or power cycling	Used for encrypting or decrypting the data traffic during the SSH session
SSH Authentication Key	HMAC SHA-2 (256-bits)	Generated internally using NIST SP 800-90A CTR DRBG	Never exits the module	DDR3 RAM (plaintext)	Exiting FIPS-Approved mode, session termination, rebooting, or power cycling	Used for data integrity and authentication during SSH sessions
AES GCM Key	128, 256-bit	Generated internally using NIST SP 800-90A CTR DRBG *	Never exits the module	DDR3 RAM (plaintext)	Exiting FIPS-Approved mode, session termination, rebooting, or power cycling	Used for encrypting or decrypting the data traffic
AES GCM IV[70]	96-bits	Generated internally using NIST SP 800-90A CTR DRBG *	Never exits the module	DDR3 RAM (plaintext)	Exiting FIPS-Approved mode, session termination, rebooting, or power cycling	Used as an IV input to AES GCM function
DRBG Key	DRBG key	Internally generated using entropy input string	Never exits the module	DDR3 RAM (plaintext)	Rebooting or power cycling	DRBG internal state value
DRBG V Value	DRBG internal state value	Internally generated using entropy input string	Never exits the module	DDR3 RAM (plaintext)	Rebooting or power cycling	DRBG Internal state value
DRBG seed	256-bit value	Generated internally using entropy input	Never exits the module	DDR3 RAM (plaintext)	Exiting FIPS-Approved mode, session termination, rebooting, or power cycling	Random number generation
Entropy Input string	256-bit value	Generated internally by entropy source	Never exits the module	DDR3 RAM (plaintext)	Exiting FIPS-Approved mode, session termination, rebooting, or power cycling	Random number generation

[70] IV – Initialization Vector

©2024 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

CSP	CSP Type	Generation / Input	Output	Storage	Zeroization	Use
Password	Crypto-Officer and User passwords	Entered by Crypto-Officer or User	Never exits the module	NVRAM (stored in AES-256 CBC encrypted format)	Exiting FIPS-Approved mode	Used for authenticating the Crypto-Officer or User
Firmware Upgrade Authentication Key	Hardcoded with RSA 4096-bit public key	Embedded in pre-boot image	Never exits the module	Image in Flash memory	When overwritten with a new key	Used to verify RSA signature of items loaded through Firmware Upgrade utility

* Note: The AES GCM key and IV:

TLS: AES GCM key and IV are generated internally in cryptographic module using the module's Approved NIST SP 800-90A CTR DRBG and meet the requirements specified in IG A.5. The module follows the mechanism for IV generation defined in RFC 5288 and is used only within the TLS protocol and for the protocol versions specified in Section 4 of RFC 5288 which is TLS 1.2. The IV length is 96 bits. Overflow of the nonce_explicit would require 2^64 (~18.4 billion billion) messages within the same TLS session, so this is expected to never occur

SSH: The IV is only used in the context of the AES GCM mode encryptions within the SSHv2 protocol. The module is compliant with RFCs 4252, 4253 and RFC 5647.

©2024 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

2.8 EMI / EMC

iLO 5 was tested and found conformant to the EMI/EMC requirements specified by 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class A (business use).

2.9 Self-Tests

Cryptographic self-tests are performed by the module when the module is first powered up and loaded into memory as well as when a random number or asymmetric key pair is created. The following sections list the self-tests performed by the module, their expected error status, and the error resolutions.

2.9.1 Power-Up Self-Tests

iLO 5 performs the following self-tests at power-up to verify the integrity of the firmware images and the correct operation of the FIPS-Approved algorithms implemented in the module:

- Firmware integrity test using CRC-32 EDC verification of the kernel
- Firmware integrity test using CRC-32 EDC verification of the Dynamic Download
- Self-Tests in hardware
    - AES Encryption KAT[71]
    - AES Decryption KAT
    - AES GCM Encryption KAT
    - AES GCM Decryption KAT
    - SHA-512 KAT
- Self-Tests in firmware
    - AES Encryption KAT
    - AES Decryption KAT
    - AES GCM Encryption KAT
    - AES GCM Decryption KAT
    - SHA-1 KAT
    - HMAC with SHA-256, SHA-384, and SHA-512 KATs
    - RSA Signature Generation KAT
    - RSA Signature Verification KAT
    - DSA Pairwise Consistency Test
    - ECDSA Pairwise Consistency Test
    - EC DH KAT
    - DH KAT
    - TLS KDF KAT
    - SSH KDF KAT
    - KBKDF KAT
    - RCT on Entropy Source according to SP 800-90B §4.4.1 (runs over a continuously provided sequence of 1024 samples)
    - APT on Entropy Source according to SP 800-90B §4.4.2(runs over a continuously provided sequence of 1024 samples)
    - DRBG KAT

The power-up self-tests can be performed at any time by power-cycling the module or via resetting the module.

[71] KAT – Known Answer Test

©2024 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

2.9.2 Conditional Self-Tests

iLO 5 performs the following conditional self-tests (all in firmware):

- Continuous Random Number Generator Test (CRNGT) for the DRBG
- RCT according to SP 800-90B §4.4.1
- APT according to SP 800-90B §4.4.2
- RSA Pairwise Consistency Test for key pair generation
- DSA Pairwise Consistency Test for key pair generation
- ECDSA Pairwise Consistency Test for key pair generation
- Firmware Load Test (RSA 4096 bit signature verification)

2.9.3 Critical Functions Self-Tests

iLO 5 performs the following critical functions self-tests (all in firmware):

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

2.9.4 Self-Test Failure Handling

Upon failure of any power-up self-test, conditional self-test, or critical function test, the module demonstrates the following behavior:

- On failure of firmware integrity test, the module reaches the “Boot Error” state in which the module firmware is not loaded and the module aborts. The only way to continue from this state is by rebooting or power-cycling the module. If the error still exists, the module must be returned to the factory.
- In case of failure of any other self-test, the module reaches the “Critical Error” state and disables all access to cryptographic functions and CSPs. All data outputs via data output interfaces are inhibited upon any self-test failure. A permanent error status will be relayed via the status output interface, which is then recorded as an entry to the module log file and also relayed via the status output interfaces. The module then zeroizes all keys and CSPs, performs a reset to factory default settings, and performs a reboot. The factory default reset changes the FIPS mode flag, taking the module out of FIPS mode. The module will have to be reset in order to reconfigure the module to FIPS mode.

2.10 Mitigation of Other Attacks

This section is not applicable. The module does not mitigate any other attacks.

©2024 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

3. Secure Operation

The iLO 5 meets Level 1 requirements for FIPS 140-2. The sections below describe how to place and keep the module in the 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 5 card as well as the steps necessary to configure the module for a FIPS-Approved mode of operation.

3.1.1 Initialization

The module is delivered in an uninitialized factory state, and requires first-time configuration in order to operate in FIPS-Approved mode. Access to the module shall be limited to the Crypto-Officer, and it is the CO's responsibility to configure the module into the FIPS-Approved mode. In case the iLO 5 is deployed on a Synergy chassis, the locally connected Frame Link Module gains the initial access to iLO 5 and creates a CO account for future use. This access is inhibited once the CO completes all initialization steps. iLO 5 contains a distinct FIPS- Approved mode of operation that can be set through the configuration of a single parameter during initial initialization. The following sections provide the necessary step-by-step instructions for the secure installation of the iLO 5 as well as the steps necessary to configure the module for a FIPS-Approved mode of operation.

Once the host platform is properly installed, the CO shall immediately configure iLO 5 to operate in FIPS- Approved mode. It is expected that iLO 5 will be configured for FIPS-Approved mode only once during initial host platform installation.

The following steps outline the procedure to configure iLO 5 to run in FIPS-Approved mode:

1. Locate the iLO 5 Administrator name and password, located on the pull tab in the server's bezel.
2. Access the iLO 5 over the Ethernet port via WebUI (over TLS) using the IP address, e.g., https://192.168.1.4/.
3. Accept the certificate warning.
4. Use the credentials provided on the server's pull tab to log on.
5. Click on Security on the left.
6. Click on the Encryption tab.
7. In the Security Settings section's dropdown list, choose the FIPS option.
8. Click the Apply button.
9. Click the OK button on the pop-up warning.
10. iLO 5 will wipe the memories, reinitialize (zeroizing all existing keying material), and reboot.
11. Access the iLO again, using the first four steps outlined above.
12. Click on Administration on the left.
13. Put a check mark in the box next to Administrator under Local Users.
14. Click the Edit button.
15. Click on the checkbox for Change password.
16. Put in the New Password and Confirm Password textboxes, type the new Administrator password.
17. Click the Update User button.

©2024 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

18. Click on Security on the left.
19. Click on the SSL Certificate tab.
20. Click on the Customize Certificate button.
21. Please follow the steps provided in the section titled Obtaining and Importing an SSL Certificate of the HPE iLO 5 User Guide to configure the Certificate Signing Request (CSR) and import the new certificate.
22. Since the module resets, login again using the current username and password.
23. Click on Remote Console & Media on the left.
24. Click on the Security tab.
25. Change the IRC requires a trusted certificate in iLO option to Enabled.
26. Click the Apply button.

The module is now initialized and in FIPS-Approved mode.

3.1.2 Secure Management

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

- IPMI[72] shall be disabled while the module is running in the FIPS-Approved mode of operation.
- SNMP shall be disabled while the module is running in the FIPS-Approved mode of operation.
- The CO shall not enter the DSA or RSA public keys manually while the module is operating in the FIPS-Approved mode.
- Remote administration must only be performed over the WebUI (HTTPS) and CLI (SSH) interfaces.

Once the module is provisioned into FIPS mode during initialization, 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 restoring the module to factory default.

To check the module's FIPS mode status, the CO can check the "iLO Event Log" tab, under the "Information" page. 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.

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, if any.

Any firmware loaded into this module that is not shown on the module certificate is out of the scope of this validation and requires a separate FIPS 140-2 validation.

[72] IPMI – Intelligent Platform Management Interface

©2024 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

3.3 Module's Mode of Operation

On the first power-up (i.e. out of the box), the module automatically runs in default configuration. Configuration is required only to turn on the FIPS mode. Once the module is provisioned into FIPS mode during initialization, the module will operate and remain in FIPS-Approved mode of operation unless the module enters an error state and performs a factory reset (i.e. default configuration).

The module persists the configuration during reboot and power cycle, which includes FIPS mode configuration. An authorized operator can access the module via the WebUI or the CLI to determine the operational mode of the module. Detailed steps and procedures required to determine whether the module is operating in FIPS-Approved mode can be found in the "Enabling FIPS Mode" section of the *iLO User's Guide*, available at: https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=a00105236en_us.

3.4 Non-FIPS-Approved Mode

When initialized and configured according to the Crypto-Officer guidance in this Security Policy, the module does not support a non-FIPS-Approved mode of operation.

©2024 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

4. Acronyms

Table 10 provides definitions for the acronyms used in this document.

Table 10 – Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
ASIC	Application Specific Integrated Circuit
ASM	Advanced Server Management
CAC	Common Access Card
CAN	Controller Area Network
CBC	Cipher Block Chaining
CCCS	Canadian Centre for Cyber Security
CIF	Common Interface Format
CKG	Cryptographic Key Generation
CLI	Command Line Interface
CMVP	Cryptographic Module Validation Program
CNSA	Commercial National Security Algorithm
CO	Crypto-Officer
CRNGT	Continuous Random Number Generator Test
CSP	Critical Security Parameter
CSR	Certificate Signing Request
CTR	Counter
CVL	Component Validation List
DDR3	Double Data Rate v3
DES	Data Encryption Standard
DH	Diffie Hellman
DP	Display Port
DRBG	Deterministic Random Bit Generator
DSA	Digital Signature Algorithm
DVI	Digital Visual Interface
EC	Elliptical Curve
ECB	Electronic Codebook
ECC	Elliptic Curve Cryptography

©2024 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Acronym	Definition
ECDSA	Elliptical Curve Digital Signature Algorithm
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
ESKM	Enterprise Secure Key Manager
eSPI	Enhanced Serial Peripheral Interface
FIPS	Federal Information Processing Standard
GCM	Galois Counter Mode
GMII	Gigabit Media Independent Interface
GPC	General Purpose Computer
GPIO	General Purpose Input Output
HMAC	(Keyed-) Hash Message Authentication Code
HP	Hewlett Packard
HTTPS	Hypertext Transfer Protocol Secure
I2C	Inter-Integrated Circuit
iLO	Integrated Lights-Out
IPMI	Intelligent Platform Management Interface
IV	Initialization Vector
KAS	Key Agreement Scheme
KAT	Known Answer Test
KBKDF	Key Based Key Derivation Function
KDF	Key Derivation Function
KVM	Keyboard, Video, Mouse
MB	Megabyte
MHz	Megahertz
MII	Media Independent Interface
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
OS	Operating System
PCIe	Peripheral Component Interconnect Express
PIV	Personal Identification Verification
PKI	Public Key Infrastructure
POST	Power On Self Test
RAM	Random Access Memory

©2024 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Acronym	Definition
RBSU	ROM-Based Set-up Utility
REST	Representational State Transfer
RMII	Reduced Media Independent Interface
RNG	Random Number Generator
ROM	Read-Only Memory
RSA	Rivest Shamir and Adleman
SDRAM	Synchronous Dynamic Random Access Memory
SHA	Secure Hash Algorithm
SMBus	System Management Bus
SNMP	Simple Network Management Protocol
SP	Special Publication
SPI	Serial Peripheral Interface
SSC	Shared Secret Computation
SSH	Secure Shell
SSO	Single Sign On
TDES	Triple Data Encryption Standard
TLS	Transport Layer Security
UART	Universal Asynchronous Receiver/Transmitter
US	United States
USB	Universal Serial Bus
VGA	Video Graphics Array
WebUI	Web User Interface
XML	Extensible Markup Language

©2024 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.