Hewlett Packard Enterprise Development LP

iLO 5 & iLO 6 Cryptographic Module

FIPS 140-3 Non-Proprietary Security Policy

Prepared for:

Hewlett Packard Enterprise Development LP

11445 Compaq Center Dr. W.

Houston, TX 77070
United States of America

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

Prepared by:

Acumen Security, LLC.

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

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

©2025 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Table of Contents

1 General 6
1.1 Overview 6
1.2 Security Levels 7
1.3 Additional Information 7
2 Cryptographic Module Specification 8
2.1 Description 8
2.2 Tested and Vendor Affirmed Module Version and Identification 11
2.3 Excluded Components 12
2.4 Modes of Operation 13
2.5 Algorithms 13
2.6 Security Function Implementations 20
2.7 Algorithm Specific Information 22
2.8 RBG and Entropy 23
2.9 Key Generation 24
2.10 Key Establishment 24
2.11 Industry Protocols 24
3 Cryptographic Module Interfaces 24
3.1 Ports and Interfaces 24
4 Roles, Services, and Authentication 26
4.1 Authentication Methods 26
4.2 Roles 27
4.3 Approved Services 28
4.4 Non-Approved Services 35
5 Software/Firmware Security 35
5.1 Integrity Techniques 35
5.2 Initiate on Demand 35
6 Operational Environment 35
6.1 Operational Environment Type and Requirements 35
7 Physical Security 36
8 Non-Invasive Security 36
8.1 Mitigation Techniques 36
9 Sensitive Security Parameters Management 36

©2025 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

9.1 Storage Areas 36
9.2 SSP Input-Output Methods 36
9.3 SSP Zeroization Methods 37
9.4 SSPs 37
9.5 Transitions 45
10 Self-Tests 45
10.1 Pre-Operational Self-Tests 45
10.2 Conditional Self-Tests 46
10.3 Periodic Self-Test Information 52
10.4 Error States 54
11 Life-Cycle Assurance 55
11.1 Installation, Initialization, and Startup Procedures 55
11.2 Administrator Guidance 56
11.3 Non-Administrator Guidance 56
11.4 Design and Rules 56
11.5 Maintenance Requirements 57
11.6 End of Life 57
12 Mitigation of Other Attacks 57
12.1 Attack List 57

©2025 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

List of Tables

Table 1: Security Levels 7
Table 2: Tested Module Identification – Hardware 12
Table 3: Modes List and Description 13
Table 4: Approved Algorithms 19
Table 5: Vendor-Affirmed Algorithms 19
Table 6: Security Function Implementations 22
Table 7: Entropy Certificates 23
Table 8: Entropy Sources 23
Table 9: Ports and Interfaces 25
Table 10: Authentication Methods 27
Table 11: Roles 27
Table 12: Approved Services 35
Table 13: Storage Areas 36
Table 14: SSP Input-Output Methods 37
Table 15: SSP Zeroization Methods 37
Table 16: SSP Table 1 42
Table 17: SSP Table 2 45
Table 18: Pre-Operational Self-Tests 45
Table 19: Conditional Self-Tests 52
Table 20: Pre-Operational Periodic Information 52
Table 21: Conditional Periodic Information 54
Table 22: Error States 54

List of Figures

Figure 1 - HPE iLO 6 (Example Management Screen) 7
Figure 2 - iLO 5 ASIC 9
Figure 3 - iLO 6 ASIC 9
Figure 4 - iLO 5 Block Diagram 10
Figure 5 - iLO 6 Block Diagram 11

Purpose

This is a non-proprietary Cryptographic Module Security Policy for the iLO 5 & iLO 6 Cryptographic Module from Hewlett Packard Enterprise Development LP (HPE). This Security Policy describes how the iLO 5 & iLO 6 Cryptographic Module meets the security requirements of Federal Information Processing Standards (FIPS) Publication 140-3, which details the U.S.[1] government requirements for cryptographic modules. More information about the FIPS 140-3 standard and validation program is available on the National Institute of Standards and Technology (NIST) 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 Approved mode of operation.

[1] U.S. – United States

©2025 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

This security policy was prepared as part of the Level 1 FIPS 140-3 validation of the module. The iLO 5 & iLO 6 Cryptographic Module is referred to in this document as iLO, crypto module, or the module.

References

This document deals only with operations and capabilities of the module in the technical terms of a FIPS 140-3 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.

©2025 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

1 General

1.1 Overview

HPE's Integrated Lights-Out (iLO) is a proprietary embedded server management technology that provides out- of-band management functionality. HPE's fifth and sixth generation of iLO (iLO 5 & iLO 6) is the foundation of HPE's Gen10 Plus and Gen11 series enterprise server consisting of HPE ProLiant servers, HPE Edgeline, HPE Apollo and HPE Synergy systems. The HPE iLO 5 built into HPE ProLiant Gen10 Plus and HPE iLO 6 built into HPE ProLiant Gen11 servers is an autonomous, secure management component embedded directly on the server motherboard. iLO 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, regardless of the state of the host server. The Embedded Remote Support (ERS) options allow Gen10 Plus and Gen11 servers to use their Insight Remote Support (IRS) server's registration from iLO, 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 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.

iLO 5 & iLO6 is supported on all HPE Gen10 Plus and Gen11 servers with iLO.

HPE enterprise 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. It also works with the server to enable remote network booting through a variety of methods.

The iLO architecture ensures the availability of the majority of iLO 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 provides Microsoft device driver support, improved .NET framework support, and HPE SSO[3] support.

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 HPE Systems Insight Manager, Insight Control, Insight Dynamics, HPE OneView, iLO Amplifier Pack & HPE Cloud .

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.

[2] SNMP – Simple Network Management Protocol

[3] SSO – Single Sign-On

©2025 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

1.2 Security Levels

Section	Title	Security Level
1	General	1
2	Cryptographic module specification	1
3	Cryptographic module interfaces	1
4	Roles, services, and authentication	3
5	Software/Firmware security	1
6	Operational environment	1
7	Physical security	1
8	Non-invasive security	N/A
9	Sensitive security parameter management	1
10	Self-tests	1
11	Life-cycle assurance	1
12	Mitigation of other attacks	N/A
	Overall Level	1

Table 1: Security Levels

1.3 Additional Information

Figure 1 below shows a screenshot of the iLO 6 management interface.

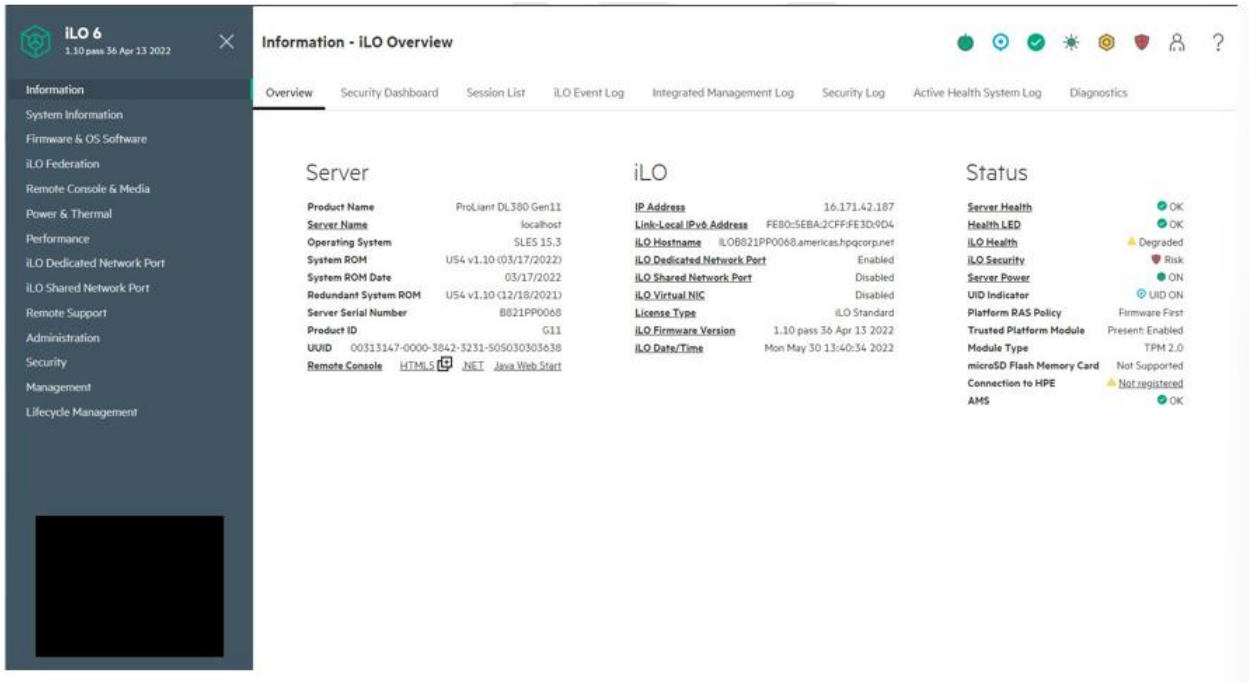


Figure 1 - HPE iLO 6 (Example Management Screen)

©2025 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Table 1 – iLO Features

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

2 Cryptographic Module Specification

2.1 Description

Purpose and Use:

iLO is deployed in the form of an ASIC[4], a system-on-a-chip with an independent Cortex A9 processor running an embedded real-time operating system. iLO 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.

The HPE iLO Cryptographic Module includes the iLO ASIC and its associated memory components incorporated directly onto the motherboards of HPE servers. The module also includes the iLO 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 RAM5 chips lead directly to the iLO 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 Figures 4 & Figure 5 below.

The iLO is a hardware module with a multiple-chip embedded embodiment. The overall security level of the module is 1.

Module Type: Hardware

Module Embodiment: Multi-Chip Embedded

Module Characteristics :

Cryptographic Boundary:

The cryptographic boundary of the module surrounds the iLO ASIC, Flash memory, battery-backed NVRAM[6], and DDR4[7] SDRAM[8] (highlighted in the red) as seen in Figures 3 and 4. (see Table "Tested Module Identification – Hardware" for part number of these components).

[4] ASIC – Application-Specific Integrated Circuit

[5] RAM – Random Access Memory

[6] NVRAM – Non-Volatile Random Access Memory

[7] DDR4 – Double Data Rate v4

[8] SDRAM – Synchronous Dynamic Random Access Memory

©2025 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

HPE affirms that the GXP2 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. Pairing happens in the factory between iLO and secure element.



Figure 2 - iLO 5 ASIC



Figure 3 - iLO 6 ASIC

©2025 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

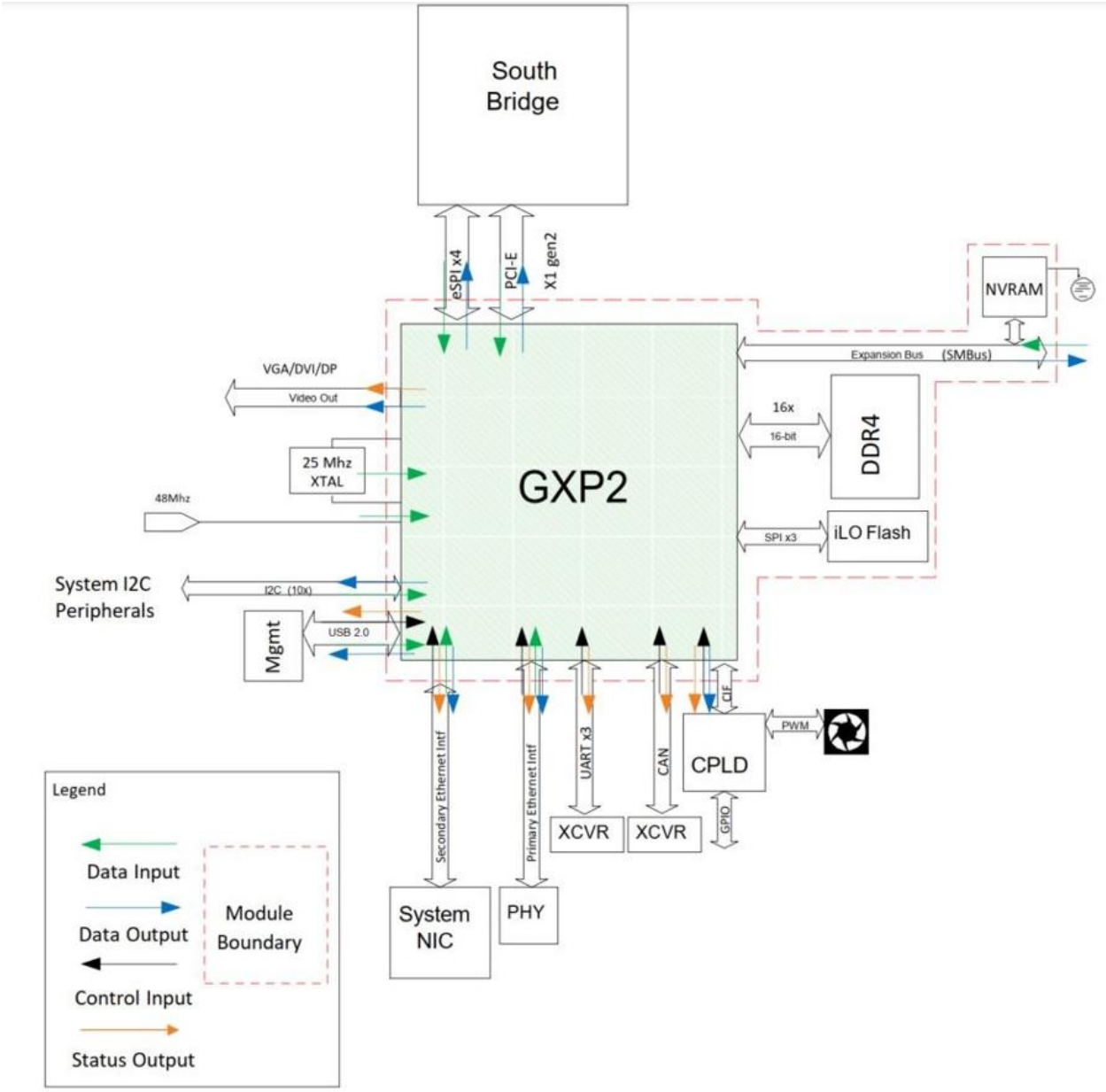


Figure 4 - iLO 5 Block Diagram

©2025 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

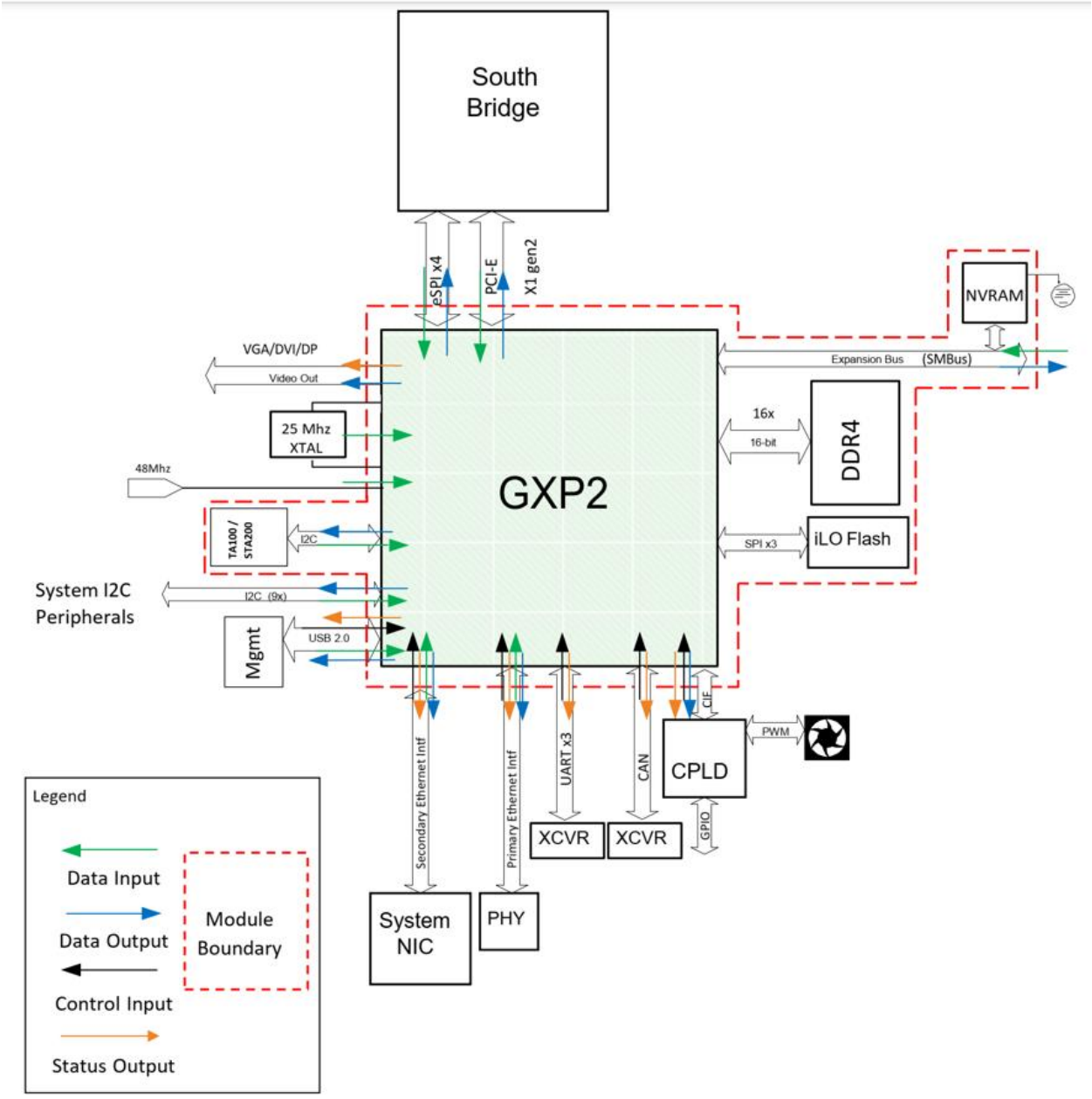


Figure 5 - iLO 6 Block Diagram

2.2 Tested and Vendor Affirmed Module Version and Identification

Tested Module Identification – Hardware:

©2025 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
iLO5 Part Number: P00197-001	P00197-001	3.05a	Cortex A9	The part number can also be labelled as P00197-285; the first section/base number (00197) is what denotes the actual physical part, die and packaging and the last 3 digits only represent the programming of the die. The cryptographic implementation is exactly the same across all ASICs with the specific base number.
iLO6 Part Number: P00197-285	P00197-285	1.60a	Cortex A9	The part number can also be labelled as P00197-265; the first section/base number (00197) is what denotes the actual physical part, die and packaging and the last 3 digits only represent the programming of the die. The cryptographic implementation is exactly the same across all ASICs with the specific base number.

Table 2: Tested Module Identification – Hardware

Tested Module Identification – Software, Firmware, Hybrid (Executable Code Sets):

N/A for this module.

Tested Module Identification – Hybrid Disjoint Hardware:

N/A for this module.

Tested Operational Environments - Software, Firmware, Hybrid:

N/A for this module.

Vendor-Affirmed Operational Environments - Software, Firmware, Hybrid:

N/A for this module.

2.3 Excluded Components

Crypto co-processor TA100 is excluded from the scope of validation, and it is only used for storage purpose and no cryptographic operations are performed.

©2025 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

2.4 Modes of Operation

Modes List and Description:

Mode Name	Description	Types of Services	Status Indicator
Approved mode	On the first power-up, the module is not configured in its Approved mode. During initial configuration and setup, the module is explicitly set to operate in the Approved mode of operation. An authorized operator can access the module via the WebUI or the CLI to determine the operational mode of the module.	Approved	Successful initialization of the module, denoted by the module name (iLO 5, iLO 6) displayed in the web interface.

Table 3: Modes List and Description

On the first power-up, the module is not configured in its Approved mode. During initial configuration and setup, the module is explicitly set to operate in the Approved mode of operation. An authorized operator can access the module via the WebUI or the CLI to determine the operational mode of the module. Detailed steps and procedure required to determine whether the module is operating in Approved mode can be found in the “Enabling FIPS Mode” section of the *iLO User’s Guide*, which is available at https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=a00105236en_us.

Mode Change Instructions and Status:

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

Degraded Mode Description:

The module does not support degraded mode of operation.

2.5 Algorithms

Approved Algorithms:

Algorithm	CAVP Cert	Properties	Reference
AES-CBC	A3430	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CBC	A6621	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CBC	A6622	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A

©2025 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Algorithm	CAVP Cert	Properties	Reference
AES-CTR	A6621	Direction - Decrypt, Encrypt Key Length - 128, 192, 256 Payload Length - Payload Length: 128 Incremental Counter - Yes Counter Tests Performed - Yes	SP 800-38A
AES-CTR	A6622	Direction - Decrypt, Encrypt Key Length - 128, 192, 256 Payload Length - Payload Length: 128 Incremental Counter - Yes Counter Tests Performed - Yes	SP 800-38A
AES-GCM	A3430	Direction - Decrypt, Encrypt IV Generation - External IV Generation Mode - 8.2.1 Key Length - 128, 192, 256 Tag Length - 104, 112, 120, 128, 32, 64, 96 IV Length - IV Length: 96 Payload Length - Payload Length: 504, 512, 1016, 1024 AAD Length - AAD Length: 0, 504, 512, 1016, 1024	SP 800-38D
AES-GCM	A6621	Direction - Decrypt, Encrypt IV Generation - Internal IV Generation Mode - 8.2.1 Key Length - 128, 192, 256 Tag Length - 104, 112, 120, 128, 32, 64, 96 IV Length - IV Length: 96 Payload Length - Payload Length: 504, 512, 1016, 1024 AAD Length - AAD Length: 0, 504, 512, 1016, 1024	SP 800-38D
AES-GCM	A6622	Direction - Decrypt, Encrypt IV Generation - Internal IV Generation Mode - 8.2.1 Key Length - 128, 192, 256 Tag Length - 104, 112, 120, 128, 32, 64, 96 IV Length - IV Length: 96 Payload Length - Payload Length: 504, 512, 1016, 1024 AAD Length - AAD Length: 0, 504, 512, 1016, 1024	SP 800-38D
Counter DRBG	A6621	Prediction Resistance - No, Yes Supports Reseed - No Mode - AES-256 Derivation Function Enabled - Yes Additional Input - Additional Input: 0-256 Increment 8	SP 800-90A Rev. 1

©2025 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Algorithm	CAVP Cert	Properties	Reference
		Entropy Input - Entropy Input: 256 Nonce - Nonce: 128 Personalization String Length - Personalization String Length: 0-256 Increment 8 Returned Bits - 512	
Counter DRBG	A6622	Prediction Resistance - No, Yes Supports Reseed - No Mode - AES-256 Derivation Function Enabled - Yes Additional Input - Additional Input: 0-256 Increment 8 Entropy Input - Entropy Input: 256 Nonce - Nonce: 128 Personalization String Length - Personalization String Length: 0-256 Increment 8 Returned Bits - 512	SP 800-90A Rev. 1
ECDSA KeyGen (FIPS186-5)	A6621	Curve - P-256, P-384 Secret Generation Mode - testing candidates	FIPS 186-5
ECDSA KeyGen (FIPS186-5)	A6622	Curve - P-256, P-384 Secret Generation Mode - testing candidates	FIPS 186-5
ECDSA KeyVer (FIPS186-5)	A6621	Curve - P-256, P-384	FIPS 186-5
ECDSA KeyVer (FIPS186-5)	A6622	Curve - P-256, P-384	FIPS 186-5
ECDSA SigGen (FIPS186-5)	A6621	Curve - P-256, P-384 Hash Algorithm - SHA2-256, SHA2-384, SHA2-512 Component - No	FIPS 186-5
ECDSA SigGen (FIPS186-5)	A6622	Curve - P-256, P-384 Hash Algorithm - SHA2-256, SHA2-384, SHA2-512 Component - No	FIPS 186-5
ECDSA SigVer (FIPS186-5)	A6621	Curve - P-256, P-384 Hash Algorithm - SHA2-256, SHA2-384, SHA2-512	FIPS 186-5
ECDSA SigVer (FIPS186-5)	A6622	Curve - P-256, P-384 Hash Algorithm - SHA2-256, SHA2-384, SHA2-512	FIPS 186-5
HMAC-SHA2-256	A6621	MAC - MAC: 32-256 Increment 8 Key Length - Key Length: 8-4096 Increment 8	FIPS 198-1
HMAC-SHA2-256	A6622	MAC - MAC: 32-256 Increment 8 Key Length - Key Length: 8-4096 Increment 8	FIPS 198-1
HMAC-SHA2-384	A6621	MAC - MAC: 32-384 Increment 8 Key Length - Key Length: 8-4096 Increment 8	FIPS 198-1

©2025 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Algorithm	CAVP Cert	Properties	Reference
HMAC-SHA2-384	A6622	MAC - MAC: 32-384 Increment 8 Key Length - Key Length: 8-4096 Increment 8	FIPS 198-1
HMAC-SHA2-512	A6621	MAC - MAC: 32-512 Increment 8 Key Length - Key Length: 8-4096 Increment 8	FIPS 198-1
HMAC-SHA2-512	A6622	MAC - MAC: 32-512 Increment 8 Key Length - Key Length: 8-4096 Increment 8	FIPS 198-1
KAS-ECC-SSC Sp800-56Ar3	A6621	Domain Parameter Generation Methods - P-256, P-384, P-521 Scheme - ephemeralUnified - KAS Role - initiator, responder	SP 800-56A Rev. 3
KAS-ECC-SSC Sp800-56Ar3	A6622	Domain Parameter Generation Methods - P-256, P-384, P-521 Scheme - ephemeralUnified - KAS Role - initiator, responder	SP 800-56A Rev. 3
KAS-FFC-SSC Sp800-56Ar3	A6621	Domain Parameter Generation Methods - ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192 Scheme - dhEphem - KAS Role - initiator, responder	SP 800-56A Rev. 3
KAS-FFC-SSC Sp800-56Ar3	A6622	Domain Parameter Generation Methods - ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192 Scheme - dhEphem - KAS Role - initiator, responder	SP 800-56A Rev. 3
KDF SP800-108	A6621	KDF Mode - Feedback MAC Mode - HMAC-SHA2-512 Supported Lengths - Supported Lengths: 8-512 Increment 8 Fixed Data Order - none Counter Length - 0 Supports Empty IV - Yes Custom Key In Length - 0	SP 800-108 Rev. 1
KDF SP800-108	A6622	KDF Mode - Feedback MAC Mode - HMAC-SHA2-512 Supported Lengths - Supported Lengths: 8-512 Increment 8 Fixed Data Order - none Counter Length - 0 Supports Empty IV - Yes Custom Key In Length - 0	SP 800-108 Rev. 1

©2025 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Algorithm	CAVP Cert	Properties	Reference
KDF SSH (CVL)	A6621	Cipher - AES-256 Hash Algorithm - SHA-1, SHA2-256, SHA2-384	SP 800-135 Rev. 1
KDF SSH (CVL)	A6622	Cipher - AES-256 Hash Algorithm - SHA-1, SHA2-256, SHA2-384	SP 800-135 Rev. 1
PBKDF	A6621	Iteration Count - Iteration Count: 1-10000 Increment 1 HMAC Algorithm - SHA-1, SHA2-256, SHA2-384, SHA2-512 Password Length - Password Length: 8-128 Increment 1 Salt Length - Salt Length: 128-4096 Increment 8 Key Data Length - Key Data Length: 112-4096 Increment 8	SP 800-132
PBKDF	A6622	Iteration Count - Iteration Count: 1-10000 Increment 1 HMAC Algorithm - SHA-1, SHA2-256, SHA2-384, SHA2-512 Password Length - Password Length: 8-128 Increment 1 Salt Length - Salt Length: 128-4096 Increment 8 Key Data Length - Key Data Length: 112-4096 Increment 8	SP 800-132
RSA KeyGen (FIPS186-5)	A6621	Key Generation Mode - probable Modulo - 2048, 3072, 4096 Primality Tests - 2powSecStr Fixed Public Exponent - 010001 Info Generated By Server - Yes Private Key Format - standard Public Exponent Mode - fixed	FIPS 186-5
RSA KeyGen (FIPS186-5)	A6622	Key Generation Mode - probable Modulo - 2048, 3072, 4096 Primality Tests - 2powSecStr Fixed Public Exponent - 010001 Info Generated By Server - Yes Private Key Format - standard Public Exponent Mode - fixed	FIPS 186-5
RSA SigGen (FIPS186-5)	A6621	Hash Pair - Hash Algorithm - SHA2-256 Modulo - 2048, 3072, 4096 Signature Type - pkcs1v1.5, pss Mask Function - mgf1	FIPS 186-5

©2025 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Algorithm	CAVP Cert	Properties	Reference
RSA SigGen (FIPS186-5)	A6622	Hash Pair - Hash Algorithm - SHA2-256 Modulo - 2048, 3072, 4096 Signature Type - pkcs1v1.5, pss Mask Function - mgf1	FIPS 186-5
RSA SigVer (FIPS186-2)	A6621	Public Exponent Mode - Random Signature Type - PKCS 1.5 Modulo - 1024, 1536, 2048, 3072, 4096 Hash Pair - Hash Algorithm - SHA-1	FIPS 186-4
RSA SigVer (FIPS186-2)	A6622	Public Exponent Mode - Random Signature Type - PKCS 1.5 Modulo - 1024, 1536, 2048, 3072, 4096 Hash Pair - Hash Algorithm - SHA-1	FIPS 186-4
RSA SigVer (FIPS186-5)	A6621	Hash Pair - Hash Algorithm - SHA2-384 Salt Length - 48 Mask Function - mgf1 Modulo - 2048, 3072, 4096 Signature Type - pkcs1v1.5, pss Public Exponent Mode - random	FIPS 186-5
RSA SigVer (FIPS186-5)	A6622	Hash Pair - Hash Algorithm - SHA2-384 Salt Length - 48 Mask Function - mgf1 Modulo - 2048, 3072, 4096 Signature Type - pkcs1v1.5, pss Public Exponent Mode - random	FIPS 186-5
Safe Primes Key Generation	A6621	Safe Prime Groups - ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192	SP 800-56A Rev. 3
Safe Primes Key Generation	A6622	Safe Prime Groups - ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192	SP 800-56A Rev. 3
Safe Primes Key Verification	A6621	Safe Prime Groups - ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192	SP 800-56A Rev. 3
Safe Primes Key Verification	A6622	Safe Prime Groups - ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192	SP 800-56A Rev. 3
SHA2-256	A6621	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-256	A6622	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-384	A3430	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-384	A6621	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4

©2025 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Algorithm	CAVP Cert	Properties	Reference
SHA2-384	A6622	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-512	A3430	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-512	A6621	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-512	A6622	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
TLS v1.2 KDF RFC7627 (CVL)	A6621	Hash Algorithm - SHA2-256, SHA2-384, SHA2-512 Key Block Length - Key Block Length: 1024	SP 800-135 Rev. 1
TLS v1.2 KDF RFC7627 (CVL)	A6622	Hash Algorithm - SHA2-256, SHA2-384, SHA2-512 Key Block Length - Key Block Length: 1024	SP 800-135 Rev. 1
TLS v1.3 KDF (CVL)	A6621	HMAC Algorithm - SHA2-256, SHA2-384 KDF Running Modes - DHE, PSK, PSK-DHE	SP 800-135 Rev. 1
TLS v1.3 KDF (CVL)	A6622	HMAC Algorithm - SHA2-256, SHA2-384 KDF Running Modes - DHE, PSK, PSK-DHE	SP 800-135 Rev. 1

Table 4: Approved Algorithms

Vendor-Affirmed Algorithms:

Name	Properties	Implementation	Reference
CKG	Key type:Symmetric and Asymmetric	N/A	SP 800-133r2 Sections 4 example 1, 5.2, 6.2.1

Table 5: Vendor-Affirmed Algorithms

Non-Approved, Allowed Algorithms:

N/A for this module.

Non-Approved, Allowed Algorithms with No Security Claimed:

N/A for this module.

Non-Approved, Not Allowed Algorithms:

N/A for this module.

©2025 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

2.6 Security Function Implementations

Name	Type	Description	Properties	Algorithms
Random Bit Generation	DRBG	Used in the process of key generation		Counter DRBG: (A6621, A6622)
CKG (Symmetric Key Generation)	CKG	Symmetric key for AES generated during key exchange for encryption/decryption		CKG : () Counter DRBG: (A6621, A6622)
SP800-108 Key Derivation	KBKDF	Used in key derivation		KDF SP800-108: (A6621, A6622)
Domain Parameter Generation	AsymKeyPair-DomPar	Domain parameter generation for DH keys		Safe Primes Key Generation: (A6621, A6622) Safe Primes Key Verification: (A6621, A6622)
Signature Generation and Verification	DigSig-SigGen DigSig-SigVer	Generate and verify signatures as part of SSH and TLS		ECDSA SigGen (FIPS186-5): (A6621, A6622) ECDSA SigVer (FIPS186-5): (A6621, A6622) RSA SigGen (FIPS186-5): (A6621, A6622) RSA SigVer (FIPS186-2): (A6621, A6622) RSA SigVer (FIPS186-5): (A6621, A6622)

©2025 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Name	Type	Description	Properties	Algorithms
Firmware Integrity	DigSig-SigVer	Used to verify integrity of the firmware image		RSA SigVer (FIPS186-5): (A6621, A6622)
Key Agreement Scheme KAS1	KAS-Full	Key agreement schemes using DH, ECDH and RSA for SSH and TLS	IG:IG D.F Scenario 2, path (2), split Key confirmation:no Key derivation:IG 2.4.B SP 800-135rev1 CVL Caveat:Key establishment methodology provides between 112 and 256 bits of security strength	KAS-ECC-SSC Sp800-56Ar3: (A6621, A6622) KAS-FFC-SSC Sp800-56Ar3: (A6621, A6622) TLS v1.2 KDF RFC7627: (A6621, A6622) TLS v1.3 KDF: (A6621, A6622) KDF SSH: (A6621, A6622)
Asymmetric Key Generation	AsymKeyPair-KeyGen AsymKeyPair-KeyVer CKG	RSA, ECDSA Key generation		RSA KeyGen (FIPS186-5): (A6621, A6622) ECDSA KeyGen (FIPS186-5): (A6621, A6622) ECDSA KeyVer (FIPS186-5): (A6621, A6622) CKG : ()
Symmetric Encryption and Decryption	BC-Auth	AES-GCM used for symmetric encryption for TLS and SSH		AES-GCM: (A6622, A6621, A3430) AES-CTR:

©2025 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Name	Type	Description	Properties	Algorithms
				(A6621, A6622) AES-CBC: (A3430, A6621, A6622)
Hashing	SHA	Hashing used for TLS and SSH		SHA2-384: (A3430, A6621, A6622) SHA2-512: (A3430, A6621, A6622) SHA2-256: (A6621, A6622)
Message Authentication	MAC	Message authentication used for TLS and SSH		HMAC-SHA2-256: (A6621, A6622) HMAC-SHA2-384: (A6621, A6622) HMAC-SHA2-512: (A6621, A6622)
PBKDF	PBKDF	Used to derive password encryption keys		PBKDF: (A6621, A6622)

Table 6: Security Function Implementations

2.7 Algorithm Specific Information

AES-GCM:

Scenario 1d: The module generates IV in the context of SSHv2 protocol. The module complies with RFC 4252, 4253 and 5647. If the invocation counter reaches 2^64-1, the next encryption is performed with the counter set to 0 or 1. In a same session, no more than 2^64-1 encryptions are performed. When a session is terminated, a new key and IV is generated. When the module's power is lost and restored, a new key is generated for AES-GCM encryption.

©2025 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Scenario 1a: The module generates IV in the context of TLS v1.2 and TLS v1.3 protocol. For TLS v1.2, the nonce_explicit management logic ensures that when the nonce_explicit part of the IV reaches the maximum value 2^64-1, the session is terminated. For TLS v1.3, when the sequence number wraps, the module terminates the connection.

RSA

Per IG C.E, the module generates RSA signature keys using an approved key generation procedure per RSA KeyGen validated for conformance to FIPS 186-5 Certs. #A6621 and #A6622. Per IG C.F, the RSA SigGen and SigVer implementations have been tested for all implemented RSA modulus lengths where CAVP testing is available.

Per IG C.M, RSA SigVer FIPS 186-2 can be used for legacy purposes.

Legacy Algorithms

RSA Signature Verification (FIPS 186-2), SHA-1 for Digital Signature Verification are CAVP tested, have their self-tests implemented and available for legacy purposes, per IG C.M.

CVL

Per IG 2.4.B, TLS v1.2 KDF RFC7627, TLS v1.3 KDF and KDF SSH (CVL) shall only be used within the context of the TLS v1.2, TLS v1.3 and SSHv2 protocols respectively.

PBKDF

The PBKDF aligns with option 1a in Section 5.4 of SP 800-132 and IG D.N. The PBKDF algorithm parameters are: Password length can be 8-128 characters long, Salt length can be 128-4096 bits long, and the number of iterations is 10000. For a 8-character password/passphrase chosen from 94 printable ASCII characters, the total combinations are: 8^94. Thus, the probability of guessing the correct password/passphrase on a random attempt is: 1/94^8. The resulting key material is only used for encrypting passwords for storage.

2.8 RBG and Entropy

Cert Number	Vendor Name
E268	Hewlett Packard Enterprise Company

Table 7: Entropy Certificates

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
RTOS Scheduler Jitter Entropy Source	Non-Physical	iLO5, iLO6	384	384	A6621, A6622

Table 8: Entropy Sources

©2025 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

The module generates 256 bits of entropy which is sufficient for the generation of the SSPs (using the approved DRBGs of the module) with the maximum target security strength (256 bits) needed.

As can be verified from the Public Use Document and the ESV Cert. #E268, the module generates a minimum of 384 bits of overall entropy per 384-bit output sample i.e. full entropy for SSP generation.

2.9 Key Generation

The module implements vendor affirmed key generation for AES, HMAC, RSA, ECDSA, DH and EC-DH. 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. Please refer to Table “Security Function Implementation” and “Vendor Affirmed Algorithms” for details on the Key Generation.

2.10 Key Establishment

Key Agreement:

The module implements approved Key Agreement Scheme that is compliant with IG D.F scenario 2 path (2), where shared secret computation (KAS-ECC-SSC, KAS-FFC-SSC) and KDF (TLS v1.2 KDF RFC7627, TLS v1.3 KDF, KDF SSH) are separately tested.

KAS-ECC-SSC provides between 128 and 256 bits of security strength. KAS-FFC-SSC provides between 112 to 200 bits of security strength.

2.11 Industry Protocols

The module supports TLSv1.2, TLSv1.3 and SSH for secure access. No parts of these protocols, other than the approved cryptographic algorithms and the KDFs have been tested by the CAVP and CMVP.

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

Physical Port	Logical Interface(s)	Data That Passes
PCIe	Data Input Data Output	Ciphertext, plaintext and keys

©2025 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Physical Port	Logical Interface(s)	Data That Passes
CAN	Control Input Status Output	Service requests, status
eSPI	Data Input Data Output	Ciphertext, plaintext and keys
USB 2.0	Data Input Data Output Control Input Status Output	Ciphertext, plaintext, keys, service requests and status
SMBus	Data Input Data Output	Ciphertext, plaintext and keys
VGA/DVI/DP	Data Output Status Output	Ciphertext, plaintext and status
GPIO	Control Input Status Output	Service requests, status
I2C	Data Input Data Output	Ciphertext, plaintext and keys
GMII /MII (Primary Ethernet)	Data Input Data Output Control Input Status Output	Ciphertext, plaintext, keys, service requests and status
RMII /MII (Secondary Ethernet)	Data Input Data Output Control Input Status Output	Ciphertext, plaintext, keys, service requests and status
UART	Control Input Status Output	Service requests, status
CIF	Data Output Control Input Status Output	Ciphertext, plaintext, keys, service requests and status
SPI	Data Input Data Output	Ciphertext, plaintext and keys
Power	Power	N/A

Table 9: Ports and Interfaces

iLO offers a WebUI[9] (accessible over TLS) and a Command Line (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

[9] WebUI – Web User Interface

©2025 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

The iLO 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 ASIC as described by logical interfaces in Table Ports and Interfaces. All these interfaces are also separated into logical interfaces defined by FIPS 140-3 in Table “Ports and Interfaces”.

4 Roles, Services, and Authentication

4.1 Authentication Methods

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
Password	Authenticate using username/password	Password based	The module enforces 8 character password at minimum chosen from the 94 human-readable ASCII characters. The probability of a successful random attempt is 1/(94^8), which is less than 1/1,000,000	The module can be configured to have no delay for first 5 failures (which is the least restrictive configuration) and have at least 2 seconds of delay for each following attempt. For first 5 attempts, there will be no delay; 6th attempt = 2 seconds delay, 7th attempt = 4 seconds delay, 8th attempt = 6 seconds delay and any further attempts will have 6 second delay i.e. 9th and following attempts all will have a 6 seconds delay. This leads to a maximum of 16 attempts in a one-minute period. The probability of successfully authenticating to the module within one minute is 16/(94^8), which is less than 1/100,000
RSA public key	Authenticate using RSA public key	Key based	The module supports RSA modulus 2048, 3072, 4096, which has a	The module supports 18 sessions per minute. Based on that, the probability of successfully

©2025 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
			minimum resistance to attack of 2^112 (2048 bits). The probability of a successful random attempt is 1/ (2^112), which is less than 1/1,000,000	authenticating to the module within one minute is 18/(2^112), which is less than 1/100,000
ECDSA public key	Authenticate using ECDSA public key	Key based	The module supports ECDSA curves P-256, P-384 which has a minimum resistance to attack of 2^128 (P-256 curve). The probability of a successful random attempt is 1/ (2^128), which is less than 1/1,000,000	The module supports 18 sessions per minute. Based on that, the probability of successfully authenticating to the module within one minute is 18/(2^128), which is less than 1/100,000

Table 10: Authentication Methods

Although the module performs authentication, the security level for Section is 1.

4.2 Roles

Name	Type	Operator Type	Authentication Methods
Crypto Officer	Identity	CO	Password RSA public key ECDSA public key
User	Identity	User	Password RSA public key ECDSA public key

Table 11: Roles

The module supports two roles (as required by FIPS 140-3) that operators may assume: a Cryptographic Officer (CO) role and a User role. Roles are assumed explicitly by using a username and password or based on public key authentication.

©2025 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

4.3 Approved Services

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Add, remove, modify or assign users and roles	Create, edit, and delete users; Define user accounts and assign permissions	N/A	Username, password	Successful creation of user and new user/permissions listed in the user settings	None	Crypto Officer
View system information	View and monitor system information, event logs, power settings, etc.	N/A	N/A	System information, boot logs displayed via WebUI and SSH	None	Crypto Officer User
View network statistics (WebUI only)	View and monitor network information and statistics	N/A	N/A	Network information and statistics displayed via WebUI	None	Crypto Officer User
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	N/A	N/A	N/A	None	Crypto Officer

©2025 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	video recording and playback					
Zeroize keys and CSPs	Zeroize all the keys and CSPs stored within iLO by taking it out of Approved mode	Successful reboot of the module by verifying Security -> Encryption -> Security Settings shows "FIPS"	N/A	N/A	None	Crypto Officer - RSA public key: Z - RSA private key: Z - Diffie-Hellman public key component: Z - Diffie-Hellman private key component: Z - EC Diffie-Hellman public key component: Z - EC Diffie-Hellman private key component: Z - TLS Pre-Master Secret: Z - TLS Master Secret: Z - TLS Session Key: Z - KBKDF Secret Value: Z - SSH Session Key: Z

©2025 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- AES GCM IV : Z - DRBG Key: Z - HMAC Key: Z - Password: Z - ECDSA public key: Z - ECDSA private key: Z
Show status	Indicate whether the module is in Approved mode (Security -> Encryption -> Security Settings should show "FIPS")	N/A	N/A	N/A	None	Crypto Officer User
Perform self-tests	Perform power-up self-tests on demand by power cycling the module	Security -> Encryption -> Security Settings should show "FIPS"	N/A	N/A	None	Crypto Officer User
Access the module via SSH/CLI	Login to the module via CLI using SSH protocol	Security -> Encryption -> Security Settings should	Password/public key	N/A	CKG (Symmetric Key Generation) Key Agreement	Crypto Officer - RSA public key: G,R - RSA private key:

©2025 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
		show "FIPS"			Scheme KAS1 Asymmetric Key Generation None Random Bit Generation Domain Parameter Generation Signature Generation and Verification Symmetric Encryption and Decryption Hashing Message Authentication	G,E - EC Diffie-Hellman public key component : G,R - EC Diffie-Hellman private key component : G,E - Diffie-Hellman public key component : G,R - Diffie-Hellman private key component : G,E - ECDSA public key: G,R - ECDSA private key: G,E - SSH Session Key: G,E - AES GCM IV : G,E - DRBG Key: G,E - DRBG V Value: G,E - DRBG seed: G,E - Entropy Input string: G,E - Shared secret: G,E - Domain parameters

©2025 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						: G,E User
Access the module via TLS/Web UI	Login to the module via WebUI using TLS protocol	Security -> Encryption -> Security Settings should show "FIPS"	Password/public key	N/A	CKG (Symmetric Key Generation) Key Agreement Scheme KAS1 Asymmetric Key Generation Random Bit Generation Domain Parameter Generation Signature Generation and Verification Symmetric Encryption and Decryption Hashing Message Authentication	Crypto Officer - RSA public key: G,R - RSA private key: G,E - Diffie-Hellman public key component: G,R - Diffie-Hellman private key component: G,E - EC Diffie-Hellman public key component: G,R - EC Diffie-Hellman private key component: G,E - TLS Pre-Master Secret: G,E - TLS Master Secret: G,E - TLS Session Key: G,E - AES GCM IV : G,E - DRBG Key: G,E - DRBG V Value: G,E - DRBG

©2025 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						seed: G,E - Entropy Input string: G,E - Shared secret: G,E - Domain parameters: G,E User
Firmware Upgrade	Load new firmware and perform an integrity test using RSA digital signature verification	Security -> Encryption -> Security Settings should show "FIPS". If verification is successful, the module performs reboot with the loaded image. If verification failed, then the module rejects the loaded firmware	N/A	N/A	Firmware Integrity	Crypto Officer - Firmware Upgrade Authentication Key (not a SSP): E
Change Password	Change the CO/user password	N/A	Password	N/A	PBKDF	Crypto Officer - Password: R - PBKDF Secret Value: G,E

©2025 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						User - Password: R - PBKDF Secret Value: G,E
Show Version	Display module version and name. Module name and firmware version can be observed by logging into the module (it is displayed in the left panel of the dashboard). Hardware version can be queried by executing the command "show system1/ asicid" on an SSH session.	N/A	N/A	Module name (iLO 5, iLO 6), FW version (v3.05a, v1.60a), HW version (iLO5: P00197-001, iLO6: P00197-285)	None	Crypto Officer User
Remote Console	Initiate a console to the host server via WebUI (encrypted session	Security -> Encryption -> Security Settings should	N/A	N/A	SP800-108 Key Derivation	Crypto Officer - KBKDF Secret Value: G,E User - KBKDF

©2025 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	using symmetric key derived from KBKDF)	show "FIPS"				Secret Value: G,E

Table 12: Approved Services

The CO role can 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 to operate in 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 Approved Services.

The User role can monitor the module configurations and the host system. Descriptions of the services available to the User role are provided in Table Approved Services.

4.4 Non-Approved Services

N/A for this module.

5 Software/Firmware Security

5.1 Integrity Techniques

The module performs RSA Signature Verification using 4096-bit key on the iLO firmware image upon every boot.

5.2 Initiate on Demand

The integrity test can be initiated on demand by power-cycling the module.

6 Operational Environment

6.1 Operational Environment Type and Requirements

Type of Operational Environment: Limited

How Requirements are Satisfied :

The module employs a limited operating environment. The module's firmware (Firmware versions: iLO5 3.05a, iLO6 1.60a) is executed by the module's Cortex A9 processor. The

©2025 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

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.

7 Physical Security

The iLO is a multiple-chip embedded cryptographic module. The module consists of production-grade components that include standard passivation techniques and meets Level 1 requirements for this section.

8 Non-Invasive Security

8.1 Mitigation Techniques

Not Applicable

9 Sensitive Security Parameters Management

9.1 Storage Areas

Storage Area Name	Description	Persistence Type
NVRAM (plaintext)	Non-Volatile Random Access Memory	Static
DDR4 RAM (plaintext)	Double Data Rate 4 Random Access Memory	Dynamic
NVRAM (stored in AES-256 CBC encrypted format)	Non-Volatile Random Access Memory	Static
Image in Flash memory	Firmware image (only for firmware authentication key storage)	Static

Table 13: Storage Areas

9.2 SSP Input-Output Methods

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
Entered by Crypto-Officer or User	Outside the module boundary	NVRAM (stored in AES-256 CBC encrypted format)	Plaintext	Manual	Electronic	
Public key output to the client	NVRAM (plaintext)	Exits the module in plaintext in	Plaintext	Manual	Electronic	

©2025 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
		the form of a certificate				

Table 14: SSP Input-Output Methods

9.3 SSP Zeroization Methods

Zeroization Method	Description	Rationale	Operator Initiation
Exiting Approved mode	Entered when an option other than "FIPS" is selected under "Security Settings" section's dropdown list	Once the module is configured not to be in Approved mode, the module resets and zeroizes all the SSPs	Operator Initiated
Session termination	TLS or SSH session termination	The ephemeral keys used for encrypting the data during TLS and SSH session	Operator Initiated
Reboot	Rebooting the module	Rebooting the module zeroizes the SSPs stored in RAM	Operator Initiated

Table 15: SSP Zeroization Methods

9.4 SSPs

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
RSA public key	Used for TLS authentication and RSA signature verification	2048, 3072, 4096 bits - 112, 128, 152 bits	Public key - PSP	Asymmetric Key Generation		Signature Generation and Verification Firmware Integrity
RSA private key	Used for TLS authentication and RSA signature generation	2048, 3072, 4096 bits - 112, 128, 152 bits	Private key - CSP	Asymmetric Key Generation		Signature Generation and Verification
Diffie-Hellman public key component	Used for key agreement during SSH sessions	2048, 3072, 4096, 6144, 8192 bits	Public key - PSP	Domain Parameter Generation		Key Agreement Scheme KAS1

©2025 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	(deriving SSH session and authentication keys)	- 112, 128, 152, 176, 200 bits				
Diffie-Hellman private key component	Used for key agreement during SSH sessions (deriving SSH session and authentication keys)	2048, 3072, 4096, 6144, 8192 bits - 112, 128, 152, 176, 200 bits	Private key - CSP	Domain Parameter Generation		Key Agreement Scheme KAS1
EC Diffie-Hellman public key component	Used for key agreement during TLS and SSH sessions (deriving TLS and SSH session and authentication keys)	NIST defined P-256 and P-384 curves - 128, 192 bits	Public key - PSP	Asymmetric Key Generation		Key Agreement Scheme KAS1
EC Diffie-Hellman private key component	Used for key agreement during TLS and SSH sessions (deriving TLS and SSH session and authentication keys)	NIST defined P-256 and P-384 curves - 128, 192 bits	Private key - CSP	Asymmetric Key Generation		Key Agreement Scheme KAS1
TLS Pre-Master Secret	Used to derive the TLS Master Secret as part of TLS Pseudo-	384 bits -	Pre-Master Secret - CSP		Key Agreement Scheme KAS1	

©2025 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	Random Function					
TLS Master Secret	Used to derive the TLS Session and Authentication Keys as part of TLS Pseudo-Random Function	384 bits -	Master Secret - CSP	TLS v1.2 KDF RFC7627 (A6621) TLS v1.3 KDF (A6621) TLS v1.2 KDF RFC7627 (A6622) TLS v1.3 KDF (A6622)	Key Agreement Scheme KAS1	
TLS Session Key	Used for encrypting or decrypting the data traffic during the TLS session	128, 256 bits - 128, 256 bits	Symmetric Key - CSP	TLS v1.2 KDF RFC7627 (A6621) TLS v1.3 KDF (A6621) TLS v1.2 KDF RFC7627 (A6622) TLS v1.3 KDF (A6622)		
KBKDF Secret Value	Used for deriving additional keys using SP 800-108 KBKDF during Remote Console sessions	128 bit - 128 bit	Symmetric Key - CSP	SP800-108 Key Derivation		
SSH Session Key	Used for encrypting or decrypting the data traffic	256 bits - 256 bits	Symmetric Key - CSP	KDF SSH (A6621) KDF SSH (A6622)		

©2025 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	during the SSH session					
AES GCM IV	Used as an IV input to AES GCM function	96 bits - 96 bits	Initialization Vector - CSP			Key Agreement Scheme KAS1
DRBG Key	DRBG internal state value, claimed per IG D.L	256 bit - 256 bit	DRBG Key - CSP			Random Bit Generation
DRBG V Value	DRBG Internal state value, claimed per IG D.L	256 bit - 256 bit	DRBG Internal state value - CSP			Random Bit Generation
DRBG seed	Random number generation, claimed per IG D.L	256-bit value - 256-bit value	DRBG Seed - CSP			Random Bit Generation
Entropy Input string	Random number generation, claimed per IG D.L	256-bit value - 256-bit value	Entropy Input - CSP			Random Bit Generation
Firmware Upgrade Authentication Key (not a SSP)	Used to verify RSA signature of items loaded through Firmware Upgrade utility	Hardcoded with RSA 4096-bit public key - 152 bits	non-SSP - Neither			Firmware Integrity
HMAC Key	Used to verify integrity and authentication of data	256, 512 bits - 128, 256 bits	Authentication Key - CSP	KDF SSH (A6621) TLS v1.2 KDF RFC7627 (A6621) TLS v1.3 KDF (A6621) KDF SSH		Key Agreement Scheme KAS1 Message Authentication

©2025 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
				(A6622) TLS v1.2 KDF RFC7627 (A6622) TLS v1.3 KDF (A6622)		
Password	Crypto-Officer and User passwords	>=64 bit - N/A	Password - CSP			
ECDSA public key	Used for SSH authentication	NIST defined P-256 and P-384 curves - 128, 192 bits	Public key - PSP	Asymmetric Key Generation		Signature Generation and Verification
ECDSA private key	Used for SSH authentication	NIST defined P-256 and P-384 curves - 128, 192 bits	Private key - CSP	Asymmetric Key Generation		Signature Generation and Verification
PBKDF Secret Value	Used to derive symmetric keys to encrypt the password	>=112 bit - >=112 bit	Symmetric key - CSP	PBKDF		
Shared secret	Derived from the key agreement for TLS/SSH	256-8192 bits - 112 to 256 bits	Shared secret - CSP		Key Agreement Scheme KAS1	
Domain parameters	Public values used to calculate shared secret	2048-8192 bits (FFC), 256-521 bits (ECC) -	Domain Parameters - PSP	Domain Parameter Generation		Key Agreement Scheme KAS1

©2025 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
		112-200 bits (FFC), 128-256 bits (ECC)				

Table 16: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
RSA public key	Public key output to the client	NVRAM (plaintext):Plaintext	Stored temporarily until zeroized as specified for this SSP	Exiting Approved mode	
RSA private key		NVRAM (plaintext):Plaintext	Stored temporarily until zeroized as specified for this SSP	Exiting Approved mode	
Diffie-Hellman public key component	Public key output to the client	DDR4 RAM (plaintext):Plaintext	Stored temporarily until zeroized as specified for this SSP	Session termination Reboot	
Diffie-Hellman private key component		DDR4 RAM (plaintext):Plaintext	Stored temporarily until zeroized as specified for this SSP	Session termination Reboot	
EC Diffie-Hellman public key component	Public key output to the client	DDR4 RAM (plaintext):Plaintext	Stored temporarily until zeroized as specified for this SSP	Session termination Reboot	
EC Diffie-Hellman private key component		DDR4 RAM (plaintext):Plaintext	Stored temporarily until zeroized as specified for this SSP	Session termination Reboot	
TLS Pre-Master Secret		DDR4 RAM (plaintext):Plaintext	Stored temporarily until zeroized as specified for this SSP	Exiting Approved mode Session	

©2025 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
				termination Reboot	
TLS Master Secret		DDR4 RAM (plaintext):Plaintext	Stored temporarily until zeroized as specified for this SSP	Exiting Approved mode Session termination Reboot	
TLS Session Key		DDR4 RAM (plaintext):Plaintext	Stored temporarily until zeroized as specified for this SSP	Exiting Approved mode Session termination Reboot	
KBKDF Secret Value		DDR4 RAM (plaintext):Plaintext	Stored temporarily until zeroized as specified for this SSP	Exiting Approved mode Session termination Reboot	
SSH Session Key		DDR4 RAM (plaintext):Plaintext	Stored temporarily until zeroized as specified for this SSP	Exiting Approved mode Session termination Reboot	
AES GCM IV		DDR4 RAM (plaintext):Plaintext	Stored temporarily until zeroized as specified for this SSP	Exiting Approved mode Session termination Reboot	
DRBG Key		DDR4 RAM (plaintext):Plaintext	Stored temporarily until zeroized as specified for this SSP	Reboot	
DRBG V Value		DDR4 RAM (plaintext):Plaintext	Stored temporarily until zeroized as specified for this SSP	Reboot	
DRBG seed		DDR4 RAM (plaintext):Plaintext	Stored temporarily until zeroized	Exiting Approved mode Session	

©2025 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
			as specified for this SSP	termination Reboot	
Entropy Input string		DDR4 RAM (plaintext):Plaintext	Stored temporarily until zeroized as specified for this SSP	Exiting Approved mode Session termination Reboot	
Firmware Upgrade Authentication Key (not a SSP)		NVRAM (plaintext):Plaintext	Never zeroized	N/A	
HMAC Key		DDR4 RAM (plaintext):Plaintext	Stored temporarily until zeroized as specified for this SSP	Exiting Approved mode Session termination Reboot	
Password	Entered by Crypto-Officer or User	NVRAM (stored in AES-256 CBC encrypted format):Encrypted	Stored temporarily until zeroized as specified for this SSP	Exiting Approved mode	
ECDSA public key	Public key output to the client	NVRAM (plaintext):Plaintext	Stored temporarily until zeroized as specified for this SSP	Exiting Approved mode	
ECDSA private key		NVRAM (plaintext):Plaintext	Stored temporarily until zeroized as specified for this SSP	Exiting Approved mode	
PBKDF Secret Value		DDR4 RAM (plaintext):Plaintext	Stored temporarily until zeroized as specified for this SSP	Exiting Approved mode	
Shared secret		DDR4 RAM (plaintext):Plaintext	Stored temporarily until zeroized as specified for this SSP	Exiting Approved mode	
Domain parameters		DDR4 RAM (plaintext):Plaintext	Stored temporarily until zeroized	Exiting Approved mode	

©2025 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
			as specified for this SSP		

Table 17: SSP Table 2

9.5 Transitions

Please note that the minimum key size transitions from 112 bits to 128 bits in 2030. After that, only key sizes >= 128 can be used.

10 Self-Tests

10.1 Pre-Operational Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
RSA SigVer (FIPS186-5) (A6621)	RSA Signature Verification of firmware using 4096-bit modulo	KAT	SW/FW Integrity	Pass: Successful initialization of the module and login GUI coming up; Fail: "iLO detected invalid iLO firmware" error.	iLO performs this self-test at power-up to verify the integrity of the firmware images and the correct operation of the Approved algorithms implemented in the module.
RSA SigVer (FIPS186-5) (A6622)	RSA Signature Verification of firmware using 4096-bit modulo	KAT	SW/FW Integrity	Pass: Successful initialization of the module and login GUI coming up; Fail: "iLO detected invalid iLO firmware" error.	iLO performs this self-tests at power-up to verify the integrity of the firmware images and the correct operation of the Approved algorithms implemented in the module.

Table 18: Pre-Operational Self-Tests

iLO performs the above self-tests at power-up to verify the integrity of the firmware image and the correct operation of the Approved algorithms implemented in the module.

The pre-operational self-tests can be performed at any time by power-cycling the module.

©2025 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

10.2 Conditional Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
SHA2-384 (A3430)	SHA2-384	KAT	CAST	The self-test function returns '0' on failure and '1' on success	Hash	Power-on
SHA2-512 (A3430)	SHA2-512	KAT	CAST	The self-test function returns '0' on failure and '1' on success	Hash	Power-on
AES-CBC (A3430)	128, 192 and 256 bit	KAT	CAST	The self-test function returns '0' on failure and '1' on success	Encrypt	Power-on
AES-GCM (A3430)	256 bit	KAT	CAST	The self-test function returns '0' on failure and '1' on success	Encrypt	Power-on
AES-GCM (A6621)	256 bit	KAT	CAST	The self-test function returns '0' on failure and '1' on success	Encrypt	Power-on
Counter DRBG (A6621)	128 bit	KAT	CAST	The self-test function returns '0' on failure and '1' on success	Generate, Reseed, Instantiate functions	Power-on
ECDSA KeyGen (FIPS186-5) (A6621)	P-256, P-384	PCT	PCT	The PCT function returns '0' on failure and '1' on success	Sign and verify to validate keypair	Upon ECDSA key generation
ECDSA SigGen	P-224	KAT	CAST	The self-test function	Sign	Power-on

©2025 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
(FIPS186-5) (A6621)				returns '0' on failure and '1' on success		
ECDSA SigVer (FIPS186-5) (A6621)	P-224	KAT	CAST	The self-test function returns '0' on failure and '1' on success	Verify	Power-on
HMAC-SHA-1 (A6621)	SHA-1	KAT	CAST	The self-test function returns '0' on failure and '1' on success	MAC	Power-on
KAS-ECC-SSC Sp800-56Ar3 (A6621)	P-256	KAT	CAST	The self-test function returns '0' on failure and '1' on success	SSC	Power-on
KAS-FFC-SSC Sp800-56Ar3 (A6621)	2048 bit	KAT	CAST	The self-test function returns '0' on failure and '1' on success	SSC	Power-on
KDF SP800-108 (A6621)	Counter mode HMAC-SHA2-256	KAT	CAST	The self-test function returns '0' on failure and '1' on success	KDF	Power-on
KDF SSH (A6621)	SHA-1	KAT	CAST	The self-test function returns '0' on failure and '1' on success	KDF	Power-on
RSA KeyGen (FIPS186-5) (A6621)	2048, 3072, 4096 bit	PCT	PCT	The PCT function returns '0' on failure and '1' on success	Sign and verify to validate keypair	Upon RSA key generation

©2025 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
RSA SigGen (FIPS186-5) (A6621)	2048 bit	KAT	CAST	The self-test function returns '0' on failure and '1' on success	Sign	Power-on
RSA SigVer (FIPS186-5) (A6621)	2048 bit	KAT	CAST	The self-test function returns '0' on failure and '1' on success	Verify	Power-on
SHA2-512 (A6621)	SHA2-512	KAT	CAST	The self-test function returns '0' on failure and '1' on success	Hash	Power-on
TLS v1.2 KDF RFC7627 (A6621)	SHA2-256	KAT	CAST	The self-test function returns '0' on failure and '1' on success	KDF	Power-on
TLS v1.3 KDF (A6621)	SHA2-256	KAT	CAST	The self-test function returns '0' on failure and '1' on success	KDF	Power-on
Safe Primes Key Generation (A6621)	ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192	PCT	PCT	The PCT function returns '0' on failure and '1' on success	Recalculate pubkey and compare	Upon DH key generation
RSA SigVer (FIPS186-5) (A6621)	RSA Signature Verification of firmware using 4096-bit modulo	KAT	SW/FW Load	Pass: Successful initialization of the module and login GUI coming up; Fail: "iLO detected invalid iLO	iLO performs this self-test at power-up to verify the integrity of the firmware images and the correct operation of the Approved	On firmware loading

©2025 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				firmware" error	algorithms implemented in the module	
RSA SigVer (FIPS186-5) (A6622)	RSA Signature Verification of firmware using 4096-bit modulo	KAT	SW/FW Load	Pass: Successful initialization of the module and login GUI coming up; Fail: "iLO detected invalid iLO firmware" error	iLO performs this self-test at power-up to verify the integrity of the firmware images and the correct operation of the Approved algorithms implemented in the module	On firmware loading
Safe Primes Key Generation (A6622)	ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192	PCT	PCT	The PCT function returns '0' on failure and '1' on success	Recalculate pubkey and compare	Upon DH key generation
TLS v1.3 KDF (A6622)	SHA2-256	KAT	Critical Function	The self-test function returns '0' on failure and '1' on success	KDF	Power-on
TLS v1.2 KDF RFC7627 (A6622)	SHA2-256	KAT	CAST	The self-test function returns '0' on failure and '1' on success	KDF	Power-on
SHA2-512 (A6622)	SHA2-512	KAT	CAST	The self-test function returns '0' on failure and '1' on success	Hash	Power-on
RSA SigVer (FIPS186-5) (A6622)	2048 bit	KAT	CAST	The self-test function returns '0' on failure and '1' on success	Verify	Power-on

©2025 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
RSA SigGen (FIPS186-5) (A6622)	2048 bit	KAT	CAST	The self-test function returns '0' on failure and '1' on success	Sign	Power-on
RSA KeyGen (FIPS186-5) (A6622)	2048, 3072, 4096 bit	PCT	PCT	The PCT function returns '0' on failure and '1' on success	Sign and verify to validate keypair	Upon RSA key generation
KDF SSH (A6622)	SHA-1	KAT	CAST	The self-test function returns '0' on failure and '1' on success	KDF	Power-on
KDF SP800-108 (A6622)	Counter mode HMAC-SHA2-256	KAT	CAST	The self-test function returns '0' on failure and '1' on success	KDF	Power-on
KAS-FFC-SSC Sp800-56Ar3 (A6622)	2048 bit	KAT	CAST	The self-test function returns '0' on failure and '1' on success	SSC	Power-on
KAS-ECC-SSC Sp800-56Ar3 (A6622)	P-256	KAT	CAST	The self-test function returns '0' on failure and '1' on success	SSC	Power-on
HMAC-SHA-1 (A6622)	SHA-1	KAT	CAST	The self-test function returns '0' on failure and '1' on success	MAC	Power-on
ECDSA SigVer (FIPS186-5) (A6622)	P-224	KAT	CAST	The self-test function returns '0' on failure and	Verify	Power-on

©2025 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				'1' on success		
ECDSA SigGen (FIPS186-5) (A6622)	P-224	KAT	CAST	The self-test function returns '0' on failure and '1' on success	Sign	Power-on
ECDSA KeyGen (FIPS186-5) (A6622)	P-256, P-384	PCT	PCT	The PCT function returns '0' on failure and '1' on success	Sign and verify to validate keypair	Upon ECDSA key generation
Counter DRBG (A6622)	128 bit	KAT	CAST	The self-test function returns '0' on failure and '1' on success	Generate, Reseed, Instantiate functions	Power-on
AES-GCM (A6622)	256 bit	KAT	CAST	The self-test function returns '0' on failure and '1' on success	Encrypt	Power-on
AES-GCM (A6622)	256 bit	KAT	CAST	The self-test function returns '0' on failure and '1' on success	Decrypt	Power-on
AES-CBC (A3430)	128, 192 and 256 bit	KAT	CAST	The self-test function returns '0' on failure and '1' on success	Decrypt	Power-on
AES-GCM (A3430)	256 bit	KAT	CAST	The self-test function returns '0' on failure and '1' on success	Decrypt	Power-on
AES-GCM (A6621)	256 bit	KAT	CAST	The self-test function	Decrypt	Power-on

©2025 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				returns '0' on failure and '1' on success		
PBKDF (A6621)	SHA2-256	KAT	CAST	The self-test function returns '0' on failure and '1' on success	KDF	Power-on
PBKDF (A6622)	SHA2-256	KAT	CAST	The self-test function returns '0' on failure and '1' on success	KDF	Power-on

Table 19: Conditional Self-Tests

10.3 Periodic Self-Test Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
RSA SigVer (FIPS186-5) (A6621)	KAT	SW/FW Integrity	On Demand	Performed any time by power-cycling the module.
RSA SigVer (FIPS186-5) (A6622)	KAT	SW/FW Integrity	On Demand	Performed any time by power-cycling the module.

Table 20: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
SHA2-384 (A3430)	KAT	CAST	On Demand	Power-on
SHA2-512 (A3430)	KAT	CAST	On Demand	Power-on
AES-CBC (A3430)	KAT	CAST	On Demand	Power-on
AES-GCM (A3430)	KAT	CAST	On Demand	Power-on
AES-GCM (A6621)	KAT	CAST	On Demand	Power-on
Counter DRBG (A6621)	KAT	CAST	On Demand	Power-on
ECDSA KeyGen (FIPS186-5) (A6621)	PCT	PCT	Upon ECDSA key generation	Programmatically
ECDSA SigGen (FIPS186-5) (A6621)	KAT	CAST	On Demand	Power-on
ECDSA SigVer (FIPS186-5) (A6621)	KAT	CAST	On Demand	Power-on
HMAC-SHA-1 (A6621)	KAT	CAST	On Demand	Power-on

©2025 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
KAS-ECC-SSC Sp800-56Ar3 (A6621)	KAT	CAST	On Demand	Power-on
KAS-FFC-SSC Sp800-56Ar3 (A6621)	KAT	CAST	On Demand	Power-on
KDF SP800-108 (A6621)	KAT	CAST	On Demand	Power-on
KDF SSH (A6621)	KAT	CAST	On Demand	Power-on
RSA KeyGen (FIPS186-5) (A6621)	PCT	PCT	Upon RSA key generation	Programmatically
RSA SigGen (FIPS186-5) (A6621)	KAT	CAST	On Demand	Power-on
RSA SigVer (FIPS186-5) (A6621)	KAT	CAST	On Demand	Power-on
SHA2-512 (A6621)	KAT	CAST	On Demand	Power-on
TLS v1.2 KDF RFC7627 (A6621)	KAT	CAST	On Demand	Power-on
TLS v1.3 KDF (A6621)	KAT	CAST	On Demand	Power-on
Safe Primes Key Generation (A6621)	PCT	PCT	Upon DH key generation	Programmatically
RSA SigVer (FIPS186-5) (A6621)	KAT	SW/FW Load	On firmware loading	Operator initiated
RSA SigVer (FIPS186-5) (A6622)	KAT	SW/FW Load	On firmware loading	Operator initiated
Safe Primes Key Generation (A6622)	PCT	PCT	Upon DH key generation	Programmatically
TLS v1.3 KDF (A6622)	KAT	Critical Function	On Demand	Power-on
TLS v1.2 KDF RFC7627 (A6622)	KAT	CAST	On Demand	Power-on
SHA2-512 (A6622)	KAT	CAST	On Demand	Power-on
RSA SigVer (FIPS186-5) (A6622)	KAT	CAST	On Demand	Power-on
RSA SigGen (FIPS186-5) (A6622)	KAT	CAST	On Demand	Power-on
RSA KeyGen (FIPS186-5) (A6622)	PCT	PCT	Upon RSA key generation	Programmatically
KDF SSH (A6622)	KAT	CAST	On Demand	Power-on
KDF SP800-108 (A6622)	KAT	CAST	On Demand	Power-on
KAS-FFC-SSC Sp800-56Ar3 (A6622)	KAT	CAST	On Demand	Power-on
KAS-ECC-SSC Sp800-56Ar3 (A6622)	KAT	CAST	On Demand	Power-on
HMAC-SHA-1 (A6622)	KAT	CAST	On Demand	Power-on
ECDSA SigVer (FIPS186-5) (A6622)	KAT	CAST	On Demand	Power-on

©2025 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
ECDSA SigGen (FIPS186-5) (A6622)	KAT	CAST	On Demand	Power-on
ECDSA KeyGen (FIPS186-5) (A6622)	PCT	PCT	Upon ECDSA key generation	Programmatically
Counter DRBG (A6622)	KAT	CAST	On Demand	Power-on
AES-GCM (A6622)	KAT	CAST	On Demand	Power-on
AES-GCM (A6622)	KAT	CAST	On Demand	Power-on
AES-CBC (A3430)	KAT	CAST	On Demand	Power-on
AES-GCM (A3430)	KAT	CAST	On Demand	Power-on
AES-GCM (A6621)	KAT	CAST	On Demand	Power-on
PBKDF (A6621)	KAT	CAST	On Demand	Power-on
PBKDF (A6622)	KAT	CAST	On Demand	Power-on

Table 21: Conditional Periodic Information

10.4 Error States

Name	Description	Conditions	Recovery Method	Indicator
Boot Error	On failure of firmware integrity test, the module reaches "Boot Error" state in which the module firmware does not get loaded and the module aborts.	Firmware integrity test failure	The only way to continue from this state is by rebooting the module with a valid firmware image.	The module returns "iLO detected invalid iLO firmware".
Critical Error	In case of failure of any self-test or PCT in firmware, the module reaches the "Critical Error" state and it disables all access to cryptographic functions and CSPs. All data outputs via data output interfaces are inhibited upon any self-test failure.	Self-test or PCT failure in firmware	Exiting Approved mode will zeroize all the keys and CSPs and performs a reboot to rerun the tests..	The self-test function returns '0' on failure and '1' on success.

Table 22: Error States

Upon failure of any pre-operational self-tests, conditional self-test, or critical function test, the module demonstrates the following behavior:

- On failure of firmware integrity test, the module reaches “Boot Error” state in which the module firmware does not get loaded and the module aborts. The only way to continue from this state is by power-cycling the module. If the error still exists, then the module needs to be returned to the factory.
- In case of failure of any other self-test, the module reaches the “Critical Error” state and it disables all access to cryptographic functions and CSPs. All data outputs via

©2025 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

data output interfaces are inhibited upon any self-test failure. A permanent error status will be relayed via the status output interface, which then is recorded as an entry to the module log file and relayed via the status output interfaces. The module then zeroizes all the keys and CSPs, performs a reset to factory default settings, and performs a reboot. The factory default reset changes the Approved mode flag, taking the module out of approved mode. The module will have to be reset to reconfigure the module to approved mode, using instructions specified in Section 11.1 of this Security Policy.

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

The module is delivered in an uninitialized factory state, and require first-time configuration to operate in its 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 Approved mode. In case of iLO deployed on a Synergy chassis, the locally connected Frame Link Module gains the initial access to iLO and creates an CO account for its future use. This access is inhibited once the CO completes all initialization steps. iLO contains a distinct 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 as well as the steps necessary to configure the module for Approved mode of operation.

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

The following steps outline the procedure for configuring iLO to run in Approved mode:
Locate the iLO Administrator name and password, located on the pull tab in the server's bezel.

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

©2025 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

password.

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

The module is now initialized and in Approved mode. If the steps above are not followed exactly, the module will be operational but in a non-compliant mode.

11.2 Administrator Guidance

The User does not have the ability to configure sensitive information on the module, except for 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.

The module requires 256-bits of entropy to generate a seed for the RNG. 512 bytes of entropy are stored in NVRAM and continuously replenished via the 800 MHz[10] clock.

The User Guide is supplied with the shipment of the iLO modules or may be freely obtained at the following webpage:
https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=a00105236en_us.

11.3 Non-Administrator Guidance

Not Applicable.

11.4 Design and Rules

A CO shall change the default password after first login. When a module is powered on for the first time, a CO shall configure the module for approved mode by following the steps mentioned in Section 11.1. Additionally, the following usage policies apply:

- IPMI[11] shall be disabled while the module is running in the Approved mode of operation.
- SNMP shall be disabled while the module is running in the Approved mode of operation.
- The CO shall not enter the DSA or RSA public keys manually while the module is

[10] MHz - Megahertz

[11] IPMI – Intelligent Platform Management Interface

©2025 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.

operating in the Approved mode.
- Remote administration must only be performed over the WebUI (HTTPS) and CLI (SSH) interfaces.

Once the module is provisioned into approved mode during initialization, the module will operate and remain in Approved mode of operation unless the module enters an error state and performs a factory reset. The Crypto-Officer can also exit Approved mode on demand by restoring the module to factory default.

To check the module's Approved 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.

11.5 Maintenance Requirements

Not Applicable.

11.6 End of Life

The module can be reset at any time by using the "Exiting Approved Mode" zeroization mechanism.

12 Mitigation of Other Attacks

12.1 Attack List

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

©2025 Hewlett Packard Enterprise Development LP
This document may be freely reproduced and distributed whole and intact including this copyright notice.