Broadcom Inc.
3401 Hillview Ave
Palo Alto, CA 94304, USA
Tel: 877-486-9273
www.broadcom.com

Broadcom Inc.

VMware's Linux Kernel Cryptographic Module

FIPS 140-3 Non-Proprietary Security Policy

Table of Contents

List of Tables

List of Figures

1 General

1.1 Overview

This is a non-proprietary Cryptographic Module Security Policy for the VMware's Linux Kernel Cryptographic Module 5.0.0 from Broadcom Inc. This Security Policy describes how the VMware's Linux Kernel Cryptographic Module 5.0.0 meets the security requirements of Federal Information Processing Standards (FIPS) Publication 140-3, which details the U.S. and Canadian 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) and the Canadian Centre for Cyber Security (CCCS), a branch of the Communications Security Establishment (CSE), Cryptographic Module Validation Program (CMVP) website at https://csrc.nist.gov/projects/cryptographic-module-validation-program.

This document also describes how to run the module in a secure Approved mode of operation. This policy was prepared as part of the Software Level 1 FIPS 140-3 validation of the module. The VMware's Linux Kernel Cryptographic Module 5.0.0 is also referred to in this document as the “Module.” It also provides instructions to individuals and organizations on how to deploy or operate the product in a secure approved mode.

This document has been written for the following audiences:

- The FIPS testing laboratory.
- The Cryptographic Module Validation Program (CMVP).
- Anyone wishing to deploy this Module in a FIPS compliant manner.

1.2 Security Levels

The module has been validated at the FIPS 140-3 section levels shown in the table below.

Section	Title	Security Level
1	General	1
2	Cryptographic module specification	1
3	Cryptographic module interfaces	1
4	Roles, services, and authentication	1
5	Software/Firmware security	1
6	Operational environment	1
7	Physical security	N/A
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

2 Cryptographic Module Specification

2.1 Description

Purpose and Use:

The VMware's Linux Kernel Cryptographic Module is a software cryptographic module with a multiple-chip standalone embodiment. The overall security level of the module is 1.
As a software module, the module must rely on the physical characteristics of the host system. The physical perimeter of the cryptographic module is defined by the hard enclosure around the host system on which it runs. The module supports the physical interfaces of the Dell PowerEdge R650 Server. These interfaces include the integrated circuits of the system board, processor, RAM, hard disk, device case, power supply, and fans. See Figure 1 below for a hardware block diagram of the Dell PowerEdge R650 Server.

Module Type: Software

Module Embodiment: MultiChipStand

Module Characteristics:

Cryptographic Boundary:

As a software module, the module must rely on the physical characteristics of the host system. The physical perimeter of the cryptographic module is defined by the hard enclosure around the host system on which it runs. The module supports the physical interfaces of the Dell PowerEdge R650 Server. These interfaces include the integrated circuits of the system board, processor, RAM, hard disk, device case, power supply, and fans. See Figure 1 below for a hardware block diagram of the Dell PowerEdge R650 Server.

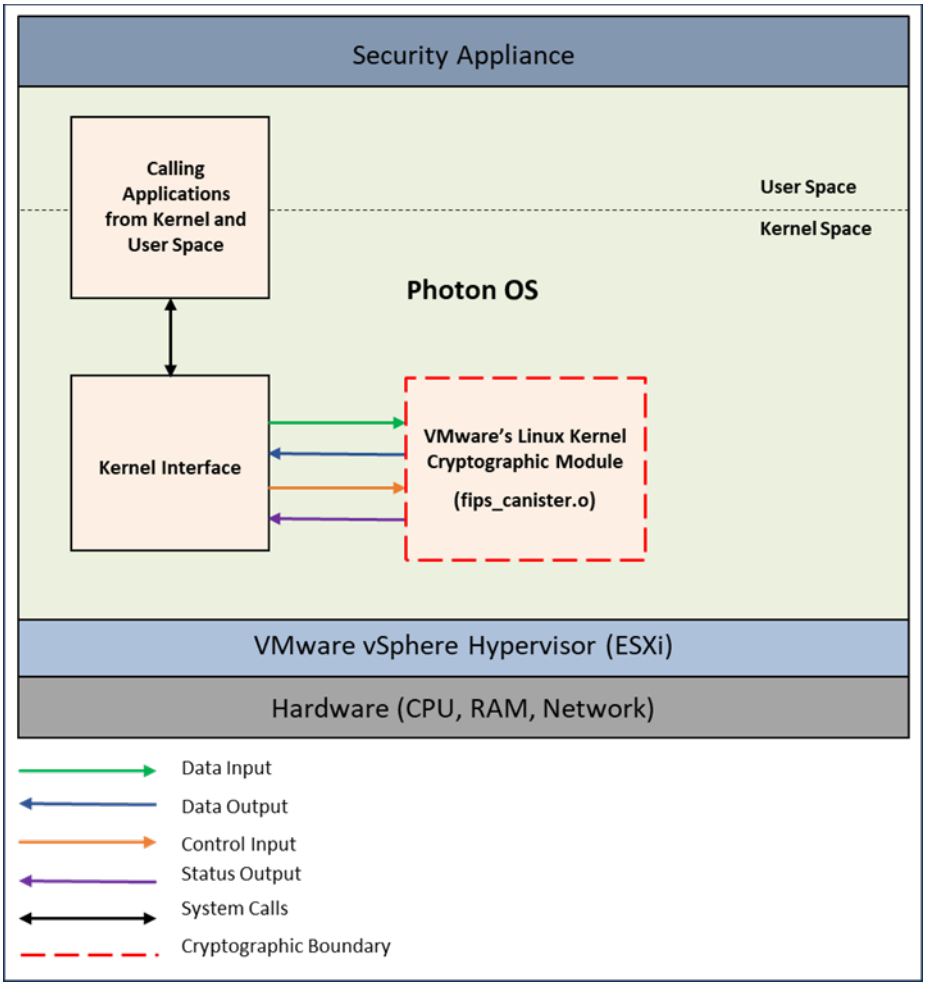

Figure 1: Block Diagram

2.2 Tested and Vendor Affirmed Module Version and Identification

Tested Module Identification – Hardware:

N/A for this module.

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

Package or File Name	Software/ Firmware Version	Features	Integrity Test
fips_canister.o	5.0.0	software cryptographic module	HMAC-SHA2-256

Table 2: Tested Module Identification – Software, Firmware, Hybrid (Executable Code Sets)

Tested Operational Environments - Software, Firmware, Hybrid:

Operating System	Hardware Platform	Processors	PAA/PAI	Hypervisor or Host OS	Version(s)
Photon OS 4.0	Dell PowerEdge R650 Server	Intel® Xeon® Gold 6330	Yes	VMware ESXi 8.0	5.0.0
Photon OS 4.0	Dell PowerEdge R650 Server	Intel® Xeon® Gold 6330	No	VMware ESXi 8.0	5.0.0
Photon OS 5.0	Dell PowerEdge R650 Server	Intel® Xeon® Gold 6330	Yes	VMware ESXi 8.0	5.0.0
Photon OS 5.0	Dell PowerEdge R650 Server	Intel® Xeon® Gold 6330	No	VMware ESXi 8.0	5.0.0

Table 3: Tested Operational Environments - Software, Firmware, Hybrid

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

Operating System	Hardware Platform
Photon OS 5.0/Photon OS 4.0 on VMware ESXi 8.0/ VMware ESXi 7.0	Dell PowerEdge R650 with an Intel® Xeon® Gold 6330 with/without PAA
Photon OS 5.0/ Photon OS 4.0 on VMware ESXi 8.0/ VMware ESXi 7.0	Dell PowerEdge R740 with an Intel® Xeon® Gold 6230R with/without PAA
Photon OS 5.0/Photon OS 4.0 on VMware ESXi 8.0/ VMware ESXi 7.0	Dell PowerEdge R640 with an Intel(R) Xeon(R) Silver 4214 with/without PAA
Photon OS 5.0/Photon OS 4.0 on VMware ESXi 8.0/ VMware ESXi 7.0	Dell PowerEdge R630 with an Intel(R) Xeon(R) CPU E5-2660 v4 with/without PAA
Photon OS 5.0/Photon OS 4.0 on VMware ESXi 8.0/ VMware ESXi 7.0	PowerEdge R6625 with an AMD EPYC 9124 with/without PAA
Photon OS 5.0/Photon OS 4.0 on VMware ESXi 8.0/ VMware ESXi 7.0	ProLiant DL385 Gen10 Plus v2 with an AMD EPYC 7343 16-Core Processor with/without PAA
Cloud computing environment executing VMware ESXi or other hypervisors	General-purpose computing platform with/without PAA

Table 4: Vendor-Affirmed Operational Environments - Software, Firmware, Hybrid

CMVP makes no statement as to the correct operation of the module or the security strengths of the generated keys when so ported if the specific operational environment is not listed on the validation certificate.

2.3 Excluded Components

There are no excluded components.

2.4 Modes of Operation

Modes List and Description:

Mode Name	Description	Type	Status Indicator
Approved	Approved Mode of Operation	Approved	API return value
Non-Approved	Non-Approved Mode of Operation	Non-Approved	Non-Approved service log message and API return value

Table 5: Modes List and Description

The module supports an FIPS 140-3 Approved mode and non-Approved mode of operation.

The module will be in Approved mode when all pre-operational self-tests have completed successfully, and only Approved services are invoked, and the success API return indicator is provided.

The module implements non-Approved Algorithms Not Allowed in the Approved Mode of Operation. When a non-Approved security function is invoked, the module will no longer be in the Approved mode of operation. A status indicator in the form of an API return code and log entry indicating the service name and "non-approved" will be provided when the module enters and exits the non-Approved mode of operation.

2.5 Algorithms

Approved Algorithms:

Algorithm	CAVP Cert	Properties	Reference
AES-CBC	A4971	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CBC-CS3	A4971	Direction - decrypt, encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CCM	A4971	Key Length - 128, 192, 256	SP 800-38C
AES-CFB128	A4971	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CMAC	A4971	Direction - Generation, Verification Key Length - 128, 192, 256	SP 800-38B
AES-CTR	A4971	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-ECB	A4971	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-GCM	A4971	Direction - Decrypt, Encrypt IV Generation - External IV Generation Mode - 8.2.2 Key Length - 128, 192, 256	SP 800-38D
AES-XTS Testing Revision 2.0	A4971	Direction - Decrypt, Encrypt Key Length - 128, 256	SP 800-38E
Counter DRBG	A4971	Prediction Resistance - No, Yes Mode - AES-128, AES-192, AES-256 Derivation Function Enabled - Yes	SP 800-90A Rev. 1
ECDSA KeyGen (FIPS186-4)	A4971	Curve - P-256, P-384 Secret Generation Mode - Extra Bits	FIPS 186-4
ECDSA KeyVer (FIPS186-4)	A4971	Curve - P-256, P-384	FIPS 186-4
ECDSA SigVer (FIPS186-4)	A4971	Curve - P-256, P-384 Hash Algorithm - SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512	FIPS 186-4

Algorithm	CAVP Cert	Properties	Reference
Hash DRBG	A4971	Prediction Resistance - No, Yes Mode - SHA-1, SHA2-256, SHA2-512	SP 800-90A Rev. 1
HMAC DRBG	A4971	Prediction Resistance - No, Yes Mode - SHA-1, SHA2-256, SHA2-512	SP 800-90A Rev. 1
HMAC-SHA-1	A4971	Key Length - Key Length: 128-2048 Increment 8	FIPS 198-1
HMAC-SHA2-224	A4971	Key Length - Key Length: 128-2048 Increment 8	FIPS 198-1
HMAC-SHA2-256	A4971	Key Length - Key Length: 128-2048 Increment 8	FIPS 198-1
HMAC-SHA2-384	A4971	Key Length - Key Length: 128-2048 Increment 8	FIPS 198-1
HMAC-SHA2-512	A4971	Key Length - Key Length: 128-2048 Increment 8	FIPS 198-1
HMAC-SHA3-224	A4971	Key Length - Key Length: 128-2048 Increment 8	FIPS 198-1
HMAC-SHA3-256	A4971	Key Length - Key Length: 128-2048 Increment 8	FIPS 198-1
HMAC-SHA3-384	A4971	Key Length - Key Length: 128-2048 Increment 8	FIPS 198-1
HMAC-SHA3-512	A4971	Key Length - Key Length: 128-2048 Increment 8	FIPS 198-1
KAS-ECC-SSC Sp800-56Ar3	A4971	Domain Parameter Generation Methods - P-256, P-384 Scheme - ephemeralUnified - KAS Role - initiator, responder	SP 800-56A Rev. 3
RSA SigGen (FIPS186-4)	A4971	Signature Type - PKCS 1.5 Modulo - 2048, 3072, 4096	FIPS 186-4
RSA SigVer (FIPS186-4)	A4971	Signature Type - PKCS 1.5 Modulo - 2048, 3072, 4096	FIPS 186-4
SHA-1	A4971	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-224	A4971	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-256	A4971	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-384	A4971	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-512	A4971	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA3-224	A4971	Message Length - Message Length: 0-65536 Increment 8	FIPS 202
SHA3-256	A4971	Message Length - Message Length: 0-65536 Increment 8	FIPS 202
SHA3-384	A4971	Message Length - Message Length: 0-65536 Increment 8	FIPS 202
SHA3-512	A4971	Message Length - Message Length: 0-65536 Increment 8	FIPS 202

Algorithm	CAVP Cert	Properties	Reference
AES-GCM	A4972	Direction - Decrypt, Encrypt IV Generation - External, Internal IV Generation Mode - 8.2.1, 8.2.2 Key Length - 128, 192, 256	SP 800-38D

Table 6: Approved Algorithms

The module implements the approved algorithms listed in the table above.

Vendor-Affirmed Algorithms:

N/A for this module.

The module does not implement any vendor-affirmed algorithms.

Non-Approved, Allowed Algorithms:

N/A for this module.

The module does not implement any non-Approved Algorithms Allowed in the Approved Mode of Operation.

Non-Approved, Allowed Algorithms with No Security Claimed:

N/A for this module.

The module does not implement any Non-Approved Allowed in the Approved Mode of Operation with No Security Claimed.

Non-Approved, Not Allowed Algorithms:

Name	Use and Function
AES CBC-MAC (SP 800-38C)	CBC-MAC as an authentication mode outside of the CCM context.
GHASH (SP 800-38D)	GHASH as a keyed hash function outside of GCM context
AES GCM	Encryption (External IV)
RSA PKCS1v1.5	Key Transport
AES using modes using RFC 3686 (CTR)	Encryption and Decryption
AES using modes using RFC 4543 (GCM) and RFC 4309 (CCM)	Authenticated Encryption and Decryption

Table 7: Non-Approved, Not Allowed Algorithms

The module does implement the non-approved algorithms listed in the table above.

2.6 Security Function Implementations

Name	Type	Description	Properties	Algorithms
Symmetric Ciphers	BC-Auth BC-UnAuth	Symmetric Encrypt/Decrypt	Strength:>= 128 bits	AES-CBC AES-CBC-CS3 AES-CCM AES-CFB128 AES-CTR AES-ECB AES-GCM AES-XTS Testing Revision 2.0 AES-GCM
Random Number Generation	DRBG	Deterministic Random Number Generation	Strength:>= 128 bits	Counter DRBG Hash DRBG HMAC DRBG
Digital Signature	DigSig-SigGen DigSig-SigVer	Generate or verify data integrity	Strength:=> 112 bits	ECDSA SigVer (FIPS186-4) RSA SigVer (FIPS186-4) RSA SigGen (FIPS186-4)
Message Authentication	BC-Auth MAC	Generate or verify data integrity	Strength:=>112	AES-CMAC HMAC-SHA-1 HMAC-SHA2-224 HMAC-SHA2-256 HMAC-SHA2-384 HMAC-SHA2-512 HMAC-SHA3-224 HMAC-SHA3-256 HMAC-SHA3-384 HMAC-SHA3-512
Key Agreement	KAS-SSC	Perform key agreement primitives on behalf of the calling process (does not establish keys into the module)	Strength:=> 112 bits	KAS-ECC-SSC Sp800-56Ar3
Asymmetric Key Generation	AsymKeyPair-KeyGen	Generate an asymmetric keypair	Strength:>= 112 bits	ECDSA KeyGen (FIPS186-4)
Message Digest	SHA	Hashing	Strength: >= 112 bits	SHA-1 SHA2-224 SHA2-256 SHA2-384 SHA2-512 SHA3-224 SHA3-256 SHA3-384 SHA3-512
Asymmetric Key Verification	AsymKeyPair-KeyVer	Verify an asymmetric keypair	Strength:>= 112 bits	ECDSA KeyVer (FIPS186-4)

Table 8: Security Function Implementations

The module implements the security functions listed in the table above.

2.7 Algorithm Specific Information

IG Compliance:

- Per IG C.C, all FIPS 202 functions are CAVP tested in all operating environments - see cert. #A4971.
- Per IG C.F, for RSA Signature and key generation, all 2048, 3072, and 4096 modulus sizes are CAVP tested in all operating environments - see cert. #A4971.
- Per IG C.H, GCM IVs Construct the IV in compliance with the provisions of a peer-to-peer industry standard protocol whose mechanism for generating the IVs for AES-GCM has been reviewed and deemed acceptable. GCM IV internally generated used by the IPsec-v3 protocol, as described in RFC 4106 following scenario 1 b. The AES GCM is generated internally using SP800-38D section 8.2.1.
- Per IG C.H scenario 1, AES GCM with internal IV generation in Approved mode is in compliance with RFC 4106 and shall only be used in conjunction with the IPsec stack of the kernel.
- Per IG C.I, AES-XTS keys are generated by the calling application. Additionally, the module implements a conditional AES-XTS duplicate key test which checks that Key_1 ≠ Key_2.
- Per IG D.R, Hash DRBG and HMAC DRBG use hash function SHA2-256 and SHA2-512 excluding SHA2-224 and SHA2-384.

2.8 RBG and Entropy

The following entropy sources are available to the module and have been tested to NIST SP800-90B. 256 bits of entropy input are provided to the module's DRBG from the CPU Jitter entropy source certified by ESV #E115.

The VMware CPU Jitter implementation generates an output that is considered to have full entropy. A request for 256 bits of entropy results in 256 bits of entropy per output sample, or full entropy.

Cert Number	Vendor Name
E115	Broadcom Inc.

Table 9: Entropy Certificates

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
VMware's Linux Kernel CPU Time Jitter RNG Entropy Source	Non-Physical	Photon OS 4.0 on VMware ESXi 8.0 with Intel® Xeon® Gold 6330 without PAA; Photon OS 5.0 on VMware ESXi 8.0 with Intel® Xeon® Gold 6330 without PAA	64 bits	0.333	A4658

Table 10: Entropy Sources

2.9 Key Generation

The module implements asymmetric key generation using ECDSA as per FIPS 186-4.

2.10 Key Establishment

The module does perform key agreement primitives on behalf of the calling process but does not establish keys into the module.

2.11 Industry Protocols

The module does not implement any industry protocols.

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

Physical Port	Logical Interface(s)	Data That Passes
Physical data input port(s) of the host platform	Data Input	Data to be encrypted, decrypted, signed, verified, or hashed. Keys to be used in cryptographic services. Random seed material for the module's DRBG. Keying material to be used as input to key establishment services
Physical data output port(s) of the host platform	Data Output	Data that has been encrypted, decrypted, or verified. Digital signatures, Hashes, Random values generated by the module's DRBG. Keys established using module's key establishment methods
Physical control input port(s) of the host platform	Control Input	API commands invoking cryptographic services. Modes, key sizes, etc. used with cryptographic services
Physical status output port(s) of the host platform	Status Output	Status Output API call return values

Table 11: Ports and Interfaces

The table above lists the module's physical ports and logical interfaces.

4 Roles, Services, and Authentication

4.1 Authentication Methods

N/A for this module.

The module does not support an authentication mechanism.

4.2 Roles

Name	Type	Operator Type	Authentication Methods
Crypto Officer	Role	Crypto Officer	None
User	Role	User	None

Table 12: Roles

There are two roles in the module that operators may assume: a Cryptographic Officer (CO) role and a User role. Roles are assumed implicitly through the execution of either a CO or User service. The module does not support an authentication mechanism. Each role and their corresponding services are detailed in the sections below.

The CO and User roles share many services, including encryption, decryption, and random number generation services. The CO performs installation and initialization, show status, self-tests on demand, and key zeroization services. Table 7 below describes the Approved CO and User roles.

4.3 Approved Services

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Installation and initialization	Installation and initialization of the module	Status output	N/A	Status	None	Crypto Officer
Show Status	Return module status	Status output	Command input	Status	None	Crypto Officer
On demand self-test	Perform pre-operational self-tests by rebooting the OS	Status output	N/A	Status	None	Crypto Officer
Show version	Return module	Status output,	Command input	Status output,	None	Crypto Officer

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	versioning information	Module version		Module version		
Key Zeroization	Zeroize and de-allocate memory containing sensitive data	N/A	N/A	Status	None	Crypto Officer - AES Key: Z - Entropy: Z - RSA Public Key: Z - RSA Private Key: Z - ECDSA Public Key: Z - ECDSA Private Key: Z - HMAC Key: Z - Hash_DRBG V value: Z - Hash_DRBG C value: Z - HMAC_DRBG V value: Z - HMAC_DRBG Key value: Z - CTR_DRBG V value: Z - CTR_DRBG Key value: Z
Symmetric Encryption	Encrypt plaintext data	API return value	API Parameters, plaintext data	Status, ciphertext data	Symmetric Ciphers	User - AES Key: W,E - AES XTS key: W,E
Symmetric Decryption	Decrypt ciphertext data	API return value	API Parameters, ciphertext data	Status, plaintext data	Symmetric Ciphers	User - AES Key: W,E - AES XTS key: W,E
Authenticated Symmetric Encryption	Encrypt plaintext using AES GCM key	API return value	API Parameters, plaintext data	Status, ciphertext data	Symmetric Ciphers	User - GCM Key: W,E - GCM IV: W,E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	with IV or CCM					- AES CCM Key: W,E
Authenticated Symmetric Decryption	Decrypt ciphertext using AES GCM key with IV or CCM	API return value	API Parameters, ciphertext data	Status, plaintext data	Symmetric Ciphers	User - GCM Key: W,E - GCM IV: W,E - AES CCM Key: W,E
Generate random number	Return random bits to the calling application	API return value	API Parameters	Status, random number	Random Number Generation	User - Entropy: W,E - DRBG Random Number: W,E - Hash_DRBG V value: G,E - Hash_DRBG C value: G,E - HMAC_DRBG V value: G,E - HMAC_DRBG Key value: G,E - CTR_DRBG V value: G,E - CTR_DRBG Key value: G,E
Generate Symmetric Digest	Generate Symmetric Digest	API return value	API Parameters	Status, Symmetric Digest	Symmetric Ciphers Message Authentication	User - AES CMAC Key: W,E
Verify Symmetric Digest	Verify Symmetric Digest	API return value	API Parameters	Status	Symmetric Ciphers Message Authentication	User - AES CMAC Key: W,E
Perform Keyed Hash Operations	Compute a message authentication code	API return value	API Parameters	Status, Message Authentication Code	Message Authentication	User - HMAC Key: W,E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Perform hash operation	Compute a message digest	API return value	API Parameters	Status, Message Digest	Message Digest	User
Generate asymmetric key pair	Generate a public/private key pair	API return value	API Parameters	Status	Asymmetric Key Generation	User - ECDSA Public Key: G,R - ECDSA Private Key: G,R
Verify ECDSA public key	Verify an ECDSA public key	API return value	API Parameters	Status	Asymmetric Key Verification	User - ECDSA Public Key: W
Generate Digital Signature	Generate Digital Signature	API return value	API Parameters	Status	Digital Signature	User - RSA Private Key: W,E
Verify digital signature	Verify digital signature	API return value	API Parameters	Status	Digital Signature	User - RSA Public Key: W,E - ECDSA Public Key: W,E
Compute Shared Secret	Compute ECDH shared secret	API return value	API Parameters	Status	Key Agreement	User - ECDH Private Component: W,E - ECDH public component: W,E

Table 13: Approved Services

The table above lists the approved services available to module operators.
Access rights are indicated using the following notation:

- G – Generate: The module generates or derives the SSP.
- R – Read: The SSP is read from the module (e.g., the SSP is output).
- W – Write: The SSP is updated, imported, or written to the module.
- E – Execute: The module uses the SSP in performing a cryptographic operation.
- Z – Zeroize: The module zeroizes the SSP.

4.4 Non-Approved Services

Name	Description	Algorithms	Role
Perform authenticated symmetric encryption/decryption	Encryption/decryption	AES CBC-MAC (SP 800-38C)	User

Name	Description	Algorithms	Role
Perform keyed hash function	Hashing	GHASH (SP 800-38D)	User
Perform authenticated symmetric encryption	Encryption with External IV	AES GCM	User
RSA Key Transport	Key padding / Key transport	RSA PKCS1v1.5	User
Perform symmetric encryption/decryption	Encryption/decryption	AES using modes using RFC 3686 (CTR)	User
Perform authenticated symmetric encryption/decryption	Authenticated encryption/decryption	AES using modes using RFC 4543 (GCM) and RFC 4309 (CCM)	User

Table 14: Non-Approved Services

The module implements the non-approved services listed in the table above.

4.5 External Software/Firmware Loaded

The module does not implement external software loading.

5 Software/Firmware Security

5.1 Integrity Techniques

The integrity of the module's cryptographic boundary is verified by a hash generated by HMAC-SHA2-256 digest. The software integrity test is performed by VMware's Linux Kernel Cryptographic Module. The module automatically invokes separate KATs for the HMAC and SHA2-256 algorithms then the module will invoke the HMAC-SHA2-256 integrity test pre-operationally during the boot sequence.

5.2 Initiate on Demand

An operator can initiate the integrity test on-demand by rebooting the OS. If an integrity test fails, the module will enter the critical error state.

6 Operational Environment

6.1 Operational Environment Type and Requirements

Type of Operational Environment: Modifiable

How Requirements are Satisfied:

The VMware's Linux Kernel Cryptographic Module 5.0.0 comprises a software cryptographic library that executes in a modifiable operational environment. The cryptographic module has control over its own SSPs. The process and memory management functionality of the host

device's OS prevents unauthorized access to plaintext, private and secret keys, intermediate key generation values and other SSPs by external processes during module execution.

The module only allows access to SSPs through its well-defined API. The operational environments provide the capability to separate individual application processes from each other by preventing uncontrolled access to CSPs and uncontrolled modifications of SSPs regardless of whether this data is in the process memory or stored on persistent storage within the operational environment. Processes that are spawned by the module are owned by the module and are not owned by external processes/operators.

7 Physical Security

The cryptographic module is a software module and does not include physical security mechanisms. Therefore, per ISO/IEC 19790:2021 section 7.7.1, requirements for physical security are not applicable.

8 Non-Invasive Security

This section is not applicable. There are currently no approved non-invasive mitigation metrics defined at the time of writing. (Ref: ISO/IEC 19790:2012 Annex F).

9 Sensitive Security Parameters Management

9.1 Storage Areas

Storage Area Name	Description	Persistence Type
RAM	Memory	Dynamic

Table 15: Storage Areas

All SSPs are only stored in memory.

9.2 SSP Input-Output Methods

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
External to RAM	External	RAM	Plaintext	Automated	Electronic	
RAM to External	RAM	External	Plaintext	Automated	Electronic	

Table 16: SSP Input-Output Methods

All SSPs are passed to the module via a well-defined API.

9.3 SSP Zeroization Methods

Zeroization Method	Description	Rationale	Operator Initiation
Reboot OS	Reboot Operating System	Memory is zeroized upon reboot	Operator Initiated

Table 17: SSP Zeroization Methods

There is no mechanism within the module boundary for the persistent storage of keys and CSPs. Maintenance, including protection and zeroization, of any keys and CSPs that exist outside the module's boundary are the responsibility of the end-user. For the zeroization of keys in volatile memory, module operators can reboot the OS.

9.4 SSPs

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
AES Key	AES Key	128, 192, 256-bit key - 128 to 256 bits	Symmetric Key - CSP			Symmetric Ciphers
Entropy	Externally generated entropy used to seed the DRBG	256 bits - 256 bits	Entropy - CSP			Random Number Generation
Hash_DRBG V value	Internal state for DRBG	440 bits - 256 bits	DRBG Internal State - CSP	Random Number Generation		Random Number Generation
Hash_DRBG C value	Internal state for DRBG	440 bits - 256 bits	DRBG Internal State - CSP	Random Number Generation		Random Number Generation
HMAC_DRBG V value	Internal state for DRBG	256 bits - 256 bits	DRBG Internal State - CSP	Random Number Generation		Random Number Generation
HMAC_DRBG Key value	Internal state for DRBG	256 bits - 256 bits	DRBG Internal State - CSP	Random Number Generation		Random Number Generation
CTR_DRBG V value	Internal state for DRBG	128 bits - 128 bits	DRBG Internal State - CSP	Random Number Generation		Random Number Generation
CTR_DRBG Key value	Internal state for DRBG	128, 192, 256 bits - 128 to 256 bits	DRBG Internal State - CSP	Random Number Generation		Random Number Generation
RSA Public Key	Key used for RSA	≥ 2048 bits - 112 to 150 bits	RSA Keypair - PSP	Asymmetric Key Generation		Digital Signature

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	Signature Verification					
RSA Private Key	Key used for RSA Signature Generation	≥ 2048 bits - 112 to 150 bits	RSA Keypair - CSP	Asymmetric Key Generation		Digital Signature
ECDSA Public Key	Key used for ECDSA Signature Verification	P-256, P-384 - 128 or 256 bits	ECDSA Keypair - PSP	Asymmetric Key Generation		Digital Signature
ECDSA Private Key	Key used for ECDSA Signature Generation	P-256, P-384 - 128 or 256 bits	ECDSA Keypair - CSP	Asymmetric Key Generation		Digital Signature
HMAC Key	Key used for HMAC Operations	≥ 112 bits - ≥ 112 bits	HMAC Key - CSP			Message Authentication
AES CCM Key	CCM Key	128, 192, 256 bits - 128 to 256 bits	CCM Key - CSP			Symmetric Ciphers
GCM Key	GCM Key	128, 192, 256 bits - 128 to 256 bits	GCM Key - CSP			Symmetric Ciphers
GCM IV	GCM IV	96 bits - 96 bits	GCM IV - CSP			Symmetric Ciphers
AES XTS key	AES XTS Key	128, 256-bit key - 128 or 256 bits	AES XTS Key - CSP			Symmetric Ciphers
AES CMAC Key	AES CMAC Key	128, 192, 256 bits - 128 to 256 bits	AES CMAC Key - CSP			Symmetric Ciphers
DRBG Random Number	DRBG Random Number	CTR_DRBG: AES-128, AES-192, AES-256 with DF, with, without PR / Hash_DRBG: SHA-1, SHA2-256, SHA2-512 with/without PR / HMAC_DRBG: SHA-1, SHA2-256,SHA2-512 with/without PR -	DRBG Random Number - CSP	Random Number Generation		Symmetric Ciphers Message Authentication Asymmetric Key Generation

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
ECDH Private Component	ECDH Private Component	P-256, P-384 - 128 or 256 bits	ECDH Private Component - CSP	Key Agreement		Key Agreement
ECDH public component	ECDH public component	P-256, P-384 - 128 or 256 bits	ECDH public component - PSP	Key Agreement		Key Agreement

Table 18: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
AES Key	External to RAM RAM to External	RAM:Plaintext	Until Reboot	Reboot OS	
Entropy	External to RAM RAM to External	RAM:Plaintext	Until Reboot	Reboot OS	
Hash_DRBG V value	External to RAM RAM to External	RAM:Plaintext	Until Reboot	Reboot OS	
Hash_DRBG C value	External to RAM RAM to External	RAM:Plaintext	Until Reboot	Reboot OS	
HMAC_DRBG V value	External to RAM RAM to External	RAM:Plaintext	Until Reboot	Reboot OS	
HMAC_DRBG Key value	External to RAM RAM to External	RAM:Plaintext	Until Reboot	Reboot OS	
CTR_DRBG V value	External to RAM RAM to External	RAM:Plaintext	Until Reboot	Reboot OS	
CTR_DRBG Key value	External to RAM RAM to External	RAM:Plaintext	Until Reboot	Reboot OS	
RSA Public Key	External to RAM RAM to External	RAM:Plaintext	Until Reboot	Reboot OS	
RSA Private Key	External to RAM RAM to External	RAM:Plaintext	Until Reboot	Reboot OS	
ECDSA Public Key	External to RAM RAM to External	RAM:Plaintext	Until Reboot	Reboot OS	
ECDSA Private Key	External to RAM RAM to External	RAM:Plaintext	Until Reboot	Reboot OS	
HMAC Key	External to RAM RAM to External	RAM:Plaintext	Until Reboot	Reboot OS	
AES CCM Key	External to RAM RAM to External	RAM:Plaintext	Until Reboot	Reboot OS	
GCM Key	External to RAM RAM to External	RAM:Plaintext	Until Reboot	Reboot OS	
GCM IV	External to RAM RAM to External	RAM:Plaintext	Until Reboot	Reboot OS	
AES XTS key	External to RAM RAM to External	RAM:Plaintext	Until Reboot	Reboot OS	
AES CMAC Key	External to RAM RAM to External	RAM:Plaintext	Until Reboot	Reboot OS	

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
DRBG Random Number	External to RAM RAM to External	RAM:Plaintext	Until Reboot	Reboot OS	
ECDH Private Component	External to RAM RAM to External	RAM:Plaintext	Until Reboot	Reboot OS	
ECDH public component	External to RAM RAM to External	RAM:Plaintext	Until Reboot	Reboot OS	

Table 19: SSP Table 2

The module manages the SSPs, and keys listed in the table above.

10 Self-Tests

The Module performs both pre-operational and conditional self-tests. Once invoked, the Module will not perform functions or services until the self-test(s) has been completed. The following sections list the self-tests performed by the Module, their expected error status, and any error resolutions.

10.1 Pre-Operational Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
HMAC-SHA2-256 (A4971)	HMAC-SHA2-256	Software Integrity Test	SW/FW Integrity	Status Output	

Table 20: Pre-Operational Self-Tests

If any of the pre-operational self-tests fail, the module enters the critical error state, and an error message is logged. In this state, cryptographic operations are halted, and the module inhibits all data output from the module as the API interface is disabled. In order to attempt to exit the error state, the module must be restarted by rebooting the OS. If the error persists, the module must be reinitialized.

Pre-operational self-tests are automatically performed by the module at module initialization or when the module powers on. The list of pre-operational self-tests that follows may also be run on-demand when the CO reboots the Operating System. The Module performs the required HMAC and SHS Cryptographic Algorithm Self-Tests (CASTs) that are required for the subsequent software integrity tests. During the execution of self-tests, cryptographic functions and data output from the module are inhibited. The VMware's Linux Kernel Cryptographic Module performs a software integrity check (HMAC with SHA2-256 Integrity Test) pre-operationally.

10.2 Conditional Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-CBC (A4971)	128, 192, 256-bit keys	KAT	CAST	Status Output	Encrypt/Decrypt	Module Initialization
AES-CBC-CS3 (A4971)	128, 192, 256-bit keys	KAT	CAST	Status Output	Encrypt/Decrypt	Module Initialization
AES-CCM (A4971)	128, 192, 256-bit keys	KAT	CAST	Status Output	Encrypt/Decrypt	Module Initialization
AES-CFB128 (A4971)	128, 192, 256-bit keys	KAT	CAST	Status Output	Encrypt/Decrypt	Module Initialization
AES-CTR (A4971)	128, 192, 256-bit keys	KAT	CAST	Status Output	Encrypt/Decrypt	Module Initialization
AES-ECB (A4971)	128, 192, 256-bit keys	KAT	CAST	Status Output	Encrypt/Decrypt	Module Initialization
AES-GCM (A4972)	128, 192, 256-bit keys	KAT	CAST	Status Output	Encrypt/Decrypt	Module Initialization
AES-GCM (A4971)	128, 192, 256-bit keys	KAT	CAST	Status Output	Encrypt/Decrypt	Module Initialization
AES-CMAC (A4971)	128, 192, 256-bit keys	KAT	CAST	Status Output	Encrypt/Decrypt	Module Initialization
AES-XTS Testing Revision 2.0 (A4971)	128, 256-bit keys	KAT	CAST	Status Output	Encrypt/Decrypt	Module Initialization
AES-CMAC (A4971)	128, 192, 256-bit keys	KAT	CAST	Status Output	Message Authentication	Module Initialization
Counter DRBG (A4971)	AES-128, AES-256, AES-192	KAT	CAST	Status Output	instantiate, generate, and reseed	On instantiate, generate, and reseed
ECDSA KeyGen (FIPS186-4) (A4971)	P-256, P-384	PCT	PCT	Status Output	Key Generation / Key Verification	After key pair generation
ECDSA SigVer (FIPS186-4) (A4971)	P-256, P-384	KAT	CAST	Status Output	Signature Verification	After Signature Verification
Hash DRBG (A4971)	SHA-1, SHA2-256, SHA2-512	KAT	CAST	Status Output	instantiate, generate, and reseed	On instantiate, generate, and reseed
HMAC DRBG (A4971)	SHA-1, SHA2-256, SHA2-512	KAT	CAST	Status Output	instantiate, generate, and reseed	On instantiate, generate, and reseed
HMAC	SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512 SHA3-224, SHA3-256, SHA3-384, SHA3-512	KAT	CAST	Status Output	Message Authentication	Module Initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
KAS-ECC-SSC Sp800-56Ar3 (A4971)	P-256, P-384	KAT	CAST	Status Output	Shared Secret Computation	Module Initialization
KAS-ECC-SSC Sp800-56Ar3 (A4971)	P-256, P-384	PCT	PCT	Status Output	Shared Secret Computation	After Key pair generation
RSA SigGen (FIPS186-4) (A4971)	PKCS1v1.5 Mod (2048, 3072, 4096) Hash (SHA2-224, SHA2-256, SHA2-384, SHA2-512)	KAT	CAST	Status Output	Signature Generation	Module Initialization
RSA SigVer (FIPS186-4) (A4971)	PKCS1v1.5 Mod (2048, 3072, 4096) Hash (SHA1, SHA2-224, SHA2-256, SHA2-384, SHA2-512)	KAT	CAST	Status Output	Signature Verification	Module Initialization
SHS	SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512 SHA3-224, SHA3-256, SHA3-384, SHA3-512	KAT	CAST	Status Output	Message Digest	Module Initialization
SP800-90Ar1 Continual Health Tests	Hash_DRBG, HMAC_DRBG and CTR_DRBG SP 800-90Ar1 Health Tests	DRBG health tests	CAST	Status Output	Message Digest	Continuously while the Module is loaded

Table 21: Conditional Self-Tests

Conditional self-tests are performed by the Module during operation when specific conditions occur.

The Module performs the conditional self-tests listed in the table above.

10.3 Periodic Self-Test Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
HMAC-SHA2-256 (A4971)	Software Integrity Test	SW/FW Integrity	User initiated module reboot	On demand self-test service

Table 22: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-CBC (A4971)	KAT	CAST	User initiated module reboot	On demand self-test service
AES-CBC-CS3 (A4971)	KAT	CAST	User initiated module reboot	On demand self-test service
AES-CCM (A4971)	KAT	CAST	User initiated module reboot	On demand self-test service
AES-CFB128 (A4971)	KAT	CAST	User initiated module reboot	On demand self-test service
AES-CTR (A4971)	KAT	CAST	User initiated module reboot	On demand self-test service
AES-ECB (A4971)	KAT	CAST	User initiated module reboot	On demand self-test service
AES-GCM (A4972)	KAT	CAST	User initiated module reboot	On demand self-test service
AES-GCM (A4971)	KAT	CAST	User initiated module reboot	On demand self-test service
AES-CMAC (A4971)	KAT	CAST	User initiated module reboot	On demand self-test service
AES-XTS Testing Revision 2.0 (A4971)	KAT	CAST	User initiated module reboot	On demand self-test service
AES-CMAC (A4971)	KAT	CAST	User initiated module reboot	On demand self-test service
Counter DRBG (A4971)	KAT	CAST	User initiated module reboot	On demand self-test service
ECDSA KeyGen (FIPS186-4) (A4971)	PCT	PCT	After key pair generation	After key pair generation / On demand self-test service
ECDSA SigVer (FIPS186-4) (A4971)	KAT	CAST	After Signature Verification	After Signature Verification/ On demand self-test service
Hash DRBG (A4971)	KAT	CAST	User initiated module reboot	On demand self-test service
HMAC DRBG (A4971)	KAT	CAST	User initiated module reboot	On demand self-test service
HMAC	KAT	CAST	User initiated module reboot	On demand self-test service
KAS-ECC-SSC Sp800-56Ar3 (A4971)	KAT	CAST	User initiated module reboot	On demand self-test service
KAS-ECC-SSC Sp800-56Ar3 (A4971)	PCT	PCT	After Key pair generation	After Key pair generation / On demand self-test service
RSA SigGen (FIPS186-4) (A4971)	KAT	CAST	User initiated module reboot	On demand self-test service

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
RSA SigVer (FIPS186-4) (A4971)	KAT	CAST	User initiated module reboot	On demand self-test service
SHS	KAT	CAST	User initiated module reboot	On demand self-test service
SP800-90Ar1 Continual Health Tests	DRBG health tests	CAST	Continuously while the Module is loaded	On demand self-test service

Table 23: Conditional Periodic Information

Periodic Self-Tests can be executed by rebooting the OS.

10.4 Error States

Name	Description	Conditions	Recovery Method	Indicator
Critical Error	The module's error state.	Any Self-test failure	Reboot OS	Status Return Code

Table 24: Error States

If any of the power-up self-tests fail, the module enters the critical error state, and an error message is logged. In this state, cryptographic operations are halted, and the module inhibits all data output from the module as the API interface is disabled. In order to attempt to exit the error state, the module must be restarted by rebooting OS. If the error persists, the module must be reinitialized.

10.5 Operator Initiation of Self-Tests

Operator initiated Self-Tests can be executed by rebooting the OS.

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

Prior to the secure installation of Photon OS, the CO shall prepare the virtual environment required to securely operate it. This includes installing VMware vSphere Hypervisor (ESXi) 8.0 (see vSphere Installation and Setup). Both virtual environments require the Dell PowerEdge R650 server to run the installation.
The tar archive containing VMware's Linux Kernel Cryptographic Module prior to build time, contains the HMAC-SHA2-256 digest:

- **ea4629447ae187005ca7a12a75220f283cde801c160aa6bfc74f63e9f9409119**

The CO will then install Photon OS as the guest OS in the virtual machine and verify the full canister version as “5.0.0.”

The cryptographic functionality of VMware's Linux Kernel Cryptographic Module comes installed with Photon OS and cannot be "unloaded".
To run Photon OS kernel in an Approved mode, the Crypto Officer shall perform following actions using root access on kernel command line interface:

1. Edit the "/boot/photon.cfg" kernel file and append 'fips=1' to the "photon_cmdline" line
2. Reboot the OS using the "reboot" command.
3. To check the Approved mode, run "cat /proc/sys/crypto/fips_enabled", which will show '1' when Approved mode is enabled or '0' when Approved mode is not enabled.
4. To verify that the OS is running certified version of VMware's Linux Kernel Cryptographic Module run command "dmesg | grep canister". It should print following output:
    - FIPS (fips_integrity_init): canister 5.0.0 found (based on 6.1.75-2.ph5-secure)
    - FIPS canister HMAC:
        - **ea4629447ae187005ca7a12a75220f283cde801c160aa6bfc74f63e9f9409119**
    - FIPS canister verification passed!

11.2 Administrator Guidance

Installation and operation of the VMware's Linux Kernel Cryptographic Module requires the proper installation of Photon OS. There are no additional steps that must be performed to use the module correctly.

There are no known CVEs with this module. The CO should ensure that the operating environment is patched and updated in a timely fashion to reduce exposure to security vulnerabilities.

11.3 Non-Administrator Guidance

There is no additional guidance for non-administrators.

12 Mitigation of Other Attacks

This section is not applicable. The module does not claim to mitigate any attacks beyond the FIPS 140-3 Level 1 requirements for this validation.