VMware, Inc.
3401 Hillview Ave
Palo Alto, CA 94304, USA
Tel: 877-486-9273
Email: info@vmware.com
http://www.vmware.com

VMware's Linux Cryptographic Module

Software Version: v4.0.1

FIPS 140-2 Non-Proprietary Security Policy

FIPS Security Level: 1
Document Version: 1.4

Table of Contents

List of Figures

List of Tables

1 Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the VMware's Linux Cryptographic Module from VMware, Inc. This Security Policy describes how the VMware's Linux Cryptographic Module meets the security requirements of Federal Information Processing Standards (FIPS) Publication 140-2, which details the U.S. and Canadian Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the National Institute of Standards and Technology (NIST) and the 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 FIPS Approved mode of operation. This policy was prepared as part of the Level 1 FIPS 140-2 validation of the module. The VMware's Linux Cryptographic Module is also referred to in this document as “the module”.

1.2 References

This document deals only with operations and capabilities of the module in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the module from the following sources:

- The VMware website (https://www.vmware.com/) contains information on the full line of products from VMware.
- The CMVP website (https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Validated-Modules/Search) contains options to get contact information for individuals to answer technical or sales-related questions for the module.

1.3 Document Organization

The Security Policy document is one document in a FIPS 140-2 Submission Package. In addition to this document, the Submission Package contains:

- Vendor Evidence document
- Finite State Model document
- Other supporting documentation as additional references

With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Submission Package is proprietary to VMware and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact VMware.

2 VMware’s Linux Cryptographic Module

2.1 Overview

VMware, Inc. is a global leader in virtualization and cloud infrastructure, delivering customer-proven solutions that accelerate Information Technology (IT) by reducing complexity and enabling more flexible, agile service delivery. VMware enables enterprises to adopt a cloud model that addresses their unique business challenges. VMware’s approach accelerates the transition to cloud computing while preserving existing investments and improving security and control.

Photon OS 4.0 is an open-source minimalist Linux operating system from VMware that is optimized for cloud computing platforms, VMware vSphere deployments, and applications native to the cloud.

Photon OS 4.0 is a Linux container host optimized for vSphere and cloud-computing platforms such as Amazon Elastic Compute and Google Compute Engine. As a lightweight and extensible operating system, Photon OS 4.0 works with the most common container formats, including Docker, Rocket, and Garden. Photon OS 4.0 includes a yum-compatible, package-based lifecycle management system called tdnf.

When used with development tools and environments such as VMware Fusion, VMware Workstation, and production runtime environments (vSphere, vCloud Air), Photon OS 4.0 lets you seamlessly migrate container-based applications from development to production. With a small footprint and fast boot and run times, Photon OS 4.0 is optimized for cloud computing and cloud applications.

2.2 IMPORTANT ADVISORY: NIST SP 800-131A Transitions

PLEASE BE ADVISED of the following algorithm transitions, in accordance with NIST Special Publication 800-131A.

Table 1 - NIST SP 800-131A Transitions

Transition	Description
NIST SP 800-67	After **December 31st, 2023**, non-compliant NIST SP 800-67 three-key TDEA is disallowed for encryption unless specifically allowed by other NIST guidance. Decryption using three-key TDEA is allowed for legacy use. **Please see A.13 SP 800-67rev1 Transition** for more information.

2.2.1 VMware’s Linux Cryptographic Module

The VMware's Linux Cryptographic Module is a software cryptographic module located in the kernel space of the Photon OS 4.0. The module contains a set of cryptographic functions available to perform various cryptographic operations via a well-defined Application Programming Interface (API).

The module itself is a statically linked object module (fips_canister.o), intended to be linked to a kernel at build time. The physical cryptographic boundary is considered as the general-purpose computing (GPC) platforms on which the module was tested. The logical cryptographic boundary of the module is the pre-compiled object file which provides the necessary cryptographic functions. Within the logical boundary lies the algorithmic boundary of VMware's Linux Cryptographic Module.

The module includes implementations of the following FIPS Approved security functions:

- Encryption and decryption using AES[1] and Triple-DES[2]
- Hashing functions using SHA[3]
- Message Authentication Code using HMAC[4] SHA
- Digital Signature Generation and Verification using RSA[5]
- Random Number Generator using NIST SP 800-90A DRBGs[6]
- Shared Secret Computation using NIST SP 800-56Ar3 ECDH[7]

The VMware's Linux Cryptographic Module is validated at the FIPS 140-2 Section levels shown in the Table 1 below.

Table 2 - Security Level Per FIPS 140-2 Section

Section	Section Title	Level
1	Cryptographic Module Specification	1
2	Cryptographic Module Ports and Interfaces	1
3	Roles, Services, and Authentication	1
4	Finite State Model	1
5	Physical Security	N/A[8]
6	Operational Environment	1
7	Cryptographic Key Management	1
8	EMI/EMC[9]	1
9	Self-tests	1
10	Design Assurance	1
11	Mitigation of Other Attacks	N/A

2.3 Module Specification

The VMware's Linux Cryptographic Module is a software cryptographic module with a multiple-chip standalone embodiment. The overall security level of the module is 1. The module is composed of the following component:

- VMware's Linux Cryptographic Module – Cryptographic algorithm implementations located in the kernel of Photon OS 4.0.

In addition to its full AES software implementations, the VMware's Linux Cryptographic Module has been

[1] AES – Advanced Encryption Standard
[2] Triple-DES – Triple Data Encryption Standard
[3] SHA – Secure Hash Algorithm
[4] HMAC – (Keyed) Hash Message Authentication Code
[5] RSA - Rivest, Shamir, Adleman
[6] DRBG – Deterministic Random Number Generator
[7] ECDH – Elliptic Curve Cryptography (ECC) Diffie-Hellman
[8] N/A – Not Applicable
[9] EMI/EMC – Electromagnetic Interference/Electromagnetic Compatibility

tested and is capable of leveraging the AES-NI[10] instruction set of supported Intel processors in order to accelerate AES calculations.

Because the VMware's Linux Cryptographic Module is defined as a software cryptographic module, it possesses both a physical cryptographic boundary and a logical cryptographic boundary.

2.3.1 Physical Cryptographic Boundary

As a software module, the module must rely on the physical characteristics of the host system. The physical boundary 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 R740 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 R740 Server.

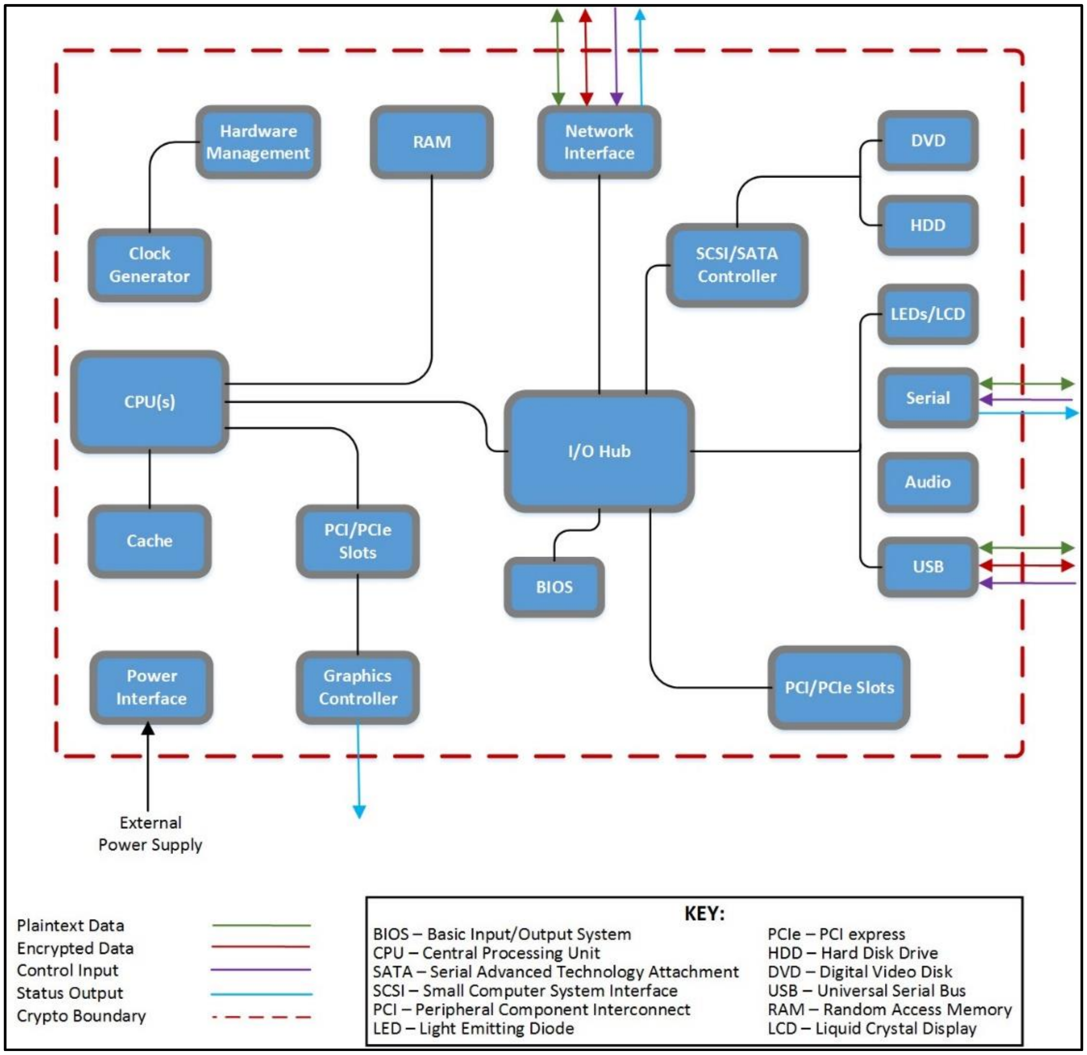

Figure 1 – Hardware Block Diagram

[10] AES-NI – Advanced Encryption Standard-New Instructions

2.3.2 Logical Cryptographic Boundary

Figure 2 depicts the logical cryptographic boundary for the single module which is the VMware's Linux Cryptographic Module. The module's logical boundary is a contiguous perimeter that surrounds all memory-mapped functionality provided by the module when loaded and stored in the host platform's memory. The colored arrows indicate the logical information flows into and out of the module. The module is shown exchanging data with the Linux kernel interface, which is also located in the kernel space of the operating system.

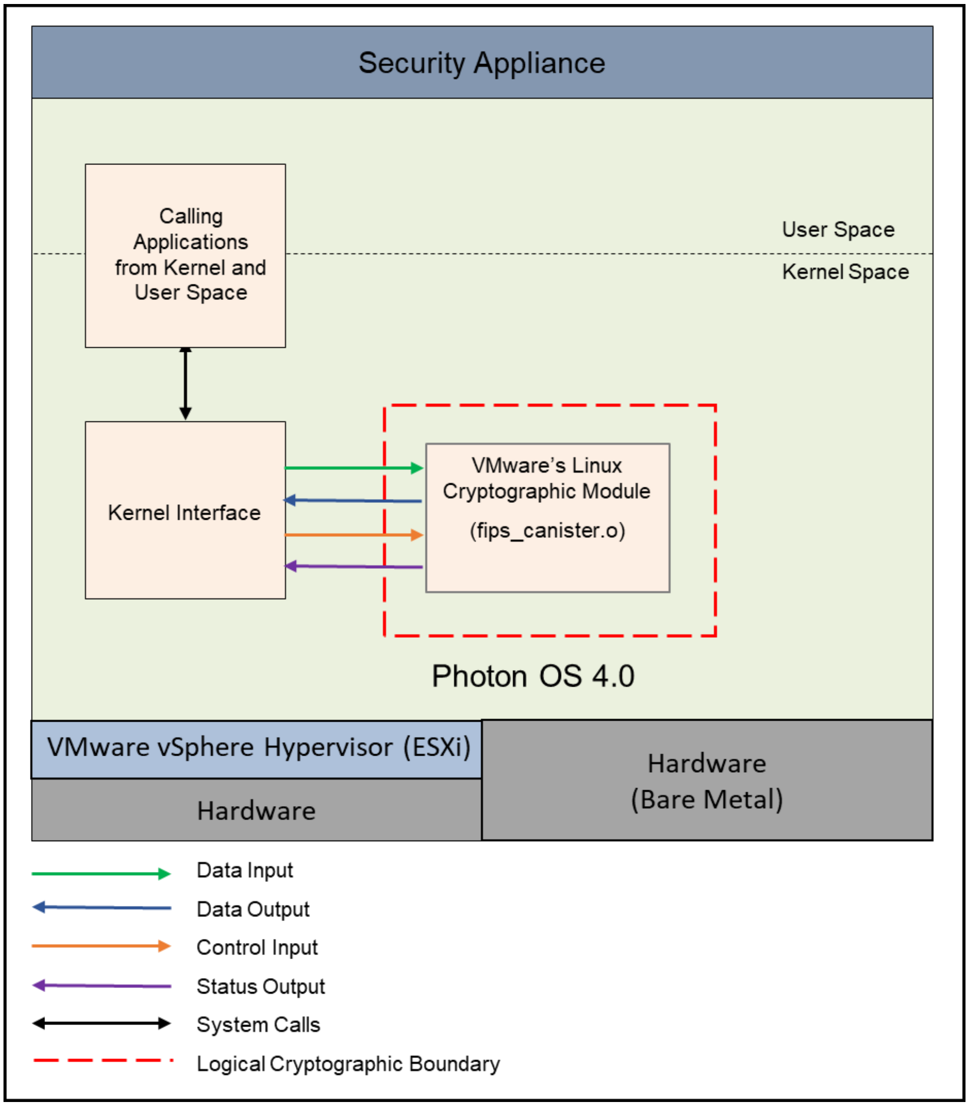

Figure 2 - Module Logical Cryptographic Boundary

2.4 Module Interfaces

The module's logical interfaces exist at a low level in the software as an API. Both the API and physical interfaces can be categorized into the following interfaces defined by FIPS 140-2:

- Data input
- Data output
- Control input
- Status output

As a software module, the module's manual controls, physical indicators, and physical ports and electrical characteristics are those of the host platform. A mapping of the FIPS 140-2 interfaces to the module logical interfaces can be found in the table below.

Table 3 - FIPS 140-2 Logical Interface Mapping

FIPS Interface	Logical Interface
Data Input	The function calls that accept input data for processing through their arguments.
Data Output	The function calls that return by means of their return codes or argument generated or processed data back to the caller.
Control Input	The function calls that are used to initialize and control the operation of the module.
Status Output	Return values for function calls; Module generated error messages.

2.5 Roles and Services

There are two roles in the module (as required by FIPS 140-2) 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. Please note that the keys and Critical Security Parameters (CSPs) listed in table below indicates the types of access required using the following notation:

- R – Read: The CSP is read.
- W – Write: The CSP is established, generated, modified, or zeroized.
- X – Execute: The CSP is used within an FIPS Approved or Allowed security function or authentication mechanism.

2.5.1 Crypto Officer and User Roles

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 4 below describes the Approved CO and User services.

Table 4 – Approved Crypto Officer and User Services

Role	Service	Description	Input	Output	CSP and Type of Access
CO, User	Encryption	Encrypt plaintext using supplied key and algorithm specification	Command and parameters	Command response/ Return code	AES Key – RX Triple-DES Key - RX
CO, User	Decryption	Decrypt ciphertext using supplied key and algorithm specification	Command and parameters	Command response/ Return code	AES Key – RX Triple-DES Key - RX
CO, User	Hash generation	Compute and return a message digest using SHA algorithm	Command and parameters	Command response/ Return code	None
CO, User	Message Authentication Code generation	Compute and return a hashed message authentication code	Command and parameters	Command response/ Return code	HMAC Key - RX
CO, User	Digital Signature	Generate and verify RSA digital signatures (keys passed in by the calling process)	Command and parameters	Command response/ Return code	RSA Private/Public Key – RX

CO, User	Random number generation	Generate random number by using the DRBGs	Command and parameters	Command response/ Return code	Hash DRBG: Entropy – R/X Hash DRBG Seed – R/W/X Hash DRBG 'V' Value – R/W/X Hash DRBG 'C' Value – R/W/X HMAC DRBG: Entropy – R/X HMAC DRBG Seed – R/W/X HMAC DRBG 'V' Value – R/W/X HMAC DRBG Key Value – R/W/X CTR DRBG: Entropy – R/X CTR DRBG Seed – R/W/X CTR DRBG 'V' Value – R/W/X CTR DRBG 'Key' Value – R/W/X
CO, User	Shared Secret Computation	Computes the shared secret on behalf of the calling application.	Command and parameters	Command response/ Return code	ECDH Private/Public Key – WX Shared Secret – WX
CO	Installation and initialization of the module	Installation and initialization of the module following the Secure Operation section of the Security Policy	Command and parameters	Command response/ Return code	None
CO	Show status	Returns the current mode of operation of the module	Command and parameters	status output	None
CO	Run Self-tests on demand	Runs Self-tests on demand during module operation	Reboot or power cycle the module	status output	None

CO	Key zeroization	Zeroizes keys and CSPs by rebooting or power cycling the module.	Reboot or power cycle the module	None	AES Key – W Triple-DES Key – W HMAC Key – W RSA Private/Public Key – W ECDH Private/Public Key – W Hash DRBG: Entropy – W Hash DRBG Seed – W Hash DRBG 'V' Value – W Hash DRBG 'C' Value – W HMAC DRBG: Entropy – W HMAC DRBG Seed – W HMAC DRBG 'V' Value – W HMAC DRBG Key – W CTR DRBG: Entropy – W CTR DRBG Seed – W CTR DRBG 'V' Value – W CTR DRBG 'Key' Value – W

The module does not provide any key generation services or perform key generation for any of its Approved algorithms. Keys are passed in from calling application via API parameters.

2.6 Algorithms

2.6.1 FIPS Approved Algorithms

Table 5 lists the cryptographic algorithms used in the FIPS mode of operation, which are only approved algorithms.

Table 5 – Approved Algorithms

Algorithm	Certificate Numbers (With/Without AES-Ni)
AES in CBC, CTR and ECB modes (encryption/decryption) with 128, 192, and 256-bit keys and XTS mode (encryption/decryption) with 128 and 256-bit keys	A1291

DRBG (SP 800-90A): **Hash_DRBG:** prediction resistance supported with SHA-1, SHA-256, SHA-384, SHA-512 **HMAC_DRBG:** prediction resistance supported with SHA-1, SHA-256, SHA-384, SHA-512 **CTR_DRBG:** prediction resistance and derivation function supported with AES-128, AES-192, AES-256	A1291
ECDSA (186-4) KeyGen and KeyVer with curve P-256	A1291
ENT (NP)	N/A
HMAC with SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512	A1291
KAS-SSC (ephemeralUnified) with curve P-256	A1291
RSA (186-4): SigGenPKCS1.5 with 2048, 3072, 4096 SigVerPKCS1.5 with 2048, 3072, 4096	A1291
SHS: SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512	A1291
Triple-DES in CBC and ECB modes (encryption/decryption with keying option 1) and CTR mode (encryption/decryption) **(Note: After December 31, 2023) this security function will no longer be allowed for use in the Approved mode)**	A1291

Note:

- For Triple-DES, the user of the module is responsible to comply with the maximum use of the same key for encryption operations, limited to 2^16 64-bit data block encryptions, as defined in Implementation Guidance A.13 SP 800-67rev1 Transition.
- XTS-AES encryption/decryption can only be used for storage applications in the Approved mode.
- The module generates random numbers that provide at least 256 bits of security strength.
- This cryptographic module has been validated for compliance with NIST SP 800-90B. Based on noise source testing and analysis, the estimated minimum amount of entropy per the source output bit is about 0.56 bits. The overall amount of generated entropy meets the required security strength of 256 bits based on the entropy per bit and amount of entropy requested by the module.
- For the SHA-1 hash function, the user of the module should not use the function for digital signature generation in the approved mode.
- ECDSA has been tested solely as a prerequisite for KAS-SCC.

2.7 Physical Security

The VMware's Linux Cryptographic Module is a software module, which FIPS defines as a multiple-chip standalone cryptographic module. As such, it does not include physical security mechanisms. Thus, the FIPS 140-2 requirements for physical security are not applicable.

2.8 Operational Environment

The module was tested and found to be FIPS 140-2 compliant in the following operational environments:

- *Photon OS 4.0 running on a Dell PowerEdge R740 with an Intel® Xeon® Gold 6230R with PAA;*
- *Photon OS 4.0 running on a Dell PowerEdge R740 with an Intel® Xeon® Gold 6230R without PAA;*
- *Photon OS 4.0 on VMware ESXi 7.0 running on a Dell PowerEdge R740 with an Intel® Xeon® Gold 6230R with PAA; and*
- *Photon OS 4.0 on VMware ESXi 7.0 running on a Dell PowerEdge R740 with an Intel® Xeon®*

Gold 6230R without PAA.

All cryptographic keys and CSPs are under the control of the OS, which protects its CSPs against unauthorized disclosure, modification, and substitution. The module only allows access to CSPs through its well-defined API.

Per IG G.5, VMware affirms that the module remains compliant with the FIPS 140-2 validation when operating on any general-purpose computer (GPC) provided that the GPC uses the specified single user operating system/mode specified on the validation certificate, or another compatible single user operating system. The CMVP allows vendor porting and re-compilation of a validated cryptographic module from the operational environment specified on the validation certificate to an operational environment which was not included as part of the validation testing as long as the porting rules are followed.

CMVP makes no claims to the correct operation of the module or the minimum strength of generated keys when ported to an OE not on the validation certificate.

- *Photon OS 4.0 running on a Dell PowerEdge R740 with an Intel® Xeon® Gold 6126 with PAA;*
- *Photon OS 4.0 running on a Dell PowerEdge R740 with an Intel® Xeon® Gold 6126 without PAA;*
- *Photon OS 4.0 on VMware ESXi 7.0 running on a Dell PowerEdge R740 with an Intel® Xeon® Gold 6126 with PAA; and*
- *Photon OS 4.0 on VMware ESXi 7.0 running on a Dell PowerEdge R740 with an Intel® Xeon® Gold 6126 without PAA.*
- *Photon OS 4.0 on VMware ESXi 6.7 running on a Dell PowerEdge R740 with an Intel® Xeon® Gold 6126 with PAA; and*
- *Photon OS 4.0 on VMware ESXi 6.7 running on a Dell PowerEdge R740 with an Intel® Xeon® Gold 6126 without PAA.*
- *Photon OS 4.0 on VMware ESXi 6.7 running on a Dell PowerEdge R740 with an Intel® Xeon® Gold 6230R with PAA; and*
- *Photon OS 4.0 on VMware ESXi 6.7 running on a Dell PowerEdge R740 with an Intel® Xeon® Gold 6230R without PAA*

2.9 Cryptographic Key Management

The module supports the CSPs listed below in Table 8.

Table 6 - List of Cryptographic Keys, Key Components, and CSPs

Key	Key Type	Generation/Input	Output	Storage	Zeroization	Use
AES key	128, 192, 256 bit keys	Input via API in plaintext	Never output from the module	In RAM	Reboot OS; Cycle host power	Encryption, Decryption
DRBG Random Number	**CTR_DRBG:** AES-128, AES-192, AES-256 with DF, with/without PR **Hash_DRBG:** SHA-1, SHA-256, SHA-384, SHA-512 with/without PR **HMAC_DRBG:** SHA-1, SHA-256, SHA-384, SHA-512 with/without PR	Generated internally	Output via API in plaintext	In RAM	Reboot OS; Cycle host power	Random Number Generation
CTR DRBG Entropy	64-byte value	Generated internally	Never output from the module	In RAM	Reboot OS; Cycle host power	Entropy input for CTR DRBG
CTR DRBG Seed	256, 320, 384 bit values	Generated internally	Never output from the module	In RAM	Reboot OS; Cycle host power	Seed material for CTR DRBG
CTR DRBG 'V' Value	128-bit value	Generated internally	Never output from the module	In RAM	Reboot OS; Cycle host power	Internal state value used with CTR DRBG
CTR DRBG 'Key' Value	128, 192, 256 bit AES keys	Generated internally	Never output from the module	In RAM	Reboot OS; Cycle host power	Internal state value used with CTR DRBG
Hash DRBG Entropy	64-byte value	Generated internally	Never output from the module	In RAM	Reboot OS; Cycle host power	Entropy input for Hash DRBG
Hash DRBG Seed	440, 888 bit values	Generated internally	Never output from the module	In RAM	Reboot OS; Cycle host power	Seed material for Hash DRBG
Hash DRBG 'V' Value	Internal state value	Generated internally	Never output from the module	In RAM	Reboot OS; Cycle host power	Internal state value used with Hash DRBG

Hash DRBG 'C' Value	Internal state value	Generated internally	Never output from the module	In RAM	Reboot OS; Cycle host power	Internal state value used with Hash DRBG
HMAC DRBG Key	Internal state value	Generated internally	Never output from the module	In RAM	Reboot OS; Cycle host power	Internal state value used with HMAC DRBG
HMAC DRBG Entropy	64-byte value	Generated internally	Never output from the module	In RAM	Reboot OS; Cycle host power	Entropy input for HMAC DRBG
HMAC DRBG Seed	440, 888 bit values	Generated internally	Never output from the module	In RAM	Reboot OS; Cycle host power	Seed material for HMAC DRBG
HMAC DRBG 'V' Value	Internal state value	Generated internally	Never output from the module	In RAM	Reboot OS; Cycle host power	Internal state value used with HMAC DRBG
ECDH Private Key	ECC CDH P-256 Curve	Generated internally via Approved DRBG	Output via API in plaintext	In RAM	Reboot OS; Cycle host power	Shared Secret Computation
ECDH Public Key	ECC CDH P-256 Curve	Computed internally	Output via API in plaintext	In RAM	Reboot OS; Cycle host power	Shared Secret Computation
ECDH Public Key (other party)	ECC CDH P-256 Curve	Input via API in plaintext	Never output from the module	In RAM	Reboot OS; Cycle host power	Shared Secret Computation
ECDH Shared Secret	ECC CDH Primitive P-256 Curve	Computed internally	Output via API in plaintext	In RAM	Reboot OS; Cycle host power	Shared Secret Computation
HMAC key	160 to 2048 bit keys	Input via API in plaintext	Never output from the module	In RAM	Reboot OS; Cycle host power	Message Authentication
RSA Private Key	2048, 3072, 4096 bit keys	Input via API in plaintext	Never output from the module	In RAM	Reboot OS; Cycle host power	Signature Generation
RSA Public Key	2048, 3072, 4096 bit keys	Input via API in plaintext	Never output from the module	In RAM	Reboot OS; Cycle host power	Signature Verification
Triple-DES key	Keying Option 1	Input via API in plaintext	Never output from the module	In RAM	Reboot OS; Cycle host power	Encryption, Decryption

2.10 EMI / EMC

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

2.11 Self-Tests

Cryptographic self-tests are performed by the module when the module is powered on. The following sections list the self-tests performed by the module, their expected error status, and any error resolutions.

2.11.1 Power-Up Self-Tests

Power-up self-tests are automatically performed by the module at module initialization or when the module powers on. The list of power-up self-tests that follows may also be run on-demand when the CO reboots the Operating System. The module will perform the listed power-up self-tests to successful completion. During the execution of self-tests, cryptographic functions and data output from the module are inhibited.

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 the Photon OS 4.0. If the error persists, the module must be reinitialized.

The VMware's Linux Cryptographic Module performs the following Power-up Self-tests:

- Software integrity check (HMAC with SHA-256 Integrity Test) - The software integrity test is performed by the VMware Linux Cryptographic Module, which coordinates the integrity check of the module's kernel package.

Known Answer Tests (KATs)

- AES Encryption and Decryption KAT in ECB, CBC and CTR modes with 128, 192 and 256-bit keys
- CTR_DRBG KAT with AES 128, 192 and 256-bit keys, with and without prediction resistance
- ECDH primitive "Z" computation test
- HASH_DRBG KAT with all combinations (SHA-1, SHA-256, SHA-384 and SHA-512)
- HMAC with SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 KATs
- HMAC_DBRG KAT with all combinations (SHA-1, SHA-256, SHA-384 and SHA-512)
- RSA (PKCS#1) Signature Generation and Verification KAT using 2048, 3072, 4096-bit keys
- SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 KATs
- Triple-DES Encryption and Decryption KAT in CBC, CTR and ECB modes
- XTS-AES KAT with 128 and 256-bit key sizes

2.11.2 Conditional Self-Tests

- DRBG Continuous RNG Test for stuck fault
- SP 800-90B Health Tests

2.11.3 Critical Function Self-Tests

The SP 800-90A specification requires that certain critical functions be tested to ensure the security of the DRBGs. Therefore, the following power-up critical function tests are implemented by the cryptographic module for each DRBG:

- SP 800-90A Instantiate Critical Function Test
- SP 800-90A Generate Critical Function Test
- SP 800-90A Reseed Critical Function Test

2.12 Mitigation of Other Attacks

The module was not designed to mitigate any other attacks.

3 Secure Operation

The VMware Linux Cryptographic Module meets Level 1 requirements for FIPS 140-2. The sections below describe how to place and keep the module in FIPS Approved mode of operation.

3.1 Crypto Officer Guidance

Installation and operation of the VMware Linux Cryptographic Module requires the proper installation of the Photon OS 4.0. There are not additional steps that must be performed to use the module correctly.

3.1.1 Initial Setup

Prior to the secure installation of the Photon OS 4.0, the CO shall prepare the virtual environment required to securely operate it. This includes installing VMware vSphere Hypervisor (ESXi) 7.0 (see *vSphere Installation and Setup*). Both virtual and "bare metal" environments require the Dell PowerEdge R740 server to run the installation.

The tar archive containing VMware's Linux Cryptographic Module prior to build time, contains the HMAC-SHA-256 digest:

"f447ffc875b3c976d17c0d8c2eaf7b25307613bcd5dbf51c743b785ccd0ea202"

The CO will then install Photon OS 4.0 and verify the full canister version as "LKCM 4.0.1".

3.1.2 Secure Installation and Operation

The cryptographic functionality of VMware's Linux Cryptographic Module comes installed with Photon OS 4.0 and cannot be "unloaded".

In order to run the Photon OS 4.0 kernel in FIPS compliant mode, the Crypto Officer **shall** perform following actions using root access on the kernel command line interface to configure the module.

1. Edit the "/boot/photon.cfg" kernel file and append 'fips=1' to the "photon_cmdline" line
2. Reboot using the "reboot" command.
3. To check the FIPS mode, run "cat /proc/sys/crypto/fips_enabled", which will show '1' when FIPS mode is enabled or '0' when FIPS mode is not enabled.
4. To verify that the OS is running certified version of VMware's Linux Cryptographic Module run command "**dmesg | grep FIPS**". It should print following output:
    - *FIPS(fips_integrity_init): canister LKCM 4.0.1 found (based on 5.10.21-3-secure)*
    - *FIPS(fips_integrity_init): processing 19 sections, 863265 bytes*
    - *FIPS canister HMAC: f447ffc875b3c976d17c0d8c2eaf7b25307613bcd5dbf51c743b785ccd0ea202*
    - *FIPS canister verification passed!*

The CO should ensure that the operating environment is patched and updated in a timely fashion to reduce exposure to security vulnerabilities.

3.2 User Guidance

The User shall adhere to the guidelines of this Security Policy. The User does not have any ability to install or configure the module. Operators in the User role are able to use the services available to the User role. The User is responsible for reporting to the CO if any irregular activity is noticed.

4 Acronyms

Table 9 provides definitions for the acronyms used in this document.

Table 7 - Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
API	Application Programming Interface
CBC	Cipher Block Chaining
CLI	Command Line Interface
CMVP	Cryptographic Module Validation Program
CO	Crypto Officer
CPU	Central Processing Unit
CSE	Communication Security Establishment
CSP	Critical Security Parameter
CTR	Counter
DES	Data Encryption Standard
DNS	Domain Name System
DRBG	Deterministic Random Bit Generator
ECB	Electronic Code Book
ECC	Elliptical curve cryptography
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FFC	Finite Field Cryptography
FIPS	Federal Information Processing Standard
GCM	Galois/Counter Mode
HDD	Hard Disk Drive
HMAC	(Keyed) Hash Message Authenticating Code
IPsec	Internet Protocol Security
IT	Information Technology
KAS	Key Agreement Scheme
RSA	Rivest, Shamir, Adleman
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
Triple-DES	Triple Data Encryption Standard
XTS	Ciphertext stealing