VMware VMkernel Cryptographic Module 2.0

ISO/IEC 19790 and FIPS 140-3 Non-Proprietary Security Policy

Document Version: 1.2

vmware®

Table of contents

Section 1. General

This non-proprietary Security Policy is provided in accordance with ISO/IEC 19790 Annex B, FIPS 140-3, and NIST 800-140B. VMware VMkernel Cryptographic Module 2.0 (software version 2.0), herein after referred as the module, the cryptographic module, or the software module, meets overall Security Level 1 requirements. Table 1 below lists the level of validation for each area in the FIPS PUB 140-3.

Table 1 –Security Levels

ISO/IEC 24759 Section 6. [Number Below]	FIPS 140-3 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 Parameters Management	1
10	Self-tests	1
11	Life-Cycle Assurance	1
12	Mitigation of Other Attacks	N/A

Section 2. Cryptographic Module Specification

The software module consists of two libraries running in a modifiable operating environment, cryptoLoader and crypto_fips. The software version of the module is 2.0. For validation purposes, the module is tested in the following operational environment:

Table 2 – Tested Operational Environments

#	Operating System	Hardware Platform	Processor	PAA/Acceleration
1	ESXi 8.0	Dell EMC PowerEdge R650	Intel Xeon Gold 6330 2.00GHz	Without PAA

The module, a set of object files/libraries, is intended to provide cryptographic services to Vmware's ESXi platform. Table 3 below lists all security functions in the module for use in approved services. Vendor Affirmed Operational Environments have not been claimed.

Table 3 – Approved Algorithms

CAVP Cert	Algorithm and Standard	Mode/Method	Description/Key Size(s)/Key Strengths(s)	Use / Function
A2792	AES-CBC FIPS PUB 197	AES-CBC	Key Size: 128, 192, 256 bits Strengths: 128, 192, 256 bits	Symmetric key encryption and decryption
A2792	AES-CBC-CS3 FIPS PUB 197	AES-CBC-CS3	Key Size: 128, 192, 256 bits Strengths: 128, 192, 256 bits	Symmetric key encryption and decryption
A2792	AES-CTR FIPS PUB 197	AES-CTR	Key Size: 128, 192, 256 bits Strengths: 128, 192, 256 bits	Symmetric key encryption and decryption
A2792	AES-ECB FIPS PUB 197	AES-ECB	Key Size: 128, 192, 256 bits Strengths: 128, 192, 256 bits	Symmetric key encryption and decryption
A2792	AES-GCM NIST SP 800-38D	AES-GCM	Key Size: 128, 192, 256 bits Strengths: 128, 192, 256 bits	Symmetric key encryption and decryption

CAVP Cert	Algorithm and Standard	Mode/Method	Description/Key Size(s)/Key Strengths(s)	Use / Function
A2792	AES-XTS Testing Revision 2.0 NIST SP 800-38E	AES-XTS	Key Size: 128, 256 Strengths: 128, 256 bits	Symmetric key encryption and decryption
A2792	HMAC-SHA-1 (FIPS PUB 198-1)	SHA-1	Key Size: 160, bits Strength: 160 bits	Authentication
A2792	HMAC-SHA2-256 (FIPS PUB 198-1)	SHA2-256	Key Size: 256 bits Strength: 256 bits	Integrity test
A2792	HMAC-SHA2-512 (FIPS PUB 198-1)	SHA2-512	Key Size: 512 bits Strength: 512 bits	Authentication
A2792	SHA-1 (FIPS 180-4)	SHA-1	N/A	Hashing
A2792	SHA2-256 (FIPS 180-4)	SHA2-256	N/A	Hashing
A2792	SHA2-512 (FIPS 180-4)	SHA2-512	N/A	Hashing
A2792	Counter DRBG (NIST SP 800-90Ar1)	CTR_DRBG	Key Size: AES-256 Strength: 256 bits	Random bit generation

The module does not implement and use any non-approved algorithms and thus does not support the following: Non-Approved Algorithms Allowed in the Approved Mode of Operation, Non-Approved Algorithms Allowed in the Approved Mode of Operation with No Security Claimed and Non-Approved Algorithms Not Allowed in the Approved Mode of Operation. The cryptographic module runs only in an Approved mode of operation. The module does not support a non-Approved mode of operation.

Below is a block diagram showing the location of the module components with respect to the ESXi operating system and the applications which interact with the module. The diagram includes the cryptographic boundary containing the module components (red dotted outline) and also depicts the physical perimeter of the module (the GPC, i.e. the TOEPP).

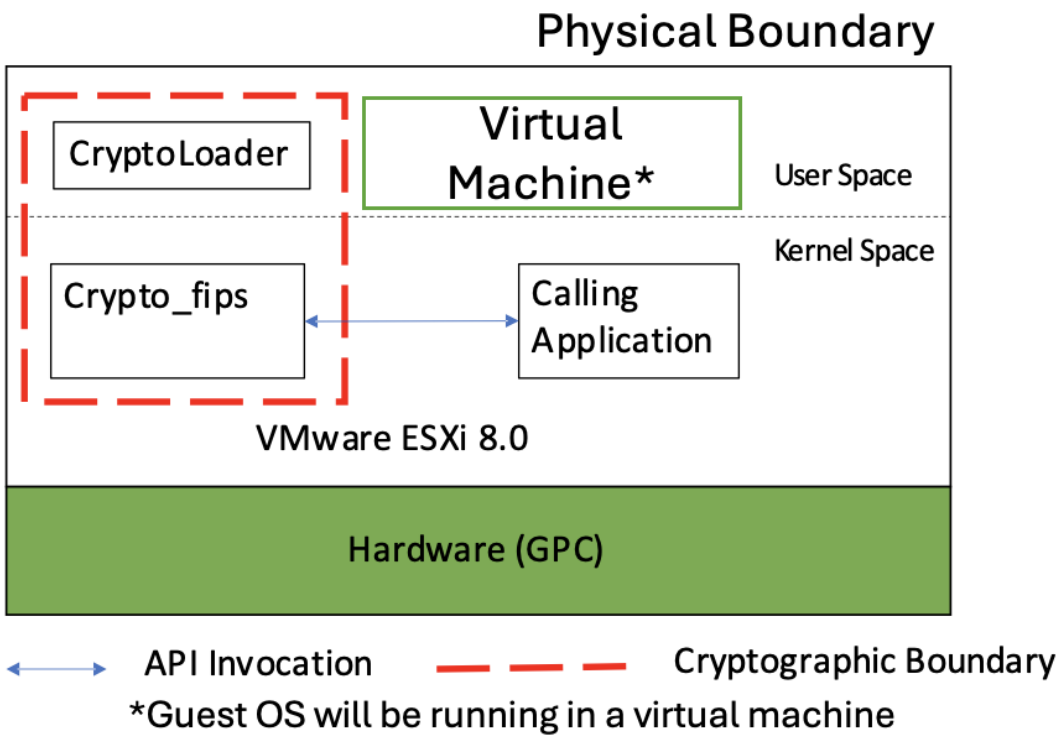

Figure 1 – Cryptographic Boundary

Overall security design and the rules of operation

When ESXi boots, the cryptoloader is called. This component self-tests its internal implementation of SHS (FIPS 180-4) and HMAC (FIPS PUB 198-1), which are both used in the pre-operational integrity test. Cryptoloader reads the entire crypto_fips file and performs the pre-operational integrity test on it as well. If it passed, cryptoloader calls the ESXi kernel to load crypto_fips as a kernel module.

Crypto_fips provides cryptographic services as described in the Approved Services table. Authentication and access to SSPs are controlled by the ESXi operating system. The module supports a single user role, Crypto Officer. This role is assumed implicitly by using the module.

The module is operated by calling the API functions and inputting the appropriate parameters. If the module enters the error state, the state is cleared by rebooting the ESXi operating system to reload the module.

To unload or shutdown the module, the ESXi operating system must be shutdown.

The module also supports internal IV generation using the module's approved DRBG. The IV is at least 96 bits in length per [SP800-38D] Section 8.2.2 and [FIPS140-3_IG] C.H Scenario 2.

In each case, in the event that the Module power is lost and restored the user must ensure that the AES GCM encryption/decryption keys are re-distributed. The module does not support persistent storage of SSPs.

The module complies with IG C.I by explicitly checking that Key_1 ≠ Key_2 before using the keys in the XTS-AES algorithm to process data with them.

Section 3. Cryptographic Module Interfaces

Table 4 below maps the logical interfaces of the module with the ISO/IEC 19790:2012 defined logical interfaces:

Table 4 – Ports and Interfaces

Physical port	Logical Interface	Data that Passes over port/interface
N/A	Data Input	The module accepts data input through the input arguments of the API functions
	Data Output	The module produces data output through the parameter of the API functions
	Control Input	The module accepts control input through the input arguments of the API functions used to control the module
	Status Output	The module produces status output through the return values for function calls and error messages
	Power input	The module is initialized by powering on the underlying host platform

The physical ports of the cryptographic module are the same as the appliance on which it is executing. The logical interfaces are C-language based Application Program Interfaces (APIs). The Data Input Interface corresponds to the input arguments of the API functions that take data to process cryptographic operations. The operation can be encryption or decryption, hashing, MAC generation or receiving seeding material for the DRBG. Similarly, Data Output interface consists of the output parameter of the API that holds the result of the operation, such as ciphertext, a MAC or a digest value. The Control Input interface is the API arguments that specifies control over input data (ex. Length of plaintext or key length). The Status Output includes the return values. The return values are associated with success or error code for the service. The module does not support a Control Output interface. The Power Input interface corresponds to the power port of the underlying appliance on which the module runs.

Section 4. Roles, Services, and Authentication

The VMware VMkernel Cryptographic Module 2.0 meets all FIPS 140-3 level 1 requirements for Roles, Services, and Authentication. The module implements only the Crypto Officer (CO) role. The CO is responsible for initializing and running the module. Table 5 lists the services offered to the CO role.

Table 5 – Roles, Service Commands, Input and Output

Role	Service	Input	Output
Crypto Officer	Initialization of the module	None	None
Crypto Officer	Run self-tests	API command	The results of each self-test
Crypto Officer	Encryption	Key and plaintext input via API	Encrypted data
Crypto Officer	Decryption	Key and ciphertext input via API	Plaintext data
Crypto Officer	Hashing	Data input via API	Hash of the input data
Crypto Officer	Message Authentication Code (MAC) Generation	Key input via API Data input via API	MAC of the input data
Crypto Officer	Deterministic Random Bit Generation (DRBG)	Seed input via API	Random bits
Crypto Officer	Show version (includes Show Status)	API command	The module version will be output to the log
Crypto Officer	Perform zeroisation	Reboot OS; Cycle host power; API call	The module version will be output to the log or a success code returned (in case of an API call)

The module is a level 1 software module and does not implement any authentication. The calling application implicitly assumes the Crypto Officer role when the ESXi operating system allows access to the module.

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 = Zeroise: The module 9eroizes the SSP.

Table 6 – Approved Services

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys and/or SSPs	Indicator
Initialization of the module.	-	-	-	Crypto Officer	-	The module is running
Run self-tests	-	All per Table 3 CAVP Cert. #A2792	All per Table 9	Crypto Officer	E	The self-test results are output in the log
Encryption	Encrypt plaintext using supplied key and algorithm specification	AES modes: ECB, CTR, CTS, CBC, and GCM CAVP Cert. #A2792	AES keys: 128-bit, 192-bit, 256-bit	Crypto Officer	WEZ	Return values indicate success or error
		AES mode: XTS CAVP Cert. #A2792	AES keys: 128-bit, 256-bit			
Decryption	Decrypt ciphertext using supplied key and algorithm specification	AES modes: ECB, CTR, CTS, CBC, and GCM CAVP Cert. #A2792	AES keys: 128-bit, 192-bit, 256-bit	Crypto Officer	WEZ	Return values indicate success or error
		AES mode: XTS CAVP Cert. #A2792	AES keys: 128-bit, 256-bit			
Hashing	Compute and return a message digest using SHA algorithm	SHA-1, SHA2-256, SHA2-512 CAVP Cert. #A2792	-	Crypto Officer	-	Return values indicate success or error
Message Authentication Code (MAC) Generation	Compute and return a hashed message authentication code	HMAC SHA-1, SHA2-256, SHA2-512 CAVP Cert. #A2792	HMAC key, 160-bit, 256-bit	Crypto Officer	WEZ	Return values indicate success or error

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys and/or SSPs	Indicator
Random Bit Generation	Generate random bits by using the DRBG	CTR_DRBG (AES-CTR 256) CAVP Cert. #A2792	DRBG seed: 384-bit DRBG Entropy Input: 256-bit	Crypto Officer	WEZ	Return values indicate success or error
Show version (includes Show Status)	Show the module name and version	-	-	Crypto Officer	-	The module name and version are output in the log
Perform zeroisation	Zeroisation of the module on demand by power-cycling the host platform, rebooting the OS or via an API call	-	-	Crypto Officer	Z	The module name and version are output in the log or a success code returned (in case of an API call)

The module does not implement any non-approved services.

Section 5. Software/Firmware Security

For the purposes of a FIPS 140-3 level 1 validation, the cryptographic module consists of two object files, cryptoloader and crypto_fips. The module performs no communications other than with the consuming host application (the process that invokes the module services via the module's API), which can be considered as the host for the module. The module runs a HMAC-SHA2-256 integrity verification during initialization by the host application. The module also runs the Known Answer Test (KAT) for HMAC-SHA2-256 prior to running the integrity check. The CO can reload the module to run the integrity test on demand. The module does not support software loading.

Section 6. Operational Environment

VMware VMkernel Cryptographic Module 2.0, a software module, runs on the VMware ESXi operating system and the Dell EMC PowerEdge R650 with Intel Xeon Gold 6330 2.00GHz, which is classified as a modifiable OE. The requirements under ISO/IEC 19790, section 7.6 “Operational environment”, are met by the module.

Section 7. Physical Security

Per ISO/IEC 19790:2012 classification, this is a multi-chip standalone cryptographic module. The appliance the software module runs on has a production grade chassis.

Section 8. Non-invasive Security

The module does not implement any non-invasive security mitigations and thus the requirements per this section do not apply to the module.

Section 9. Sensitive Security Parameters Management

The following table lists the Sensitive Security Parameters (SSP) that exist when the module runs in the Approved mode of operation.

Table 7 – SSPs

Key/SSP Name/ Type	Strength	Security Function and Cert. Number	Generation	Import /Export	Establishment	Storage	Zeroisation	Use & related keys
AES key for modes: ECB, CTR, CTS, CBC, and GCM (CSP)	128, 192, 256-bits key with 128, 192, 256-bits strength	ECB, CTR, CTS, CBC, and GCM, CAVP Cert. #A2792	N/A	Imported only, The key is not exported from the module MD/EE	N/A	RAM in plaintext	Reboot OS; Cycle host power; API call	Encryption, Decryption
AES XTS Key (CSP)	128, 256-bits key with 128, 256 bits strength	XTS. CAVP Cert. #A2792	N/A	Imported only, The key is not exported from the module MD/EE	N/A	RAM in plaintext	Reboot OS; Cycle host power; API call	Encryption, Decryption
HMAC key (CSP)	160-bit, 256-bit, 512-bit	SHA-1, SHA2-256, 512, CAVP Cert. #A2792	N/A	Imported only, The key is not exported from the module MD/EE	N/A	RAM in plaintext	Reboot OS; Cycle host power; API call	Message Authentication

Key/SSP Name/ Type	Strength	Security Function and Cert. Number	Generation	Import /Export	Establishment	Storage	Zeroisation	Use & related keys
DRBG Entropy Input (CSP)	Used to seed the DRBG	ENT (P)	N/A	Imported only, The SSP is not exported from the module MD/EE	N/A	RAM in plaintext	Reboot OS; Cycle host power; API call	Random number generation
DRBG seed (CSP)	Seed used to derive the internal state of the DRBG	CTR_DRBG, CAVP Cert. #A2792	Constructed internally per SP800-90Ar1 DRBG	The SSP is not exported from the module MD/EE	N/A	RAM in plaintext	Reboot OS; Cycle host power; API call	Random number generation
DRBG.InternalState_V (CSP)	V (128-bits) CAVP Cert. #A2792	CTR_DRBG, CAVP Cert. #A2792	Generated internally per SP800-90Ar1 DRBG	Does not enter or exit the module MD/EE	N/A	RAM in plaintext	Reboot OS; Cycle host power; API call	Random number generation
DRBG.InternalState_Key (CSP)	256-bits CAVP Cert. #A2792	CTR_DRBG, CAVP Cert. #A2792	Generated internally per SP800-90Ar1 DRBG	Does not enter or exit the module MD/EE	N/A	RAM in plaintext	Reboot OS; Cycle host power; API call	Random number generation

The module also comprises of the following non-SSP:

Software Integrity Key: HMAC key; 256-bits; Hardcoded in the module at manufacture and never zeroised. Verifies the integrity of the module upon initialization.

The module contains an AES-CTR based DRBG for random bit generation. The module does not implement a non-approved DRBG.

The module does not generate or export any keys. Keys are imported as parameters of API function calls. The keys remain in the volatile memory and are never stored on persistent memory.

The module zeroises SSPs by overwriting them with zeros. There are API functions that will zeroise any SSPs related to a specific cryptographic operation. Successful completion of the cryptographic operation/service is the implicit indicator of successful zeroisation in

this case. When the underlying host platform is shutdown any remaining SSPs will be zeroised. A successful power-cycle of the underlying host platform is the implicit indicator of successful zeroisation. Unauthorized access to the module's unprotected SSPs is prevented by the ESXi operating system.

Table 8 – Non-Deterministic Random Number Generation Specification

Entropy sources	Minimum number of bits of entropy	Details
ENT (P)	0.421389 bits of entropy per bit	FIPS 140-3 IG 9.3.A Scenario 1 (b)

Section 10. Self-tests

When the module is loaded, all self-tests are run automatically before the module becomes operational. If any of the self-tests fail, the module enters the error state. While in the error state, the module cannot perform any cryptographic operations. When the module enters the error state due to a failing self-test, the name of the self-test is shown/printed in the log. To clear the error, the module must be reloaded.

Below is the list of self-tests performed by the cryptographic module. The module performs an HMAC-SHA2-256 KAT prior to performing the software integrity test.

Pre-operational Self-Tests (POSTs):

- Software Integrity Test (HMAC-SHA2-256)

Conditional Self-Tests:

- Cryptographic Algorithm Self-Tests (CASTs):
    - AES KATs
        - AES CBC 128-bit Encrypt KAT
        - AES CBC 128-bit Decrypt KAT
        - AES CTR 128-bit Encrypt KAT
        - AES CTR 128-bit Decrypt KAT
        - AES CBC-CS 128-bit Encrypt KAT
        - AES CBC-CS 128-bit Decrypt KAT
        - AES ECB 128-bit Encrypt KAT
        - AES ECB 128-bit Decrypt KAT
        - AES GCM 256-bit Encrypt KAT
        - AES GCM 256-bit Decrypt KAT
        - AES XTS 256-bit Encrypt KAT
        - AES XTS 256-bit Decrypt KAT
    - HMAC KATs
        - HMAC-SHA1 KAT
        - HMAC-SHA2-256 KAT
        - HMAC-SHA2-512 KAT
    - NIST SP800-90Ar1 CTR_DRBG KAT
    - ENT (P) NIST SP 800-90B Health Tests
- Critical Functions Test: Performed for the DRBG, as per SP800-90A, Section 11:
    - Instantiation Test
    - Generation Test
    - Reseed Test
    - Uninstantiate Test

Section 11. Life-cycle Assurance

Distribution and Installation

VMware VMkernel Cryptographic Module 2.0 is distributed internal to VMware, it is not available to VMware customers.

The operator of the module, the Crypto Officer, does not install the module. It is shipped pre-installed by the manufacturer, VMware as part of the VMware ESXi.

Configuration

The module does not require any configuration for operating in the Approved mode.

Initialization and startup

When the ESXi operating system starts, the module is automatically loaded and initialized.

Verification of the module

The module name and version is printed in the log upon successful initialization. The log message contains: "VmkCrypto version 2.0 successfully initialized."

Destruction and Zeroisation

The module will remain on the ESXi operating system until the operating system is removed or replaced. When the ESXi operating system is removed or replaced, the module will be erased along with the operating system. Any SSPs in the module will be zeroised at that time.

Section 12. Mitigation of Other Attacks

The module does not implement mitigation of other attacks and thus the requirements per this section do not apply to it.

Acronyms

AES	Advanced Encryption Standard
API	Application Program Interface
CAST	Cryptographic Algorithm Self-Test
CBC	Cipher Block Chaining
CFB	Cipher Feedback
CO	Crypto-Officer
CSP	Critical Security Parameter
CTR	Counter
CTS	Cipher-Text Stealing
CVL	Component Validation List
DRBG	Deterministic Random Bit Generation
ECB	Electronic Code Book
FIPS	Federal Information Processing Standard
GCM	Galois/Counter Mode
GPC	General Purpose Computer
HMAC	(Keyed-)Hash Messages Authentication Code
ISO/IEC	International Organization for Standardization/ International Electrotechnical Commission
KAT	Known Answer Test
LED	Light Emitting Diode
MAC	Message Authentication Code
NIST	National Institute of Standards and Technology
OE	Operational Environment
OS	Operation System

PAA	Processor Algorithm Acceleration
POST	Pre-operational Self-Test
PUB	Publication
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
SSP	Sensitive Security Parameter
SP	Special Publication
XOR	Exclusive OR
XTS	XEX-based tweaked-codebook mode with ciphertext stealing

END OF DOCUMENT

Item No: vmw-wp-tech-temp-uslet-word-2021 8/21