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

VMware's VPN Crypto Module

Firmware version: 21.11

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

Document version: 2.3

Contents

List of tables

List of figures

1. General

This is a non-proprietary Cryptographic Module Security Policy for VMware's VPN Cryptographic Module from Broadcom Inc. This Security Policy describes how VMware's VPN Cryptographic Module 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 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.

Security Levels

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

Table 1 - ISO/IEC 24759 Section 6 Security Levels for Module Validation

ISO/IEC 24759 Section 6	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	1
8	Non-invasive Security	N/A
9	Sensitive Security Parameters	1

10	Self-Tests	1
11	Life-Cycle Assurance	1
12	Mitigation of Other Attacks	N/A
	Overall Module validation level	1

2. Cryptographic Module Specification

VMware's VPN Crypto Module is a firmware cryptographic module whose purpose is to provide FIPS 140-3 validated cryptographic functions to various applications utilizing VPN capabilities. The module was tested and found to be compliant with FIPS 140-3 security level 1 requirements on the operational environments (OE) listed in Table 2.

Table 2 - Tested Operational Environments

#	Operating System	Hardware Platform	Processor	PAA/Acceleration
1	Ubuntu 20.04 running on ESXi 8.0	Dell PowerEdge R650	Intel(R) Xeon(R) Gold 6330	Yes
2	Ubuntu 20.04 running on ESXi 8.0	Dell PowerEdge R650	Intel(R) Xeon(R) Gold 6330	No

Validation certificates for each Approved security function are listed in Table 3.

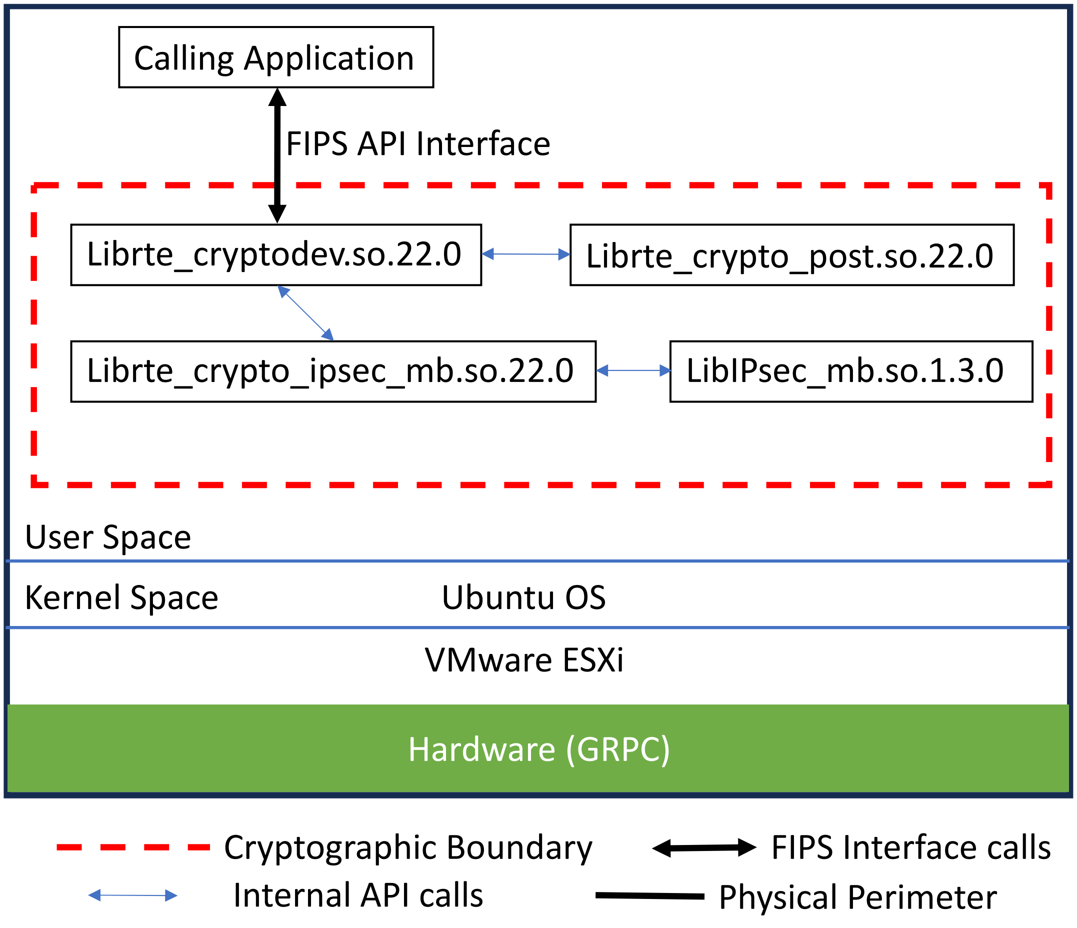
Table 3 - Approved Algorithms

CAVP Cert	Algorithm and Standard	Mode/Method	Description/Key Size/Strengths	Use / Function
A4384	AES (FIPS PUB 197)	CBC	Key Size: 128, 192, 256 bits	Symmetric key operation
A4384	AES (SP800-38B)	CMAC	Key Size: 128 bits	Symmetric key operation
A4384	AES (SP800-38C)	CCM	Key Size: 128 bits	Symmetric key operation
A4384	AES (SP800-38D)	GCM, GMAC	Key Size: 128,192,256 bits	Symmetric key operation
A4385	HMAC (FIPS PUB 198-1)	SHA2-256	Strength:256 bits	Integrity test

A4384	HMAC (FIPS PUB 198-1)	HMAC-SHA-1, HMAC-SHA2-224, HMAC-SHA2-256, HMAC-SHA2-384, HMAC-SHA2-512	Strength:128 to 256 bits	Authentication, Integrity checks
A4384	SHS (FIPS 180-4)	SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512	N/A	Hashing
A4385	SHS (FIPS 180-4)	SHA2-256	N/A	Hashing

The module does not use any allowed or non-approved algorithms and operates only in the Approved mode of operation.

Figure 1 – Cryptographic boundary and physical perimeter



Overall security design and the rules of operation

When the operating system boots, the module is initialized by calling librte_crypto_post, which runs the firmware integrity test and the KATs. Once librte_crypto_post finishes the POST tests the module is loaded as a device driver in the operating system. Calling applications can access the application once it is loaded as a device driver.

3. Cryptographic Module Interfaces

Table 4 - Ports and Interfaces

Physical Port	Logical Interface	Data that Passes over port/interface
Host computer Network Port, USB port, serial port	Data Input	The module accepts data input through the input arguments of the API functions.
Host computer Network Port, USB port, serial port	Data Output	The module produces data output through the parameters of the API functions.
Host computer Network Port, USB port, serial port, Power button	Control Input	The module accepts control input through the input arguments of the API functions used to control the module.
Host computer Network Port, USB port, serial port, LED status light	Status Output	The module produces status output through the return values for function calls and error messages.
Host computer Power Port	Power interface	N/A

The module does not implement a control output interface.

4. Roles, Services, and Authentication

Table 5 – Roles, Services and Command Input and Output

Role	Services	Input	Output
Crypto Officer	Initialization of the module	None	None
Crypto Officer	Run self-tests	The self-tests may be run on demand by rebooting the OS or cycling host power.	Results of each self-test

Crypto Officer	Show version	API command	The module version will be output to the log ("DPDK v21.11.2")
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	Zeroize	None	None
Crypto Officer	Show Status	None	Success: "Finished Self-test successfully" Error State: "Failed dpdk_init"

The module is a Level 1 firmware module and does not implement any authentication. The calling application implicitly assumes the Crypto Officer role when accessing 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 zeroizes the SSP.

Table 6 – Approved Services for Crypto Officer

Service	Description	Approved Security Functions	Keys / SSPs	Access Rights and Keys/SSPs	Indicator
Initialization of the module	Initialization of the module	-	-	N/A	The module is running

Run self-tests	The self-tests may be run on demand by rebooting the OS or cycling host power.	-	-	-	The self-test results are output in the log
Show version	Show the module name and version	-	-	-	The module name and version are output in the log
Show Status	Show the module is either operational or in an error state	-	-	-	In log messages: Success: “Finished Self-test successfully” Error State: “Failed dpdk_init”
Zeroization	Zeroize unprotected SSPs and key components	-	All SSPs	All SSPs: Z	The module reboot and startup will be shown in the log.
Encryption	Encrypt plaintext using supplied key and algorithm specification	AES modes: CBC, CCM, CMAC, GCM/GMAC	AES keys and IVs: 128-bit, 192-bit, 256-bit	All SSPs: WE	Return values indicate success. Null values or void pointers together with error logs indicate failures.
Decryption	Decrypt ciphertext using supplied key and algorithm specification	AES modes: CBC, CCM, CMAC, GCM/GMAC	AES keys and IVs: 128-bit, 192-bit, 256-bit	All SSPs: WE	Return values indicate success. Null values or void pointers together with error logs indicate failures.

Hashing	Compute and return a message digest using SHA algorithm	SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512	N/A	N/A	Return values indicate success. Null values or void pointers together with error logs indicate failures.
Message Authentication Code (MAC) Generation	Compute and return a hashed message authentication code	HMAC-SHA-1, HMAC-SHA2-224, HMAC-SHA2-256, HMAC-SHA2-384, HMAC-SHA2-512	HMAC key, 128 to 256-bits	All SSPs: WE	Return values indicate success. Null values or void pointers together with error logs indicate failures.

There are no non-approved services for the Crypto Officer.

5. Software/Firmware Security

For the purposes of a FIPS 140-3 level 1 validation, the cryptographic module is a set of files, listed here:

- librte_crypto_post.so.22.0
- librte_cryptodev.so.22.0
- libipsec_MB.so.1.3.0
- librte_crypto_ipsec_mb.so.22.0

The object code in the object module file is incorporated into the runtime executable application at the time the binary executable is generated. 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 self-test for HMAC SHA2-256 prior to running the integrity test. The temporary values generated during the integrity test of the module are zeroized upon the completion of the integrity test. The CO can reboot the OS or cycle host power to run the integrity test on demand.

6. Operational Environment

The operational environment is non-modifiable. The control plane Operating System (OS) is Linux, a multi-threaded operating system that supports memory protection between processes. Access to the underlying Linux implementation is not provided directly.

7. Physical Security

The module is a firmware module with a multi-chip standalone cryptographic embodiment. The module's host platform provides production-grade components and chassis using standard passivation.

8. Non-invasive Security

The module does not implement any non-invasive security measures, so this section is not applicable.

9. Sensitive Security Parameter Management

Table 7 – Sensitive Security Parameters

SSPs	Mode and Strength	Generation	Import/ Export	Establishment	Storage	Zeroisation	Use and Related Keys
AES Key	128, 192, 256-bit keys	N/A, the key is imported.	Imported only. The key is not exported from the module.	N/A	Random Access Memory (RAM) in plaintext	Reboot OS; Cycle host power	Encryption, Decryption
AES GCM/GMAC Key	128, 192, 256-bit keys	N/A, the key is imported.	Imported only. The key is not exported from the module.	N/A	Random Access Memory (RAM) in plaintext	Reboot OS; Cycle host power	Encryption, Decryption
AES GCM/GMAC IV	96-bit IV	N/A, the key is imported.	Imported only. The key is not exported from the module.	N/A	Random Access Memory (RAM) in plaintext	Reboot OS; Cycle host power	Encryption, Decryption
AES CCM Key	128-bit key	N/A, the key is imported.	Imported only. The key is not exported from the module.	N/A	Random Access Memory (RAM) in plaintext	Reboot OS; Cycle host power	Encryption, Decryption

AES CMAC key	128-bit key	N/A, the key is imported.	Imported only. The key is not exported from the module.	N/A	Random Access Memory (RAM) in plaintext	Reboot OS; Cycle host power	Authentication
HMAC Key	128-256 bits	N/A, the key is imported.	Imported only. The key is not exported from the module.	N/A	RAM in plaintext	Reboot OS; Cycle host power	Message Authentication
Firmware Integrity Key – HMAC key (not an SSP)	256-bit key	N/A	Does not enter or exit the module	N/A	Hardcoded in the module	No zeroization	Verifies integrity of the module upon initialization

Symmetric keys are provided to the module by the calling process and are destroyed when released by the appropriate API function calls. The module does not perform persistent storage of keys.

10. Self-tests

The self-tests are run automatically when the module powers on. The module does not allow any data output before the self-tests are completed successfully. If a KAT encryption or decryption result does not match the known answer, the test will fail. If the firmware Integrity test produces a result which does not match the Integrity MAC value, the test will fail. If a self-test fails, the module will enter an error state and the name of the failing self-test will be shown in the log. While in an error state, the module cannot perform cryptographic operations. To clear an error state, restart the module.

The self-tests may be run on demand by rebooting the OS or cycling host power.

Pre-Operational Self-Tests

- HMAC-SHA2-256 Integrity Test

Conditional Cryptographic Algorithm Tests

- AES CBC Encryption KAT (128, 192, and 256-bit)

- AES CBC Decryption KAT (128, 192, and 256-bit)
- AES GCM Encryption KAT (128, 192, and 256-bit)
- AES GCM Decryption KAT (128, 192, and 256-bit)
- AES CCM Encryption KAT (128-bit)
- AES CCM Decryption KAT (128-bit)
- AES-CMAC Encryption KAT (128-bit)
- AES-CMAC Decryption KAT (128-bit)
- HMAC-SHA-1, HMAC-SHA2-224, HMAC-SHA2-256, HMAC-SHA2-384 and HMAC-SHA2-512 KAT (note that the HMAC-SHA2-256 KAT is executed prior to the integrity test).

11. Life-cycle Assurance

Distribution and Installation

The module is distributed internally to Broadcom. It is not available to customers of Broadcom.

The operator does not install the module, it will be installed by Broadcom.

Configuration

The module does not require configuration and only Implements an approved mode of operation.

Initialization and Setup

When the OS starts, the module will be automatically loaded and initialized.

Verification of the Module

The module name and version will be printed in the log upon successful initialization.

Crypto Officer Guidance

Per IG C.H Scenario 1.b implementation ii), the AES GCM IV is constructed in compliance with the IPsecv3 protocol per RFC 4106 and is to be used in the context of the AES GCM mode within the IPsec-v3 protocol alone. The module uses RFC 7296-compliant IKEv2 to establish the shared secret SKEYSEED from which the AES GCM encryption keys are derived. Per requirements of IPSec-v3, the IV is constituted of 32-bits of salt followed by 64-bits of the deterministic nonce. The last 64 bits of the IV are deterministically constructed using an incremental counter. When the nonce portion of the IV exhausts the maximum number of possible values for a given security association, either party to the security association that encounters this condition triggers a rekeying with IKEv2 to establish a new encryption key for the security association per RFC 7296. In the event that the module's power is lost and then restored, a new key for use with the AES GCM encryption/decryption is established.

Destruction and Zeroization

The module will remain installed for the lifetime of the operating system. When the operating system is removed, the module will be erased. Any SSPs in the module will be erased at that time.

12. Mitigation of other attacks

The module does not implement mitigation of other attacks.

Acronyms

Table 8 - 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
CVL	Component Validation List
DRBG	Deterministic Random Bit Generation
FIPS	Federal Information Processing Standard
HMAC	(Keyed-)Hash Messages Authentication Code
KAT	Known Answer Test
MAC	Message Authentication Code
NIST	National Institute of Standards and Technology
OE	Operational Environment
OS	Operation System
POST	Power-On Self-Test
SHA	Secure hash Standard
SSP	Sensitive Security Parameter
SP	Special Publication