VMware, Inc.

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

VMware's OpenSSL FIPS Object Module

Software Version: 2.0.20-vmw

FIPS 140-2 Non-Proprietary Security Policy

FIPS Security Level: 1
Document Version: 0.8

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 OpenSSL FIPS Object Module from VMware, Inc. This Security Policy describes how the VMware's OpenSSL FIPS Object 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 of Cyber Security (CCCS) 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. The VMware's OpenSSL FIPS Object Module is also referred to in this document as “the module”.

1.2 Reference

This document deals only with operations and capabilities of the composite 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 (http://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.

2 VMWARE OPENSSL FIPS OBJECT MODULE

2.1 Introduction

VMware, Inc., a global leader in virtualization, cloud infrastructure, and business mobility, delivers customer-proven solutions that accelerate Information Technology (IT) by reducing complexity and enabling more flexible, agile service delivery. With VMware solutions, organizations are creating exceptional experiences by mobilizing everything, responding faster to opportunities with modern data and apps hosted across hybrid clouds, and safeguarding customer trust with a defense-in-depth approach to cybersecurity. VMware enables enterprises to adopt an IT model that addresses their unique business challenges. VMware's approach accelerates the transition to solutional-computing while preserving existing investments and improving security and control.

2.1.1 VMware OpenSSL FIPS Object Module

The VMware's OpenSSL FIPS Object Module is a software cryptographic module that is built from the OpenSSL FIPS Object Module source code according to the instructions prescribed in Appendix A. The module is a software library that provides cryptographic functions to various VMware applications via a well-defined C-language application program interface (API). The module only performs communications with the calling application (the process that invokes the module services).

The VMware's OpenSSL FIPS Object Module is validated at the FIPS 140-2 Section levels shown in Table 1:

Table 1 – 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	2
4	Finite State Model	1
5	Physical Security	N/A[1]
6	Operational Environment	1
7	Cryptographic Key Management	1
8	EMI/EMC[2]	1
9	Self-tests	1
10	Design Assurance	3
11	Mitigation of Other Attacks	N/A

2.2 Module Specification

The VMware's OpenSSL FIPS Object Module is a software cryptographic module with a multiple-chip standalone embodiment. The overall security level of the module is 1. The software version of the module is 2.0.20-vmw, and it is developed and built from the 2.0.16 version of the OpenSSL FIPS Object Module source code.

[1] N/A – Not Applicable

[2] EMI/EMC – Electromagnetic Interference/Electromagnetic Compatibility

2.2.1 Physical Cryptographic Boundary

As a software module, there are no physical protection mechanisms implemented. Therefore, the module must rely on the physical characteristics of the host system. The module runs on a General-Purpose Computer (GPC) and 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 GPC. See Figure 1 below for a block diagram of the typical GPC and its physical cryptographic boundary marked with red dotted line.

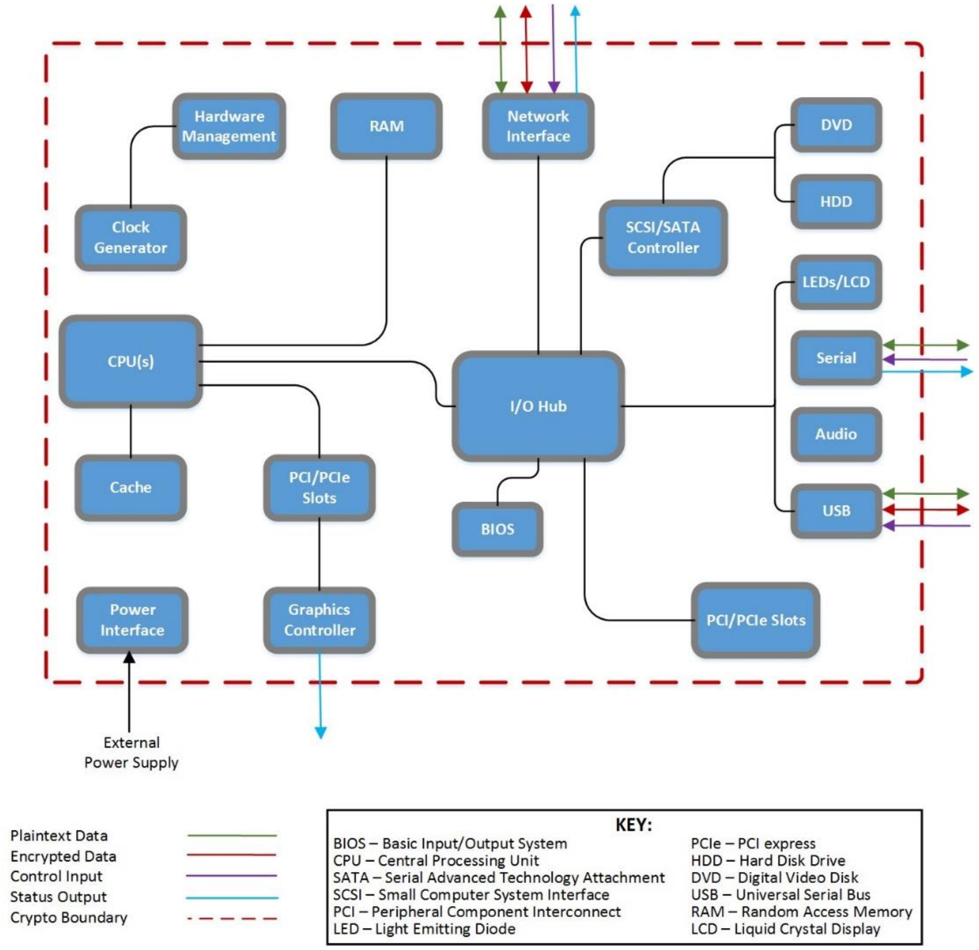

Figure 1 – Hardware Block Diagram

2.2.2 Logical Cryptographic Boundary

The logical cryptographic boundary of the module is the fipscanister object module, a single object module file named *fipscanister.o* (Linux®[3]). Figure 2 and Figure 3 depict the logical cryptographic boundary for the module which surrounds the VMware's OpenSSL FIPS Object 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.

[3] Linux is the registered trademark of Linus Torvalds in the U.S. and other countries.

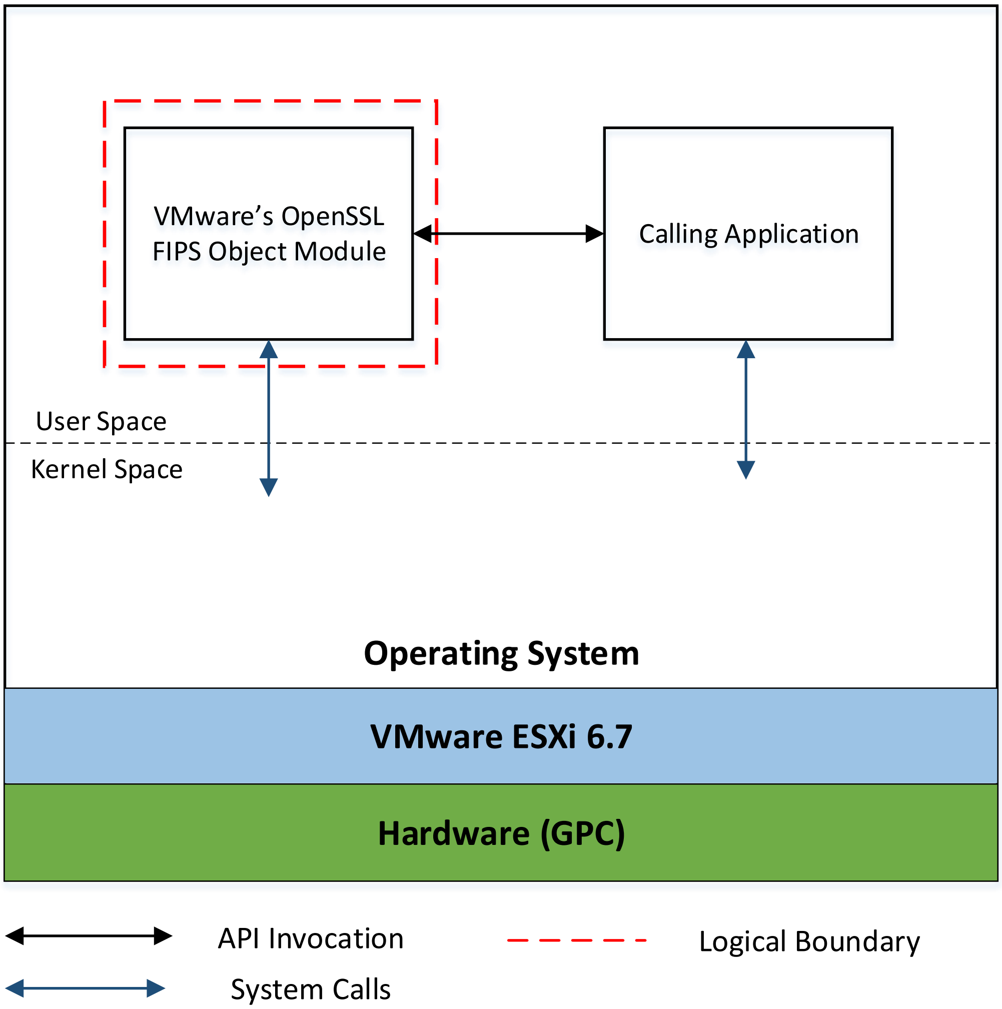

Figure 2 – Module's Logical Cryptographic Boundary in Guest OS

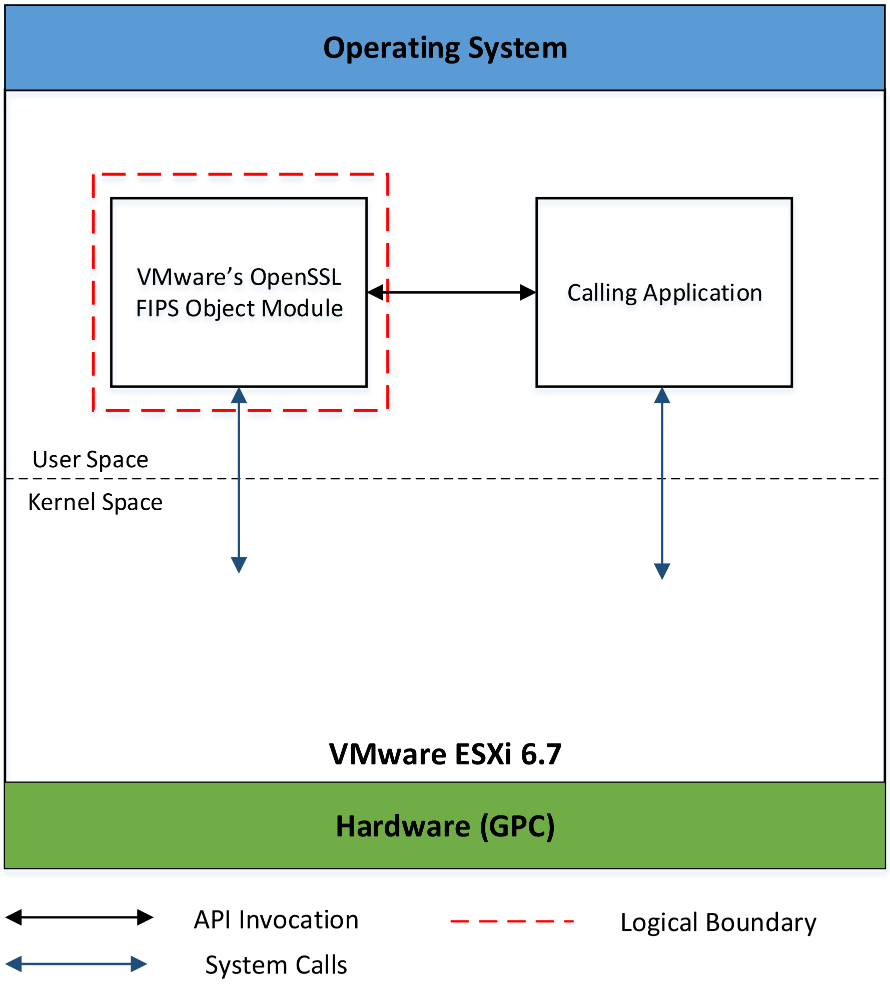

Figure 3 – Module’s Logical Cryptographic Boundary in Hypervisor

2.2.3 Cryptographic Implementation and modes of operation

The module implements the FIPS-Approved algorithms listed in Table 2 below.

Table 2 – FIPS-Approved Algorithm Implementations

Function	Algorithm	Options	Cert #
Random Number Generation; Symmetric Key Generation	[SP 800-90A] DRBG[4]	Hash DRBG (Prediction resistance supported) HMAC DRBG, no reseed CTR DRBG (AES), no derivation function (Prediction resistance supported)	C 470

[4] For all DRBGs the “supported security strength” is just the highest supported security strength per [SP 800-90A] and [SP 800-57].

Encryption, Decryption and CMAC	[SP 800-67]	3-Key TDES TECB, TCBC, TCFB 1, TCFB 8, TCFB 64, TOFB; CMAC generate and verify	C 470
	[FIPS 197] AES [SP 800-38A] ECB, CBC, CFB, OFB, CTR [SP 800-38B] CMAC [SP 800-38C] CCM [SP 800-38D] GCM [SP 800-38E] XTS	128/ 192/256 ECB, CBC, OFB, CFB 1, CFB 8, CFB 128, CTR; CCM; GCM; CMAC generate and verify; XTS (128 and 256 only)	C 470
Message Digests	[FIPS 180-4]	SHA-1, SHA-2 (224, 256, 384, 512)	C 470
Keyed Hash	[FIPS 198] HMAC	HMAC with SHA-1, SHA-2 (224, 256, 384, 512)	C 470
Digital Signature and Asymmetric Key Generation	[FIPS 186-2] RSA	SigVer9.31 (1024/1536/2048/3072/4096 with SHA-1, 256, 384, 512)	C 470
		SigVerPKCS1.5 (1024/1536/2048/3072/4096 with SHA-1, 256, 384, 512)	
		SigVerPSS (1024/1536/2048/3072/4096 with SHA-1, 256, 384, 512)	
	[FIPS 186-4] RSA	GenKey9.31 (2048/3072)	
		SigGen9.31 (2048/3072 with SHA-256, 384, 512)	
		SigGenPSS (2048/3072 with SHA-256, 384, 512)	
		SigGenPKCS1.5 (2048/3072 with SHA-256, 384, 512)	
		SigVer9.31 (2048/3072 with SHA-1, 256, 384, 512)	
		SigVerPSS (2048/3072 with SHA-1, 256, 384, 512)	
		SigVerPKCS1.5 (2048/3072 with SHA-1, 256, 384, 512)	
	[FIPS 186-4] DSA	PQG Gen (2048, 224 with SHA-224, 256, 384, 512; 2048, 256 with SHA-256, 384, 512; 3072, 256 with SHA-256, 384, 512)	C 470
		PQG Ver (1024, 160 with SHA-1, 224, 256, 384, 512; 2048, 224 with SHA-224, 256, 384, 512; 2048, 256 with SHA-256, 384, 512; 3072,256 with SHA-256, 384, 512)	
		KeyPairGen (2048, 224; 2048, 256; 3072, 256)	
		SigGen (2048, 224 with SHA-224, 256, 384, 512; 2048, 256 with SHA-224, 256, 384, 512; 3072, 256 with SHA-224, 256, 384, 512)	
		SigVer (1024/2048/3072 with SHA-1, 224, 256, 384, 512)	

	[FIPS 186-4] ECDSA	PKG: CURVES (P-224 P-256 P-384 P-521 K-233 K- 283 K-409 K-571 B-233 B-283 B-409 B-571 ExtraRandomBits TestingCandidates)	C 470
		PKV: CURVES (ALL-P ALL-K ALL-B)	
		SigGen: CURVES(P-224: (SHA-224, 256, 384, 512) P-256: (SHA-224, 256, 384, 512) P-384: (SHA-224, 256, 384, 512) P-521: (SHA-224, 256, 384, 512) K-233: (SHA-224, 256, 384, 512) K-283: (SHA-224, 256, 384, 512) K-409: (SHA-224, 256, 384, 512) K-571: (SHA-224, 256, 384, 512) B-233: (SHA-224, 256, 384, 512) B-283: (SHA-224, 256, 384, 512) B-409: (SHA-224, 256, 384, 512) B-571: (SHA-224, 256, 384, 512))	
		SigVer: CURVES(P-192: (SHA-1, 224, 256, 384, 512) P-224: (SHA-1, 224, 256, 384, 512) P-256: (SHA-1, 224, 256, 384, 512) P-384: (SHA-1, 224, 256, 384, 512) P-521: (SHA-1, 224, 256, 384, 512) K-163: (SHA-1, 224, 256, 384, 512) K-233: (SHA-1, 224, 256, 384, 512) K-283: (SHA-1, 224, 256, 384, 512) K-409: (SHA-1, 224, 256, 384, 512) K-571: (SHA-1, 224, 256, 384, 512) B-163: (SHA-1, 224, 256, 384, 512) B-233: (SHA-1, 224, 256, 384, 512) B-283: (SHA-1, 224, 256, 384, 512) B-409: (SHA-1, 224, 256, 384, 512) B-571: (SHA-1, 224, 256, 384, 512))	
ECC CDH (CVL)	[SP 800-56A] (§5.7.1.2)	All NIST defined B, K and P curves except sizes 163 and 192	C 470
FCC KAS	[SP 800-56A] All except KDF	Parameter Sets/Key sizes: FB (SHA-256), FC (SHA-256)	C 470
ECC KAS	[SP 800-56A] All except KDF	Parameter Sets/Key sizes: EC (P-256, SHA-256), ED (P-384, SHA-512), EE (P-521, SHA-512)	C 470

Per IG A.5 Scenario 2, the module generates random IVs of 96 bits or higher using the SP 800-90A DRBG and in the event Module power is lost and restored the calling application must ensure that any AES-GCM keys used for encryption or decryption are re-distributed

The module supports only NIST defined curves for use with ECDSA and ECC CDH. The module supports two operational environments configurations for elliptical curves; NIST prime curve only and all NIST defined PKB curves.

The module also employs the following key establishment methodologies, which are allowed or vendor affirmed to be used in FIPS-Approved mode of operation:

- RSA (key wrapping[5]; key establishment methodology provides between 112 and 256 bits of encryption strength)
- EC DH (CVL Cert. #C470, key agreement[6]; key establishment methodology provides between 112

[5] No claim is made for SP 800-56B compliance, and no CSPs are established into or exported out of the module using this service.

[6] Vendor Affirmed DH scheme using NIST defined P elliptical curve. Key agreement is a service provided for calling process use, but is not used to establish keys into the module. Vendor Affirmed IG D.1- rev2.

and 256 bits of encryption strength)

- CKG (vendor affirmed)
- KAS (SP 800-56Arev2; vendor affirmed)
- Entropy Input: The Module supports NDRNG as a non-Approved algorithm but allowed in FIPS Approved mode.

In accordance with FIPS 140-2 IG D.12, the cryptographic module performs Cryptographic Key Generation (CKG) as per SP800-133 (vendor affirmed). The resulting generated symmetric key and the seed used in the asymmetric key generation are the unmodified output from SP800-90A DRBG

The module employs non-compliant algorithms and associated services, which are not allowed for use in a FIPS-Approved mode of operation. Their use will result in the module operating in a non-Approved mode.

Please refer to Table 3 below for the list of non-Approved algorithms and associated services.

Table 3 – Non FIPS-Approved Algorithm Implementations and services

Algorithm	Options	Description
ANSI X9.31 PRNG	AES 128/192/256	Random Number Generation; Symmetric Key Generation
SP 800-90A Dual_EC_DRBG	Dual EC DRBG	Random Number Generation; Symmetric Key Generation
RSA (FIPS 186-2)	KeyGen9.31, SigGen9.31, SigGenPKCS1.5, SigGenPSS (1024/1536 with all SHAs, 2048/3072/4096 with SHA-1)	Digital Signature Generation and Asymmetric Key Generation
DSA (FIPS 186-2)	PQG Gen, Key Pair Gen, SigGen (1024 with all SHAs, 2048/3072 with SHA-1)	Digital Signature Generation and Asymmetric Key Generation
DSA (FIPS 186-4)	PQG Gen, Key Pair Gen, SigGen (1024 with all SHAs, 2048/3072 with SHA-1)	Digital Signature Generation and Asymmetric Key Generation
ECDSA (FIPS 186-2)	PKG: Curve (P-192 K-163 B-163) SIG (gen): Curve (P-192 P-224 P-256 P-384 P-521 K-163 K-233 K-283 K-409 K-571 B-163 B-233 B-283 B-409 B-571)	Digital Signature Generation and Asymmetric Key Generation
ECDSA (FIPS 186-4)	PKG: Curve (P-192 K-163 B-163) SigGen: Curve (P-192: (SHA-1, 224, 256, 384, 512) P-224:(SHA-1) P-256:(SHA-1) P-384: (SHA-1) P-521:(SHA-1) K-163: (SHA-1, 224, 256, 384, 512) K-233:(SHA-1) K-283:(SHA-1) K-409:(SHA-1) K-571:(SHA-1) B-163: (SHA-1, 224, 256, 384, 512) B-233: (SHA-1) B-283: (SHA-1) B-409:(SHA-1) B-571:(SHA-1))	Digital Signature Generation and Asymmetric Key Generation
ECC CDH (KAS, SP800-56A – 5.7.1.2)	All NIST recommended P, K, and B with Curves 163 and 192	Key Agreement Scheme

The Module is a cryptographic engine library, which can be used only in conjunction with additional software. Aside from the use of the NIST defined elliptic curves as trusted third-party domain parameters, all other FIPS 186-4 assurances are outside the scope of the module, and are the responsibility of the calling process.

2.3 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
- Power input

As a software module, the module's manual controls, physical indicators, and physical and electrical characteristics are those of the host platform. A mapping of the FIPS 140-2 logical interfaces, the physical interfaces, and the module interfaces can be found in Table 4 below.

Table 4 – FIPS 140-2 Logical Interface Mapping

FIPS Interface	Physical Interface	Module Interface (API)
Data Input	Network port, Serial port, USB port, SCSI/SATA Controller	The function calls that accept input data for processing through their arguments.
Data Output	Network port, Serial port, USB port, SCSI/SATA Controller	The function calls that return by means of their return codes or argument generated or processed data back to the caller.
Control Input	Network port, Serial port, USB port, Power button	The function calls that are used to initialize and control the operation of the module.
Status Output	Network port, Serial port, USB port, Graphics controller	Return values for function calls; Module generated error messages.
Power Input	AC Power socket	Not applicable.

As a software module, control of the physical ports is outside module scope. However, when the module is performing self-tests, or is in error state, all output on the logical data output interface is inhibited. The module is single-threaded and in error states returns only an error value, and no data output is returned.

2.4 Roles and Services

There are two roles in the module (as required by FIPS 140-2) that operators may assume: a Crypto Officer (CO) role and a User role. The module implements Role-based authentication of the operators. Roles are assumed implicitly by passing the appropriate password to the *FIPS_module_mode_set()* function. The password values may be specified at build time and must have a minimum length of 16 characters. Any attempt to authenticate with an invalid password will result in an immediate and permanent failure condition rendering the module unable to enter the FIPS mode of operation, even with subsequent use of a correct password. Authentication data is loaded into the module during the module build process, performed by the Crypto Officer, and otherwise cannot be accessed.

Since the minimum password length is 16 characters, the probability of a random successful authentication attempt in one try is 95^{16} (if all characters are available for the password). The module permanently disables further authentication attempts after a single failure and remains disabled until it is reloaded and reinitialized, so this probability is independent of time.

Only one role may be active at a time and the module does not allow concurrent operators. 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 5 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.

2.4.1 Crypto Officer and User Roles

The CO and User roles share many services. Both roles have access to all of the services provided by the module.

- Crypto Officer Role: Installation of the Module on the host computer system and calling of any API functions.
- User Role: Loading of the module and calling any of the API functions.

Below, Table 5 describes the CO and User services and CSP access, while Table 3 in Section 2.2.3 above describes the Non-Approved algorithms and services.

Table 5 – Crypto Officer and Users Services

Role	Service	Description	CSP and Type of Access
CO, User	Initialization of the module	Initialization of the module following the Secure Operation section of the Security Policy	None
CO, User	Run self-test	Runs Self-tests on demand during module operation	None
CO, User	Show status	Returns the current mode (Boolean) of operation of the module, and version (as unsigned long or const char*)	None
CO, User	Zeroize	Zeroizes all CSPs	All CSPs - W
CO, User	Random number generation	Generate random number and symmetric key by using the DRBGs	DRBGs CSPs – RXW
CO, User	Asymmetric key generation	Generate RSA, DSA, and ECDSA key pairs	RSA SGK – W RSA SVK – W DSA SGK – W DSA SVK – W ECDSA SGK – W ECDSA SVK – W
CO, User	Symmetric Encryption/Decryption	Encrypt or decrypt data using supplied key and algorithm specification (key passed in by the calling process)	AES EDK – RX Triple-DES EDK – RX

CO, User	Symmetric digest (CMAC)	Generate or verify data integrity using CMAC with AES or TDES (key passed in by the calling process)	AES CMAC – RX Triple-DES CMAC – RX
CO, User	Hash generation	Compute and return a message digest using SHA algorithm	None
CO, User	Message Authentication Code generation (HMAC)	Compute and return a hashed message authentication code	HMAC Key – RX
CO, User	Transport[7] key	Wrap/unwrap a key on behalf of the calling application but does not establish keys into the module (key passed in by the calling process)	RSA KEK – RX RSA KDK – RX
CO, User	Key agreement	Perform key agreement primitives on behalf of the calling process but does not establish keys into the module (keys passed in by the calling process)	EC DH Private/Public Key – RX
CO, User	Digital signature	Generate and verify RSA, DSA, and ECDSA digital signatures (keys passed in by the calling process)	RSA SGK – RX RSA SVK – RX DSA SGK – RX DSA SVK – RX ECDSA SGK – RX ECDSA SVK – RX
CO, User	Utility	Miscellaneous helper functions	None

2.5 Physical Security

The VMware's OpenSSL FIPS Object Module is a software module, which FIPS defines as a multi-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.

2.6 Operational Environment

The module was tested and found to be compliant with FIPS 140-2 requirements on the following platforms:

- A Dell PowerEdge R740 with an Intel Xeon Gold 6126 processor running Ubuntu 16.04, PhotonOS 2.0, PhotonOS 1.0, or VMware SD-WAN OS 3.3 on VMware ESXi 6.7.
- A Dell PowerEdge R740 with an Intel Xeon Gold 6126 processor running VMware ESXi 6.7.
- A VMware SD-WAN Edge 610 with an Intel Atom C3308 processor running VMware SD-WAN OS

[7] "Key transport" can refer to a) moving keys in and out of the module or b) the use of keys by an external application. The latter definition is the one that applies to the VMware OpenSSL FIPS Object Module.

3.3

- A VMware SD-WAN Edge 3800 with an Intel Xeon D-2187NT processor running VMware SD-WAN OS 3.3

Further, VMware, Inc. affirms that the VMware's OpenSSL FIPS Object Module runs in its configured, Approved mode of operation on the following binary compatible platforms executing VMware ESXi 6.0, ESXi 6.5, ESXi 6.7, ESXi 7.0, or without ESXi with any of the above listed OS:

- Dell PowerEdge T320, R530, R730, and R830 with Intel Xeon Processor
- Dell PowerEdge R740 Gen14 with Intel Xeon Processor
- Dell PowerEdge R740 Gen 14 with Intel Xeon Gold 61xx series Processor
- HPE ProLiant DL380 Gen9 with Intel Xeon Processor
- HPE ProLiant DL38P Gen8 with AMD Opteron Processor
- Cisco UCS – B22 M Series Blade Servers with Intel Processor
- Cisco UCS – C24 M3 Series Rackmount with Intel Xeon Processor
- A general-purpose computer platform with an Intel Core I, Intel Xeon, or AMD Opteron Processor executing VMware ESXi and any OS (including Apple OS (OS X, macOS, iOS), Android OS, OpenWrt, and others) with single user mode.
- A cloud computing environment composed of a general-purpose computing platform executing VMware ESXi or a VMware cloud solution that is executing VMware ESXi.

VMware also affirms that the module runs in it configured Approved mode of operation on the following binary compatible platforms executing VMware SD-WAN OS:

- VMware SD-WAN Edge 510
- VMware SD-WAN Edge 510-LTE-NAM-EMEA
- VMware SD-WAN Edge 510-LTE-APAC
- VMware SD-WAN Edge 520
- VMware SD-WAN Edge 520v
- VMware SD-WAN Edge 540
- VMware SD-WAN Edge 840
- VMware SD-WAN Edge 2000
- VMware SD-WAN Edge 620
- VMware SD-WAN Edge 640
- VMware SD-WAN Edge 680
- VMware SD-WAN Edge 3400
- VMware SD-WAN Virtual Edge

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. No assurance of the minimum strength of generated keys.

In addition to its full AES software implementations, the VMware OpenSSL FIPS Object Module is capable of leveraging the AES-NI instruction set of supported Intel and AMD processors in order to accelerate AES calculations.

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.

The tested operating systems segregate user processes into separate process spaces. Each process space is logically separated from all other processes by the operating system software and hardware. The Module functions entirely within the process space of the calling application, and implicitly satisfies the FIPS

140-2 requirement for a single user mode of operation.

2.7 Cryptographic Key Management

The module supports the CSPs listed below in Table 6 and Table 7.

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

CSP Name	Description
RSA SGK	RSA (2048 to 16384 bits) signature generation key
RSA KDK	RSA (2048 to 16384 bits) key decryption (private key transport) key
DSA SGK	[FIPS 186-4] DSA (2048/3072) signature generation key
ECDSA SGK	ECDSA (All NIST defined B, K, and P curves except B=163, K=163, and P=192) signature generation key
EC DH Private	EC DH (All NIST defined B, K, and P curves except B=163, K=163, and P=192) private key agreement key
AES EDK	AES (128/192/256) encrypt / decrypt key
AES CMAC	AES (128/192/256) CMAC generate / verify key
AES GCM	AES (128/192/256) encrypt / decrypt / generate / verify key
AES XTS	AES (256/512) XTS encrypt / decrypt key
TDES EDK	TDES (3-Key) encrypt / decrypt key
TDES CMAC	TDES (3-Key) CMAC generate / verify key
HMAC Key	Keyed hash key (160/224/256/384/512)
Hash_DRBG CSPs	V (440/888 bits) and C (440/888 bits), NDRNG (entropy input: length dependent on security strength)
HMAC_DRBG CSPs	V (160/224/256/384/512 bits) and Key (160/224/256/384/512 bits), NDRNG (entropy input: length dependent on security strength)
CTR_DRBG CSPs	V (128 bits) and Key (AES 128/192/256), NDRNG (entropy input: length dependent on security strength)
CO-AD-Digest	Pre-calculated HMAC SHA-1 digest used for Crypto Officer role authentication
User-AD-Digest	Pre-calculated HMAC SHA-1 digest used for User role authentication

The RSA generation is consistent with Table B.1 of FIPS 186-4 per IG A.14.

Authentication data is loaded into the module during the module build process, performed by an authorized operator (Crypto Officer), and otherwise cannot be accessed.

The module does not output intermediate key generation values.

Table 7 – List of Public Keys, Key Components, and CSPs

CSP Name	Description
RSA SVK	RSA (1024 to 16384 bits) signature verification key
RSA KEK	RSA (1024 to 16384 bits) key encryption (public key transport) key
DSA SVK	[FIPS 186-4] DSA (1024/2048/3072) signature verification key or [FIPS 186-2] DSA (1024) signature verification key
ECDSA SVK	ECDSA (All NIST defined B, K, and P curves) signature verification key
EC DH Public	EC DH (All NIST defined B, K, and P curves) public key agreement key

For all CSPs and Public Keys:

Storage: RAM, associated to entities by memory location. The module stores DRBG state values for the lifetime of the DRBG instance. The module uses CSPs passed in by the calling application on the stack. The module does not store any CSP persistently (beyond the lifetime of an API call), with the exception of DRBG state values used for the modules' default key generation service.

Generation: The module implements 800-90A compliant DRBG services for creation of symmetric keys, and for generation of DSA, elliptic curve, and RSA keys as shown in Table 2. The calling application is responsible for storage of generated keys returned by the module. The NDRNG provides 256 bits of entropy to the DRBG.

Entry: All CSPs enter the module's logical boundary in plaintext as API parameters, associated by memory location. However, none cross the physical boundary.

Output: The module does not output CSPs, other than as explicit results of key generation services. However, none cross the physical boundary.

Destruction: Zeroization of sensitive data is performed automatically by API function calls for temporarily stored CSPs. In addition, the module provides functions to explicitly destroy CSPs related to random number generation services. The calling application is responsible for parameters passed in and out of the module.

Private and secret keys as well as seeds and entropy input are provided to the Module by the calling application, and are destroyed when released by the appropriate API function calls. Keys residing in internally allocated data structures (during the lifetime of an API call) can only be accessed using the module defined API. The operating system protects memory and process space from unauthorized access. Only the calling application that creates or imports keys can use or export such keys. All API functions are executed by the invoking calling application in a non-overlapping sequence such that no two API functions will execute concurrently. An authorized application as user (Crypto Officer and User) has access to all key data generated during the operation of the module.

In the event module power is lost and restored the calling application must ensure that any AES-GCM keys used for encryption or decryption are redistributed.

Module users (the calling applications) shall use entropy sources that meet the security strength required for the random number generation mechanism as shown in [SP 800-90A] Table 2 (Hash_DRBG, HMAC_DRBG) and Table 3 (CTR_DRBG). This entropy is supplied by means of callback functions. Those functions must return an error if the minimum entropy strength cannot be met.

2.8 Self-Tests

Cryptographic self-tests are performed by the module on invocation of Initialize or Self-test, as well as when the module is operating in the FIPS-Approved mode and when a random number is generated, or asymmetric keys are generated. The following sections list the self-tests performed by the module, their expected error status, and any error resolutions.

2.8.1 Power-Up Self-Tests

The Module performs the self-tests listed below on invocation of Initialize or Self-test.

The VMware's OpenSSL FIPS Object Module performs the following Power-up Self-tests:

- Software integrity check (HMAC SHA-1 Integrity Test)
- Known Answer Tests (KATs)
  - AES Encryption KAT in ECB mode with 128-bit key
  - AES Decryption KAT in ECB mode with 128-bit key
  - AES CCM Encryption KAT with 192-bit key
  - AES CCM Decryption KAT with 192-bit key
  - AES GCM Encryption KAT with 256-bit key
  - AES GCM Decryption KAT with 256-bit key
  - XTS-AES KAT with 128, 256-bit key sizes to support either 256-bit key size (for XTS-AES-128) or the 512-bit key size (for XTS-AES-256)
  - AES CMAC Sign KAT with 128, 192, 256-bit keys
  - AES CMAC Verify KAT with 128, 192, 256-bit keys
  - Triple-DES Encryption KAT in ECB mode with 3-Key
  - Triple-DES Decryption KAT in ECB mode with 3-Key
  - Triple-DES CMAC Generate KAT in CBC mode with 3-Key
  - Triple-DES CMAC Verify KAT in CBC mode with 3-Key
  - HMAC SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 KATs (Per IG 9.3, this testing covers SHA POST requirements)
  - RSA (PKCS#1) Signature Generation KAT using 2048-bit key and SHA-256
  - RSA (PKCS#1) Signature Verification KAT using 2048-bit key and SHA-256
  - DSA Signature Generation KAT using 2048-bit key and SHA-384
  - DSA Signature Verification KAT using 2048-bit key and SHA-384
  - CTR_DRBG KAT with AES 256-bit key and with and without derivation function
  - HASH_DRBG KAT with SHA-256
  - HMAC_DRBG KAT with SHA-256
  - ECDSA Pairwise Consistency Test (KeyGen, Sign, Verify using P-224, K-233 and SHA-512)
  - ECC CDH KAT (Shared secret calculation per SP 800-56A, 5.7.1.2, IG 9.6)
  - FFC DH KAT (Shared secret calculation per SP 800-56A, 5.7.1.1, IG 9.6)

The module is installed using one of the set of instructions in Appendix A, as appropriate for the target system. The HMAC SHA-1 of the module distribution file as tested by the CMT Laboratory and listed in Appendix A is verified during installation of the module file as described in Appendix A.

The module performs all power-up self-tests listed above through a constructor routine with no operator intervention required.
If any component of the power-up self-test fails an internal flag is set to prevent subsequent invocation of any cryptographic function calls. The module will only enter the FIPS Approved mode if the module is reloaded and the call to the constructor succeeds.

The power-up self-tests may also be performed on-demand by calling FIPS_selftest(), which returns a “1” for success and “0” for failure. Interpretation of this return code is the responsibility of the calling application.

2.8.2 Conditional Self-Tests

The module also implements the following conditional self-tests:

- DRBG Continuous RNG Test for stuck fault
- DRBG Health Tests as required by Section 11 of SP 800-90A
- NDRNG Continuous RNG Test for stuck fault
- DSA Pairwise Consistency Test on each key pair generation
- ECDSA Pairwise Consistency Test on each key pair generation
- RSA Pairwise Consistency Test on each key pair generation
- Non-identical keys Test for XTS-AES per IG A.9

In the event of a DRBG self-test failure the calling application must uninstantiate and reinstantiate the DRBG per the requirements of [SP 800-90A]; this is not something the module can do itself.

Pairwise consistency tests are performed for both possible modes of use, e.g. Sign/Verify and Encrypt/Decrypt.

2.9 Mitigation of Other Attacks

This section is not applicable. The module was not designed to mitigate any attacks beyond the FIPS 140-2 Level 1 requirements for this validation.

3 Secure Operation

The VMware's OpenSSL FIPS Object Module meets Level 1 requirements for FIPS 140-2. The sections below describe how to install, use, and keep the module in FIPS-Approved mode of operation.

3.1 Secure Distribution and Operation

The VMware’s OpenSSL FIPS Object Module is designed for use by the VMware’s applications and as such is not accessible to unauthorized personnel outside the VMware.

The HMAC fingerprint of the FIPS validated distribution file are:

580a5a6badbf8b6dbac386a12e4e2d184cc5f66d (64-bit), and

85c37f3ef1902363e1fdd10cbbcf9a112d09296c (32-bit)

When the module is loaded and is being initialized, the module automatically starts performing Power-On Self-Tests and completed the self-tests without any user intervention. On successful completion of the self-tests, the module operates in FIPS-Approved mode of operation. In FIPS mode, the module provided only FIPS-Approved algorithms, key sizes, and functions to the calling applications.

3.1.1 Crypto Officer Guidance

VMware application contains the FIPS 140-2 validated VMware’s OpenSSL FIPS Object Module. There are not additional steps, beyond installing the application, that must be performed to use the module correctly.

3.1.2 User Guidance

The User or API functions calls should be designed to deal with the identified error cases of the VMware's VPN Crypto Module.

The user is responsible for ensuring the module’s compliance with IG A.13 regarding the maximum number of encryptions permitted with the same Triple-DES key.

Per IG A.5 the module generates random IVs of 96 bits or higher using the SP 800-90A DRBG and in the event Module power is lost and restored the calling application must ensure that any AES-GCM keys used for encryption or decryption are re-distributed.

When transitioning between an approved and non-approved service, the module needs to be reinitialized to ensure no keys or CSP are shared between the services.

There are no additional user guidance instructions for correct operation of the module.

4 Acronyms

Table 8 provides definitions for the acronyms used in this document.

Table 8 – Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
AES-NI	Advanced Encryption Standard – New Instructions
AKA	Also Known As
AMD	Advanced Micro Devices
ANSI	American National Standards Institute
API	Application Programming Interface
BIOS	Basic Input/Output System
CBC	Cipher Block Chaining
CCM	Counter with CBC-MAC
CD	Compact Disc
CFB	Cipher Feedback
CMAC	Cipher-based Message Authentication Code
CMVP	Cryptographic Module Validation Program
CO	Crypto Officer
CPU	Central Processing Unit
CCCS	Canadian Centre for Cyber Security
CSP	Critical Security Parameter
CTR	Counter
DES	Data Encryption Standard
DRBG	Deterministic Random Bit Generator
DSA	Digital Signature Algorithm
DVD	Digital Video Disc
EC	Elliptical Curve
ECB	Electronic Code Book
ECC CDH	Elliptical Curve Cryptography Cofactor Diffie-Hellman
EC DH	Elliptical Curve Diffie-Hellman
ECDSA	Elliptical Curve Digital Signature Algorithm
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference

FIPS	Federal Information Processing Standard
GCM	Galois/Counter Mode
GPC	General Purpose Computer
HDD	Hard Disk Drive
HMAC	(Keyed) Hash Message Authenticating Code
IG	Implementation Guidance
IT	Information Technology
KAS	Key Agreement Scheme
KAT	Known Answer Test
LCD	Liquid Crystal Display
LED	Light Emitting Diode
N/A	Not Applicable
NIST	National Institute of Standards and Technology
OFB	Output Feedback
OS	Operating System
PCI	Peripheral Component Interconnect
PCIe	Peripheral Component Interconnect Express
PRNG	Pseudo Random Number Generator
RAM	Random Access Memory
RNG	Random Number Generator
RSA	Rivest, Shamir and Adleman
SATA	Serial Advanced Technology Attachment
SCSI	Small Computer System Interface
SHA	Secure Hash Algorithm
SLES	SUSE Linux Enterprise Server
SP	Special Publication
TCBC	Triple-DES Cipher Block Chaining
TCFB	Triple-DES Cipher Feedback
TDES	Triple-Data Encryption Standard
TECB	Triple-DES Electronic Code Book
TOFB	Triple-DES Output Feedback
USB	Universal Serial Bus
XTS	XEX-based Tweaked-Codebook mode with Ciphertext Stealing

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com