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

VMware VMkernel Cryptographic Module

Software Version: 1.0

FIPS 140-2 Non-Proprietary Security Policy

FIPS Security Level: 1
Document Version: 1.1

vmware

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 VMkernel Cryptographic Module from VMware, Inc. This Security Policy describes how the VMware VMkernel 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 Center 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 composite 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 VMkernel Cryptographic 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.

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 VMkernel Cryptographic 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.

2.2 Cryptographic Module Specification

VMware VMkernel Cryptographic Module is a software cryptographic module whose purpose is to provide FIPS 140-2 validated cryptographic functions to various VMware applications of the VMware ESXi kernel.

The Module is defined as a multi-chip standalone cryptographic module and has been validated at the FIPS 140-2 overall Security Level 1. Table 1 below describes the level achieved by the module in each of the eleven sections of the FIPS 140-2 requirements.

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	1
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	1
11	Mitigation of Other Attacks	N/A

[1] N/A – Not Applicable

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

The FIPS 140-2 operational testing was performed on the configurations presented in Table 2.

Table 2 – Tested Configurations

Operating System	Processor	Processor Optimization	Hardware Platform
VMware ESXi 6.7	Intel Xeon E5	None	Dell PowerEdge R830
VMware ESXi 6.7	Intel Xeon E5	AES-NI	Dell PowerEdge R830
VMware ESXi 6.7 U2	Intel Xeon Gold 6126	None	Dell PowerEdge R740
VMware ESXi 6.7 U2	Intel Xeon Gold 6126	AES-NI	Dell PowerEdge R740
VMware ESXi 7.0	Intel Xeon Gold 6126	None	Dell PowerEdge R740
VMware ESXi 7.0	Intel Xeon Gold 6126	AES-NI	Dell PowerEdge R740

In addition to its full AES software implementations, the VMware VMkernel Cryptographic Module is capable of leveraging the AES-NI[3] instruction set of the supported Intel processors in order to accelerate AES calculations.

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

2.2.1 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 host system consists of integrated circuits of the system board, processor, RAM, hard disk, device case, power supply, and fans. See Figure 1 below for a block diagram of the host system.

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

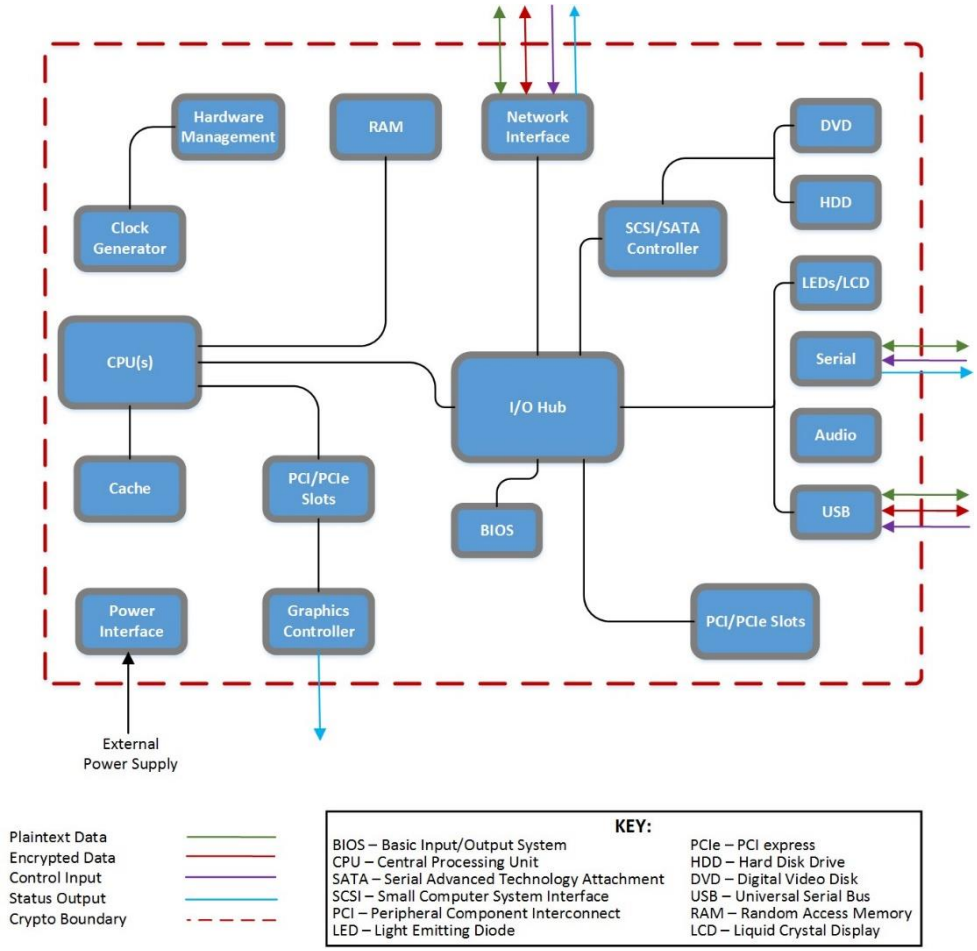


Figure 1 – Hardware Block Diagram

2.2.2 Logical Cryptographic Boundary

The logical cryptographic boundary for the VMware VMkernel Cryptographic Module is depicted in Figure 2. The VMware VMkernel Cryptographic Module boundary consists of one kernel object file, crypto_fips, and one application, cryptoLoader. The cryptoLoader is responsible for performing the integrity testing over both components and loading crypto_fips. The crypto_fips provides cryptographic services to the kernel components once the integrity tests and power-on self-tests have passed successfully.

The colored arrows, in Figure 2, indicate the logical information flows into and out of the module.

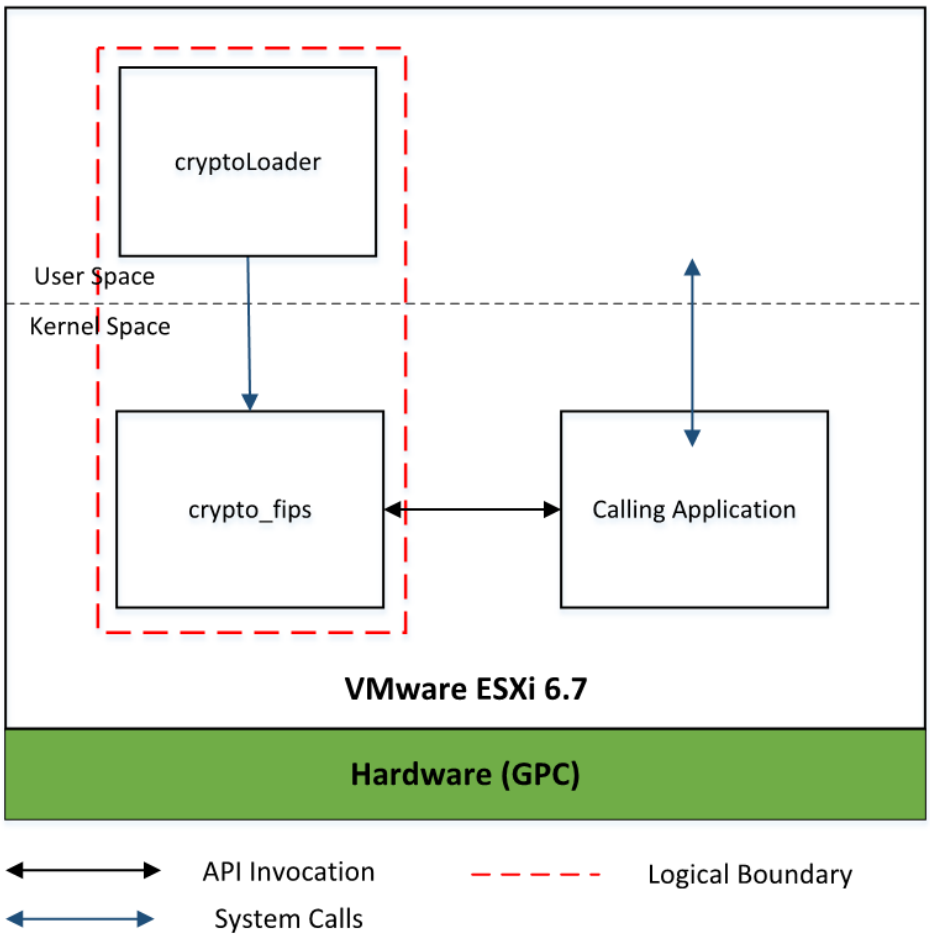


Figure 2 - Module's Logical Cryptographic Boundary

2.2.3 Modes of Operation

The VMware VMkernel Cryptographic Module only supports a FIPS-Approved mode of operation. The module must be configured as described in section 3.

Table 3 includes the FIPS-Approved algorithms for the cryptoLoader and Table 4 and Table 5 include the FIPS-Approved algorithms implemented in the crypto_fips.

Table 3 – FIPS-Approved Algorithm (cryptoLoader)

Algorithm	Implementation/Mode	Certificate Number
SHS	SHA-256	#3774, #C1171
HMAC	SHA-256	#3048, #C1171

Table 4 – FIPS-Approved Algorithms (crypto_fips)

Algorithm	Modes	Certificate Number
AES (128, 192, and 256-bit keys)	ECB, CBC, CTR (ext), GCM	#4531, #C1172
AES (128 and 256-bit keys)	XTS-AES-128, XTS-AES-256	#4531, #C1172
SHS	SHA-1, SHA-256, SHA-512	#3712, #C1172
DRBG	CTR_DRBG	#1488, #C1172
HMAC	SHA-1 and SHA-256,	#2989, #C1172

Table 5 – Vendor Affirmed Approved Functions (crypto_fips)

Algorithm	Modes	IG Reference
AES-CBC Ciphertext Stealing (CS) (128, 192, and 256-bit keys)	Mode: CBC-CS3	Vendor Affirmed IG A.3. Addendum to SP 800-38A, Oct 2010

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 defined interfaces and the logical interfaces of the module can be found in Table 6 below.

Table 6 – 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.
Power Input	Not applicable.

2.4 Roles, Services and Authentication

2.4.1 Roles

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. Each role and their corresponding services are detailed in the sections below. The User and Crypto-Officer roles are implicitly assumed by the entity accessing the module services. Please note that the keys and Critical Security Parameters (CSPs) listed in Table 7 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.

2.4.2 Services

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. Below, Table 7 describes the CO and User services.

Table 7 – Crypto Officer and Users Services

Role	Service	Description	CSP and Type of Access
CO, User	Encryption	Encrypt plaintext using supplied key and algorithm specification	AES Key – RX
CO, User	Decryption	Decrypt ciphertext using supplied key and algorithm specification	AES Key – RX
CO, User	Hashing	Compute and return a message digest using SHA algorithm	None
CO, User	Message Authentication Code generation	Compute and return a hashed message authentication code	HMAC Key – RX
CO, User	Random bit generation	Generate random bits by using the DRBG	DRBG CSPs – RXW
CO	Installation and initialization of the module	Installation and initialization of the module following the Secure Operation section of the Security Policy	None
CO	Show status	Returns the current mode of operation of the module	None
CO	Run Self-tests on demand	Runs Self-tests on demand during module operation	All CSPs – W
CO	Zeroization	Zeroizes all CSPs	All CSPs – W

2.4.3 Authentication

The module is a Level 1 software-only cryptographic module and does not implement authentication. Roles are assumed implicitly through the execution of either a CO or a User service.

2.5 Physical Security

The VMware VMkernel Cryptographic Module is a software module, which FIPS 140-2 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 a Dell PowerEdge R740 Server with an Intel Xeon Gold 6126 processor running VMware vSphere Hypervisor ESXi 6.7 U2 or ESXi 7.0

The module was also tested and found to be compliant with FIPS 140-2 requirements on a Dell PowerEdge R830 Server with an Intel Xeon E5 processor running VMware vSphere Hypervisor (ESXi) 6.7. The module only allows access to CSPs through its well-defined API.

Further, VMware, Inc. affirms that the VMware VMkernel Cryptographic Module runs in its configured, Approved mode of operation on the following binary compatible platforms executing ESXi 6.7, ESXi 6.7 U2, or ESXi 7.0:

- Dell PowerEdge T320 with Intel Xeon Processor
- Dell PowerEdge R530 with Intel Xeon Processor
- Dell PowerEdge R730 with Intel Xeon Processor
- Dell PowerEdge R830 with Intel Xeon Processor
- Dell PowerEdge T/R/Mx40 series with Intel Xeon 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

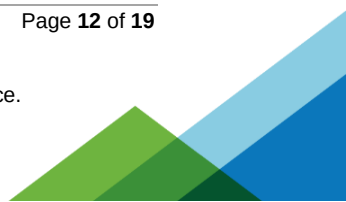
Further, VMware, Inc. affirms that the module also runs in its configured Approved mode of operation when the ESXi (6.7, 6.7 U2, or 7.0) is operated in Cloud (Private, Public, and Hybrid) itself and in Cloud solutions too.

No claim can be made as to the correct operation of the module and the security strength of keys when the module is ported to an operational environment that is not listed on the CMVP validation certificate.

In addition to its full AES software implementations, the VMware VMkernel Cryptographic 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 system segregates 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 8.

Table 8 – List of Cryptographic Keys, Key Components, and CSPs

Key/CSP	Key/CSP Description	Generation/Input	Output	Storage	Zeroization	Use
AES key	128, 192, 256-bit key	Input via API in plaintext	Output in plaintext via Tested Platform's INT Path	In RAM	Reboot OS; Cycle host power	Encryption, Decryption
AES XTS Key	128, 256-bit key	Input via API in plaintext	Output in plaintext via Tested Platform's INT Path	In RAM	Reboot OS; Cycle host power	Encryption, Decryption
HMAC key	112-bit key	Input via API in plaintext	Output in plaintext via Tested Platform's INT Path	In RAM	Reboot OS; Cycle host power	Message Authentication
DRBG seed	Seed used to derive the internal state of the DRBG.	Input via API in plaintext	Does not exit the module	In RAM	Reboot OS; Cycle host power	Random number generation
DRBG entropy	256-bits	Input via API in plaintext	Does not exit the module	In RAM	Reboot OS; Cycle host power	Random number generation
DRBG.InternalState_V	V (256-bits)	Generated Internally	Does not exit the module	In RAM	Reboot OS; Cycle host power	
DRBG.InternalState_Key	[Need Size]	Generated Internally	Does not exit the module	In RAM	Reboot OS; Cycle host power	

2.7.1 Key Generation

The Module implements a NIST SP 800-90A DRBG for the generation of random bits. The implementation of CTR_DRBG uses AES-256 (maximum of 256 bits of security strength) as the block cipher along with the appropriate derivation function. The cryptographic module is passed keys and CSPs as API parameters, associated by memory location. The application calling the cryptographic module passes keys and CSPs in plaintext within the physical boundary. Key Entry/Output.

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.

2.7.2 Zeroization

Keys and CSPs can be zeroized by rebooting the host hardware platform.

2.8 Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC)

The Dell PowerEdge R830 has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

2.9 Self-Tests

Cryptographic self-tests are performed by the module after initialization of the module, and on demand by power cycling the module. Conditional self-tests are also performed as specified by the FIPS 140-2 requirements. The following sections list the self-tests performed by the module, their expected error status, and any error resolutions.

Self-tests are health checks that ensure the cryptographic algorithms implemented within the module are operating correctly. The self-tests identified in FIPS 140-2 broadly fall within two categories:

1. Power-On Self-Tests
2. Conditional Self-Tests

2.9.1 Power-On Self-Tests

The module performs the required set of power-on self-tests. These self-tests are performed automatically by the module when the module is powered-up. The list of power-on self-tests that follows may also be run on-demand when the CO reboots the Operating System. The module will perform the listed power-on self-tests to successful completion. During the execution of self-tests, data output from the module is inhibited.

If any of the self-tests fail, the module will return an error code to the application that tried to load and initialize the module. The module will enter an error state and none of the module's services are available in the error state. In order to resolve a cryptographic self-test error, the module must be restarted by rebooting the OS. If the error persists, the module must be reinstalled.

- The VMware VMkernel Cryptographic Module performs the following power-On Self-Tests:

- Software integrity check
  - HMAC SHA-256

- Known Answer Tests (KATs)
  - AES 128 Encryption KAT: (ECB, CBC, CTR modes)
  - AES 128 Decryption KAT: (ECB, CBC, CTR modes)
  - AES GCM Encryption KAT
  - AES GCM Decryption KAT
  - AES XTS Encryption KAT
  - AES XTS Decryption KAT
  - SHA-512 KAT
  - HMAC SHA-1 and HMAC SHA-256 KAT (also test SHA-1 and SHA-256)
  - DRBG (CTR_DRBG) KAT

2.9.2 Conditional Self-Tests

The module implements the conditional self-tests identified below. If an error is encountered, the module will return an error and will remain in an error state. After entering the error state, all subsequent calls to the module will be rejected, ensuring that data output from the module is inhibited. In order to resolve a cryptographic self-test error, the module must be restarted by rebooting the OS. If the error persists, the module must be reinstalled.

The VMware VMkernel Cryptographic Module performs the following conditional self-tests:

- NIST SP 800-90A DRBG Health Tests; and
- Continuous Random Number Generation Test (CRNGT) on entropy input from NDRNG.
- Continuous Random Number Generation Test (CRNGT) on the DRBG.

2.10 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 VMkernel 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

3.1.1 VMware VMkernel Cryptographic Module Secure Operation

VMware ESXi 6.7, ESXi 6.7 U2, and ESXi 7.0 contain the FIPS 140-2 validated VMware VMkernel Cryptographic Module. There are no additional steps, beyond installing the base system, that must be performed to use the module correctly.

3.2 User Guidance

The User or API functions calls should be designed to deal with the identified error cases of the VMware VMkernel Cryptographic Module. There are no additional user guidance instructions for correct operation of the module.

4 ACRONYMS

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

Table 9 – Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
AES-NI	Advanced Encryption Standard – New Instructions
API	Application Programming Interface
CBC	Cipher Block Chaining
CMVP	Cryptographic Module Validation Program
CO	Crypto Officer
CRNGT	Continuous Random Number Generation Test
CSE	Communication Security Establishment
CSP	Critical Security Parameter
CTR	Counter
CS	Ciphertext Stealing
DRBG	Deterministic Random Bit Generator
ECB	Electronic Code Book
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FIPS	Federal Information Processing Standard
FCC	Federal Communications Commission
GCM	Galois/Counter Mode
HMAC	(Keyed) Hash Message Authenticating Code
INT	A validated Cryptographic Module which lies internal or inside of the boundary in regard to the reference diagram CM software physical boundary
IT	Information Technology
KAT	Known Answer Test
NDRNG	Non Deterministic Random Number Generator
NIST	National Institute of Standards and Technology
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
SP	Special Publication

XTS	XEX-based tweaked-codebook mode with ciphertext stealing (XTS)

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