VMware, Inc.

VMware Kernel Cryptographic Module

Software Version: 1.0

FIPS 140-2 Non-Proprietary Security Policy

FIPS Security Level: 1
Document Version: 1.0

Prepared for:

VMware, Inc.
3401 Hillview Ave
Palo Alto, CA 94304
United States of America

Phone: +1 (877) 486-9237
Email: info@vmware.com
http://www.vmware.com

Prepared by:

Corsec Security, Inc.
13135 Lee Jackson Memorial Hwy., Suite 220
Fairfax, VA 22033
United States of America

Phone: +1 (703) 267-6050
Email: info@corsec.com
http://www.corsec.com

Table of Contents

Table of Figures

List of Tables

1 Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the VMware Kernel Cryptographic Module from VMware, Inc. This Security Policy describes how the VMware Kernel 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 Communications Security Establishment (CSE) Cryptographic Module Validation Program (CMVP) website at http://csrc.nist.gov/groups/STM/cmvp.

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 Kernel Cryptographic Module is also referred to in this document as "the module".

1.2 References

This document deals only with operations and capabilities of the 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 (http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm) contains 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

This Security Policy and the other validation submission documentation were produced by Corsec Security, Inc. under contract to VMware. 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 Kernel Cryptographic Module

2.1 vCloud Networking and Security

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

One of the many virtualization products that VMware delivers to the market is vCloud Networking and Security (vCNS). vCNS provides networking and security capabilities independent of underlying physical infrastructure for virtualized computer environments that are built with vCloud Suite technologies. It provides a broad range of services delivered through virtual appliances (see Figure 1), such as a virtual firewall, virtual private network (VPN), load balancing, network address translation (NAT), DHCP and VXLAN-extended networks, while also providing a comprehensive framework to integrate third-party solutions. There are three vCloud Networking and Security virtual appliance types:

- vShield Edge – This appliance establishes a perimeter gateway for network traffic to enter and leave a virtual data center
- vShield Manager - A central management and reporting tool for vCNS components
- vShield App - A virtual firewall that provides protection directly in front of one or more specific workloads (e.g., virtual machines)

The VMware Kernel Cryptographic Module is contained within the vShield Edge. The next section contains a brief description of the vShield Edge virtual security appliance followed by a description of the VMware Kernel Cryptographic Module.

2.1.1 VMware vShield Edge

An integral part of the vCNS solution is the ability to build an agile and trusted private cloud infrastructure as part of a virtual datacenter. The Edge Gateway appliance provides a wide range of services, including a highly available stateful inspection firewall, IPsec[1] site-to-site VPN, a server-load balancer, NAT, and network services such as static routing, DHCP and DNS[2].

VPNs are essential for site-to-site communication over a shared network. vShield Edge protects the confidentiality of all data transmitted across virtual data center perimeters to remote sites using the secure IPSec protocol. IPSec provides the authentication and encryption of packets flowing between a remote site and the Edge-protected virtual data center for protected remote access. vShield Edge utilizes IPSec to provide secure access to the Edge-protected network.

2.1.2 VMware Kernel Cryptographic Module

Powering IPsec encryption and integrity in the vShield Edge is the VMware Kernel Cryptographic Module. The Tunnel mode of the Encapsulating Security Payload (ESP) protocol performed by an IPsec Service kernel stack, such as NETKEY, utilizes the VMware Kernel Cryptographic Module to encrypt, decrypt, and perform integrity checks on data entering and exiting the vShield Edge virtual appliance.

[1] IPsec – Internet Protocol Security
[2] DNS – Domain Name System

The VMware Kernel Cryptographic Module is a software cryptographic module located in the kernel space of the VMware vShield Edge virtual appliance. The module contains a set of cryptographic functions available to an IPSec kernel stack via a well-defined Application Programming Interface (API). These functions facilitate the secure transfer of information between VMware's vShield Edge Security Appliance and a remote peer attempting to connect to an Edge-protected network. The module includes implementations of the following FIPS-Approved security functions:

- Encryption and decryption using AES[3] and Triple-DES[4]
- Hashing functions using SHA[5] & HMAC[6] SHA
- ANSI[7] X9.31Random number generation using AES

Figure 1 depicts a sample deployment of the VMware Kernel Cryptographic Module running on the vCNS vShield Edge virtual appliance. In this deployment, an external entity located in the Enterprise Datacenter is attempting to connect to the remote Virtual Datacenter, located on an external network. The Virtual Datacenter is protected by the vShield Edge virtual appliance. In order to access the Virtual Datacenter from an external network, an external entity must connect to it through a VPN secured by IPsec and the VMware Kernel Cryptographic Module.

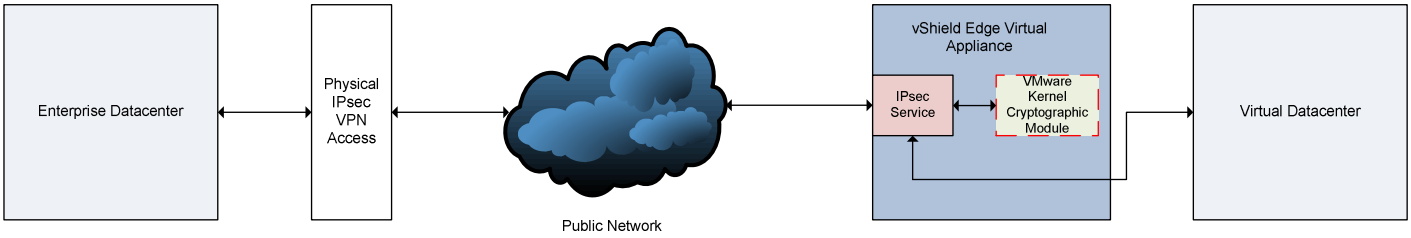

Figure 1 – vShield Edge Deployment Diagram

The VMware Kernel Cryptographic 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	1
4	Finite State Model	1
5	Physical Security	N/A
6	Operational Environment	1
7	Cryptographic Key Management	1
8	EMI/EMC[8]	1

[3] AES – Advanced Encryption Standard
[4] DES – Data Encryption Standard
[5] SHA – Secure Hash Algorithm
[6] HMAC – (keyed-) Hashed Message Authentication Code
[7] ANSI – American National Standards Institute

Section	Section Title	Level
9	Self-tests	1
10	Design Assurance	1
11	Mitigation of Other Attacks	N/A

2.2 Module Specification

The VMware Kernel Cryptographic Module is a software cryptographic module with a multiple-chip standalone embodiment. The overall security level of the module is 1. The module was tested and found to be FIPS 140-2 compliant on a HP ProLiant DL380e Gen8 Server running an Intel Xeon E5-2430 processor executing the VMware vCloud Networking and Security 5.5.0a Edge OS[9] and VMware vSphere Hypervisor (ESXi) 5.5. The composite module is composed of 3 components:

- VMware Kernel Cryptographic Module – Cryptographic algorithm implementations located in the kernel-level of the VMware vCloud Networking and Security 5.5.0a Edge OS. These implementations are leveraged by the IPsec Service implementation located in the user-space in order to perform an IPsec tunnel.
- HMAC SHA-512 utility (sha512hmac) – Integrity mechanism located in the User space of the VMware vCloud Networking and Security 5.5.0a Edge OS. This mechanism coordinates the integrity check on itself as well as the entire VMware vCloud Networking and Security 5.5.0a Edge OS kernel, which includes the VMware Kernel Cryptography. The mechanism leverages the HMAC SHA-512 algorithm implemented in the FIPS validated VMware NSS Cryptographic Module
- VMware NSS Cryptographic Module (FIPS Certificate # 2155) – The VMware NSS Cryptographic Module is a separately validated cryptographic module located in the User space of the VMware vCloud Networking and Security 5.5.0a Edge OS. The HMAC SHA-512 utility leverages the HMAC SHA-512 implementation of the VMware NSS Cryptographic Module in order to perform an integrity check on the entire VMware vCloud Networking and Security 5.5.0a Edge OS kernel.

VMware, Inc. affirms that the VMware Kernel Cryptographic Module runs in its configured, Approved mode of operation on the following binarily compatible platforms executing VMware vSphere Hypervisor (ESXi) 5.5:

- A general purpose computing platform with an AMD Opteron x86 Processor executing VMware vCloud Networking and Security 5.5.0a Edge OS
- A general purpose computing platform with an Intel Core i3, Core i5, Core i7, and Xeon x86 Processor executing VMware vCloud Networking and Security 5.5.0a Edge OS

In addition to its full AES software implementations, the VMware Kernel Cryptographic Module is capable of leveraging the AES-NI[11] instruction set of supported Intel processors in order to accelerate AES calculations.

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

[8] EMI/EMC – Electromagnetic Interference / Electromagnetic Compatibility
[9] OS – Operating System
[11] AES-NI – Advanced Encryption Standard-New Instructions

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 module supports the physical interfaces of the HP ProLiant DL380e Gen8 Server. These interfaces include the integrated circuits of the system board, processor, RAM[12], hard disk, device case, power supply, and fans. See Figure 2 below for a block diagram of the HP ProLiant DL380e Gen8 Server.

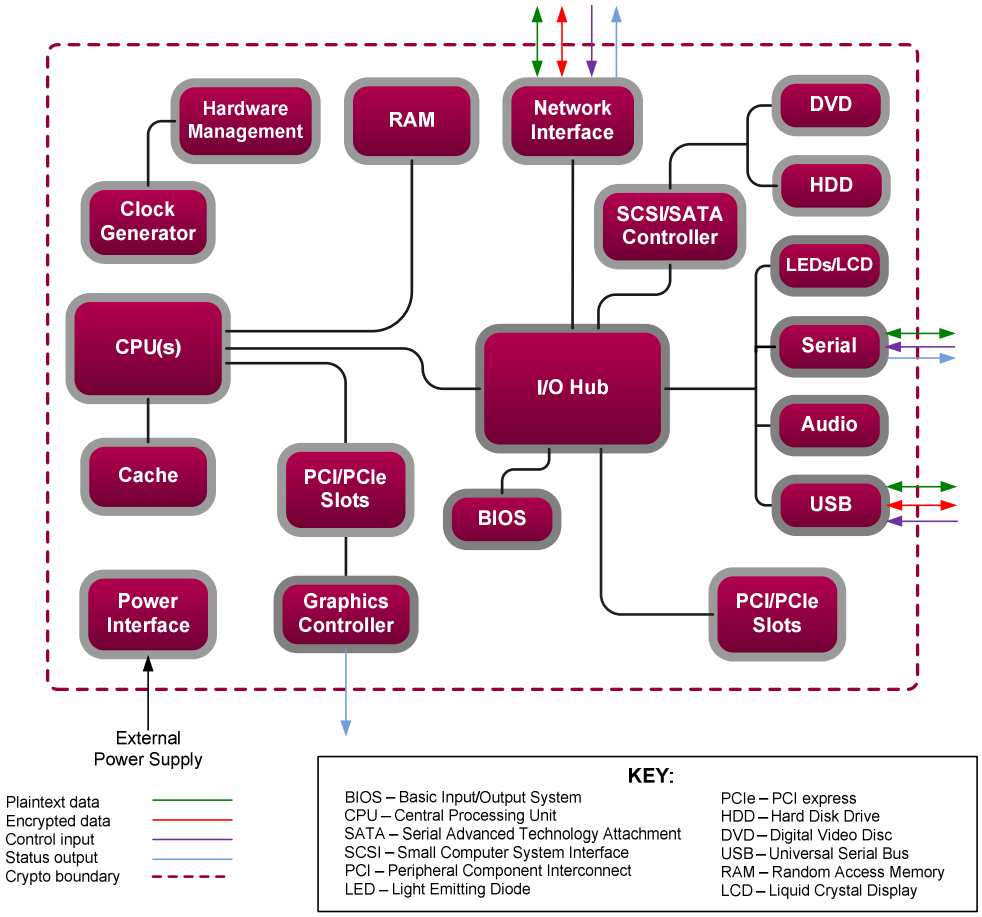

Figure 2 – HP ProLiant DL380e Gen8 Server Block Diagram

2.2.2 Logical Cryptographic Boundary

Figure 3 depicts the logical cryptographic boundary for the composite module which surrounds the VMware Kernel Cryptographic Module, the FIPS validated VMware NSS Cryptographic Module (FIPS Certificate # 2155), and the HMAC SHA-512 utility. The FIPS validated VMware NSS Cryptographic Module is included within the logical cryptographic boundary because its HMAC SHA-512 algorithm implementation is used to perform the module's integrity test.

[12] RAM – Random Access Memory

The colored arrows indicate the logical information flows into and out of the module. The module is shown exchanging data with the Linux native NETKEY Stack which is also located in the kernel space of the operating system. The IPSec Service in the user space of the operating system makes system calls to the Linux native NETKEY Stack.

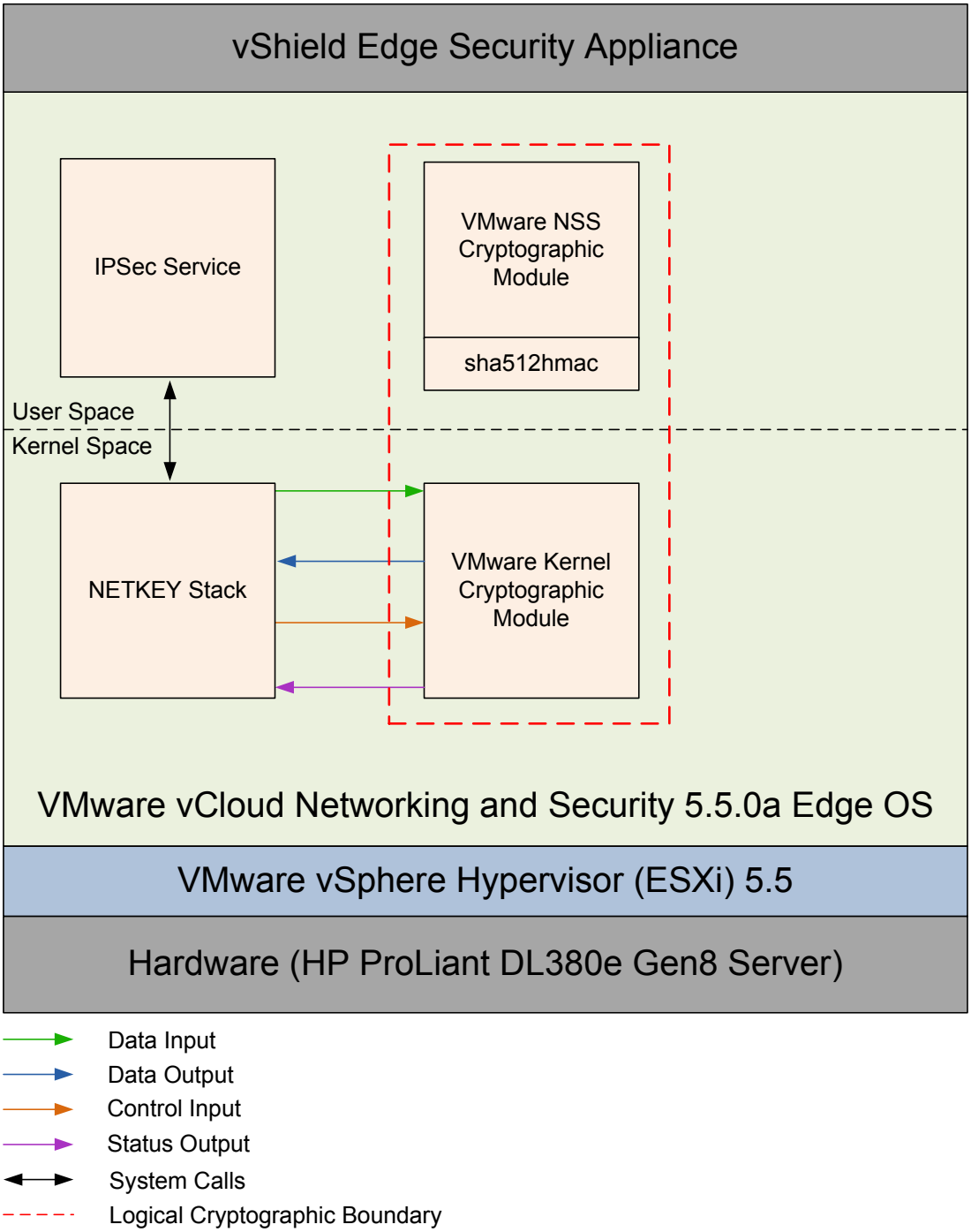

Figure 3 – VMware Kernel Cryptographic Module Logical Cryptographic Boundary

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 2 below.

Table 2 – FIPS 140-2 Logical Interface Mappings

FIPS Interface	Physical Interface	Logical 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 arguments 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

2.4 Roles and Services

There are two roles in the module (as required by FIPS 140-2) that operators may assume: a Cryptographic Officer (CO) role and a User role. Roles are assumed implicitly through the execution of either a CO or User service. The module does not support an authentication mechanism. Each role and their corresponding services are detailed in the sections below. Please note that the keys and Critical Security Parameters (CSPs) listed in Table 3 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, 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 3 describes the CO and User services and Table 4 describes the Non-Approved CO & User services.

Table 3 – Crypto Officer and User Services

Role	Service	Description	CSP and Type of Access
CO, User	Encryption	Encrypt plaintext using supplied key and algorithm specification	AES key- RX AES XTS key- RX Triple-DES key- RX
CO, User	Decryption	Decrypt ciphertext using supplied key and algorithm specification	AES key- RX AES XTS key- RX Triple-DES key- RX
CO, User	Generate Hash	Compute and return a message digest using SHA	None
CO, User	Generate Symmetric Key	Generate Symmetric keys	AES key- W AES XTS key- W Triple-DES key- W
CO, User	Generate Hashed Message Authentication Code	Compute and return a hashed message authentication code	HMAC key - RWX
CO, User	Random Number Generation	Returns the specified number of random bits to the calling application	ANSI X9.31 Seed and Seed Key- RWX
CO	Module Installation and Initialization	Installation and initialization of the module following the Secure Operation section of the Security Policy	None
CO	Show status	Returns the current mode of the module	None
CO	Run Self-Tests on Demand	Runs self-tests on demand during module operation	None
CO	Zeroize Key	Zeroizes keys	None

Table 4 – Non-Approved CO & User Services

Role	Service	Non-Approved/Non-Compliant Algorithms
CO, User	Encryption Non-Compliant	DES Triple-DES (2 Key)[13] AES CCM[14] AES GCM[15] AES XTS[16] (192 bit key)
CO, User	Decryption Non-Compliant	DES Triple-DES (2 Key) AES CCM AES GCM AES XTS (192 bit key)
CO, User	Generate Hash Non-Compliant	SHA-384 SHA-512
CO, User	Generate Hashed Message Authentication Code Non-Compliant	HMAC SHA-384 HMAC SHA-512
CO, User	Random Number Generation Non-Compliant	PRNG[17] (X9.31) when called with stdrng

The FIPS 140-2 module covers the static kernel binary and therefore provides a number of non-security relevant services to callers within the kernel space as well as the user space. The following URL[18] provides a description of these services:

- https://www.vmware.com/pdf/vshield_55_admin.pdf

2.5 Physical Security

The VMware Kernel Cryptographic 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 a HP ProLiant DL380e Gen8 Server with an Intel Xeon E5-2430 processor[19] running VMware vSphere Hypervisor (ESXi) 5.5 and

[13] To use the two-key Triple-DES algorithm to encrypt data or wrap keys in an Approved mode of operation, the module operator shall ensure that the same two-key Triple-DES key is not used for encrypting data (or wrapping keys) with more than 2^20 plaintext data (or plaintext keys). Please refer to Appendix A of SP 800-131A for restriction information regarding its use until December 31, 2015

[14] CCM – Counter with CBC-MAC

[15] GCM – Galois/Counter Mode

[16] XTS – XEX-based tweaked-codebook mode with ciphertext stealing

[17] PRNG – Pseudo-Random Number Generator

[18] URL – Uniform Resource Locator

[19] The module was tested on the same processor with AES-NI support turned on and tested again with AES-NI support turned off

the VMware vCloud Networking and Security 5.5.0a Edge OS. 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.

2.7 Cryptographic Key Management

The module implements the FIPS-Approved algorithms listed in Table 5 below.

Table 5 – FIPS-Approved Algorithm Implementations

Algorithm	Certificate Number
AES (Software Implementation) ECB, CBC, CTR encryption/decryption with 128-,192-, and 256-bit keys	2718
AES (Hardware Accelerated) ECB, CBC, CTR encryption/decryption with 128-,192-, and 256-bit keys	2718
AES (Software Implementation) XTS encryption/decryption with 128- and 256-bit keys	2718
AES (Hardware Accelerated) XTS encryption/decryption with 128- and 256-bit keys	2718
Triple-DES ECB, CBC, CTR encryption/decryption (3 Key)	1635
SHA-1, SHA-224, and SHA-256	2283
HMAC with SHA-1, SHA-224, and SHA-256 (VMware Kernel Cryptographic Module Implementation)	1697
ANSI X9.31 Appendix A.2.4 PRNG using AES 128 (when called with ansi_cprng)	1259

When used for the integrity check of the module, the VMware NSS Cryptographic Module provides the following Approved functions:

- HMAC with SHA-512 (Cert #1681)
- DSA 1024 Signature Verification (Cert #821)

The key establishment methodology for the algorithms used in this module is outside of the composite module's cryptographic boundary.

The composite 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 4 in Section 2.4.1 for the list of non-Approved algorithms and associated services.

Caveats:

- Additional information concerning SHA-1, ANSI X9.31 PRNG, and specific guidance on transitions to the use of stronger cryptographic keys and more robust algorithms is contained in NIST Special Publication 800-131A.
- The module generates cryptographic keys whose strengths may be modified by available entropy; No assurance of the minimum strength of generated keys.

The module supports the CSPs listed below in Table 6.

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

Key	Key Type	Generation[20] / Input	Output	Storage	Zeroization	Use
AES key	128, 192, 256 bit key	Generated internally by Approved PRNG; Input via API in plaintext	Output in plaintext via Tested Platform's INT[21] Path	Keys are not persistently stored by the module	Reboot OS; Cycle host power	Encryption, Decryption
AES XTS key	128, 256 bit key	Generated internally by Approved PRNG; Input via API in plaintext	Output in plaintext via Tested Platform's INT Path	Keys are not persistently stored by the module	Reboot OS; Cycle host power	Encryption, Decryption
Triple-DES key	3 key	Generated internally by Approved PRNG; Input via API in plaintext	Output in plaintext via Tested Platform's INT Path	Keys are not persistently stored by the module	Reboot OS; Cycle host power	Encryption, Decryption
HMAC key	HMAC key (112-bit)	Generated internally by Approved PRNG; Input via API in plaintext	Output in plaintext via Tested Platform's INT Path	Keys are not persistently stored by the module	Reboot OS; Cycle host power	Message Authentication with SHS[22]
ANSI X9.31 Seed	16 byte seed value	Internally generated via entropy pools	Never	Seed is not persistently stored by the module	Reboot OS; Cycle host power	Generates FIPS-Approved random number

[20] The module complies with IG 7.8 Scenario 1 for symmetric key generation
[21] INT – a validated Cryptographic Module which lies Internal or inside of the boundary in regard to the reference diagrams CM software physical boundary
[22] SHS – Secure Hash Standard

Key	Key Type	Generation[20] / Input	Output	Storage	Zeroization	Use
ANSI X9.31 Seed Key	AES 128 bit key	Internally generated via entropy pools	Never	Keys are not persistently stored by the module	Reboot OS; Cycle host power	Generates FIPS-Approved random number

2.8 Self-Tests

Cryptographic self-tests are performed by the module after the module begins operating in the FIPS-Approved mode as well as when a random number is 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

Power-up self-tests are automatically performed by the module when the module begins operation in the FIPS-Approved mode. The list of power-up self-tests that follows may also be run on-demand when the CO reboots the Operating System. The module will perform the listed power-up self-tests to successful completion. During the execution of self-tests, data output from the module is inhibited.

If any of the self-tests fail, the module will return an error to the IPSec Service and will remain in an error state. After entering the error state, all subsequent calls to the module requiring data output 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 Kernel Cryptographic Module performs the following Power-up Self-tests:

- Software integrity check (HMAC SHA-512 Integrity Test)
  - The software integrity test is performed by the HMAC SHA-512 utility, which coordinates the integrity check of the entire VMware vCloud Networking and Security 5.5.0a Edge OS kernel. The utility leverages the HMAC SHA-512 implementation provided by the VMware NSS Cryptographic Module in order to calculate the current digests of itself and the rest of the VMware Kernel Cryptographic Module[23]. Both the HMAC SHA-512 utility and VMware NSS Cryptographic Module are not utilized again after successful completion of the integrity test.
- Known Answer Tests (KATs)
  - AES Encryption KAT[24]
  - AES Decryption KAT[23]
  - Triple-DES Encryption KAT
  - Triple-DES Decryption KAT
  - SHA-1, SHA-224, SHA-256 KAT
  - HMAC SHA-1, SHA-224, SHA-256 KAT
  - ANSI X9.31 RNG[25] KAT

2.8.2 Conditional Self-Tests

A conditional self-test is performed by the module whenever a new random number is generated. If an error is encountered, the module will return an error to the IPSec Service and will remain in an error state. After entering the error state, all subsequent calls to the module requiring data output 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 Kernel Cryptographic Module performs the following conditional self-tests:

- ANSI X9.31 Continuous RNG Test

[23] Prior to performing an HMAC SHA-512 digest on the VMware Kernel Cryptographic Module, the VMware NSS Cryptographic Module will have already performed an integrity test on itself using DSA digital signature verification.
[24] The module will determine if it is running on an AES-NI supported processor and run the KAT accordingly
[25] RNG – Random Number Generator

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

3.1 Crypto Officer Guidance

Installation and operation of the VMware Kernel Cryptographic Module requires the proper installation of the vShield Edge Virtual Appliance. The sections below provide a brief summary of the installation procedures for vShield Edge. For a more comprehensive instruction set, please refer to the *vShield Installation and Upgrade Guide* provided by VMware.

All guides mentioned within these instructions are available for download at http://www.vmware.com. These instructions assume that the CO is familiar with VMware vSphere Hypervisor (ESXi) 5.5 and VMware vCloud Networking and Security 5.5.0a products.

3.1.1 Initial Setup

Prior to the secure installation of the vShield Edge Virtual Appliance, the CO shall prepare the virtual environment required to securely operate the virtual appliance. This includes installing VMware vSphere Hypervisor (ESXi) 5.5 (see *vSphere Installation and Setup*). Included in this installation are the VMware vSphere Hypervisor (ESXi) 5.5, vSphere 5.5 vSphere Client, and the vSphere 5.5 vCenter Server, all of which are prerequisites to installing the vShield Edge Virtual Appliance.

After installing the VMware vSphere 5.5 virtual environment, the CO shall log into the vCenter Server using the vSphere Client and follow the instructions provided in Chapter 3 of *vShield Installation and Upgrade Guide* to securely install and configure VMware vShield Manager Virtual Appliance; the management component needed to install vShield Edge.

3.1.2 Secure Installation

In order to install the VMware Kernel Cryptographic Module, the CO shall follow the installation instructions provided in Chapter 4 of *vShield Installation and Upgrade Guide* in order to securely install and configure the vShield Edge Virtual Appliance. A brief summary of the installation steps is provided:

- Log into the vCenter Server using vSphere Client
- Determine which ESXi host the virtual appliance will be installed on
- Access the “Add Edge Wizard”
- Follow the step-by-step instructions of the “Add Edge Wizard”
- Add an Edge Appliance
- Confirm the settings and install

Successful completion of installing a vShield Edge Virtual Appliance will be indicated by the appearance of a vShield Edge Virtual Appliance on the ESXi host which the CO specified. Using the vSphere Client, the CO can determine that the virtual appliance is operational. Troubleshooting is available in Section 7 of the *vShield Installation and Upgrade Guide*.

3.1.3 VMware Kernel Cryptographic Module Secure Operation

Following the successful installation of the vShield Edge Virtual Appliance, the CO shall power on the virtual appliance. The module is loaded at the time of the system boot. The CO shall follow the guidelines in Chapter 9 of the *vShield Administration Guide* in order to securely configure and operate the VMware Kernel Cryptographic Module. The module will continue to operate in the FIPS mode of operation unless it is disabled by changing the configuration. The HMAC SHA-512 utility leverages the FIPS validated VMware NSS Cryptographic Module one time during the boot up of the module until it has completed the

module's integrity test successfully. Both the HMAC SHA-512 utility and VMware NSS Cryptographic Module are not utilized again until another integrity check is required. To verify that the module is operating in the FIPS Approved mode, the CO can use the "show FIPS" CLI[26] command.

3.2 User Guidance

The VMware Kernel Cryptographic Module is designed for use by the VMware vShield Edge Appliance. The User shall adhere to the guidelines of this Security Policy. The User does not have any ability to install or configure the module. Operators in the User role are able to use the services available to the User role listed in Table 3. The User is responsible for reporting to the CO if any irregular activity is noticed. The FIPS validated VMware NSS Cryptographic Module, although used, is only considered to support the integrity verification and is not intended for general-purpose use with respect to this module.

[26] CLI – Command-Line Interface

4 Acronyms

Table 7 provides definitions for the acronyms used in this document.

Table 7 – Acronyms

Acronym	Definition
AES	Advanced Encryption System
ANSI	American National Standards Institute
API	Application Programming Interface
BIOS	Basic Input/Output System
CBC	Cipher Block Chaining
CCM	Counter with CBC-MAC
CLI	Command-Line Interface
CMVP	Cryptographic Module Validation Program
CO	Crypto Officer
CPU	Central Processing Unit
CSE	Communications Security Establishment
CSP	Critical Security Parameter
CTR	Counter
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DVD	Digital Video Disc
ECB	Electronic Code Book
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
ESP	Encapsulating Security Payload
FIPS	Federal Information Processing Standard
GCM	Galois/Counter Mode
HDD	Hard Disk Drive
HMAC	(keyed-) Hash Message Authentication Code
INT	A validated Cryptographic Module which lies Internal or inside of the boundary in regard to the reference diagrams CM software physical boundary
IPsec	Internet Protocol Security
IT	Information Technology

Acronym	Definition
IV	Initialization Vector
KAT	Known Answer Test
LCD	Liquid Crystal Display
LED	Light Emitting Diode
MAC	Message Authentication Code
NAT	Network Address Translation
NIST	National Institute of Standards and Technology
NSS	Network Security Services
OS	Operating System
PCI	Peripheral Component Interconnect
PCIe	PCI express
PRNG	Pseudo-Random Number Generator
RAM	Random Access Memory
REST	Representational State Transfer
RFC	Request for Comments
RNG	Random Number Generator
SATA	Serial Advanced Technology Attachment
SCSI	Small Computer System Interface
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
URL	Uniform Resource Locator
USB	Universal Serial Bus
vCNS	vCloud Networking & Security
VPN	Virtual Private Network
VXLAN	Virtual Extensible Local Area Network
XTS	XEX-based tweaked-codebook mode with ciphertext stealing

Prepared by:
Corsec Security, Inc.

13135 Lee Jackson Memorial Highway, Suite 220
Fairfax, VA 22033
United States of America

Phone: +1 (703) 267-6050
Email: info@corsec.com
http://www.corsec.com