VMware, Inc.

VMware Cryptographic Module

Software Version: 1.0

FIPS 140-2 Non-Proprietary Security Policy

FIPS Security Level: 1
Document Version: 1.1

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.vmare.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 Cryptographic Module from VMware, Inc. This Security Policy describes how the VMware 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 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 Cryptographic Module is referred to in this document as the VCM, the crypto module, or the module.

1.2 References

This document deals only with operations and capabilities of the 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 (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 Cryptographic Module

2.1 VMware Overview

VMware, Inc. is a global leader in virtualization and cloud infrastructure, delivering customer-proven solutions that accelerate 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.

2.1.1 VMware vCloud Networking and Security

One of the many virtualization products that VMware delivers to the market is vCloud Networking and Security (vCNS). vCNS provides software-defined networking and security built into the virtual infrastructure. vCNS is a networking and security solution which provides virtual firewalls, virtual private networks (VPNs), and load balancing to virtual datacenters and private cloud deployments. Three key Virtual Security Appliances are part of the vCNS solution:

- vShield Manager - A central management and reporting tool for vCNS components
- vShield Edge - A networking and security gateway for protecting virtual data centers
- vShield App - A virtual firewall to protect critical applications on virtual machines

vShield Manager, vShield Edge, and vShield App Virtual Security Appliances each provide remote CLI[1] access via the Secure Shell (SSH) server for Cryptographic Officers (CO) and Users.

2.1.2 SSH Server

The SSH server software application is vital to vCNS operation as it provides secure, remote access to VMware's vShield Virtual Security Appliances. The SSH protocol substitutes less secure protocols such as rlogin and telnet with more secure and robust cryptography. Data encryption and data integrity are provided to the CO and User when accessing any of the vShield Virtual Security Appliances remotely via the SSH server.

2.1.3 VMware Cryptographic Module

The VMware Cryptographic Module (VCM) is a shared software cryptographic library which provides FIPS-Approved cryptographic security functions and network security protocol primitives to a calling application, such as the SSH server. The module provides these security functions via a well-defined Application Programming Interface (API). The installation of a Virtual Security Appliance includes a validated release of the VMware Cryptographic Module.

The module includes implementations of the following FIPS-Approved security functions:

- Symmetric key functions using AES[2] and Triple DES[3]
- Hashing functions using SHA[4]-1 and SHA-2
- Message Authentication Functions using HMAC[5]

[1] CLI – Command Line Interface
[2] AES – Advanced Encryption Standard
[3] DES – Data Encryption Standard
[4] SHA – Secure Hash Algorithm
[5] HMAC – (Keyed-) Hash Message Authentication Code

- Asymmetric key functions using DSA[6] and RSA[7]
- Random number generation using ANSI[8] X9.31 PRNG[9]

A sample deployment scenario for the VMware Cryptographic Module being utilized by the vShield Edge Virtual Security Appliance is provided by Figure 1. The VCM is located within the light-blue boundary of the vShield Edge Virtual Appliance. In this scenario, the VCM can provide secure SSH access to the vShield Edge Virtual Appliance for remote machines located on an unprotected internal network, on an external network, or on a secure/isolated network. The VMware Cryptographic Module will work in a similar manner within the vShield Manager and vShield App appliances.

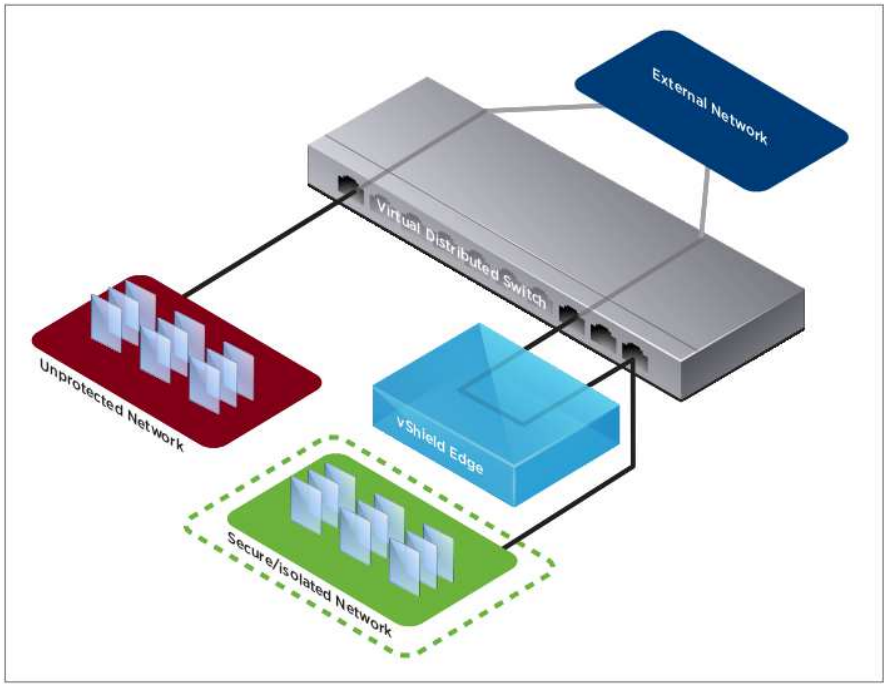

Figure 1 – vShield Edge Deployment Diagram

The VMware 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

[6] DSA – Digital Signature Algorithm
[7] RSA – Rivest, Shamir, Adleman
[8] ANSI – American National Standards Institute
[9] PRNG – Pseudo Random Number Generator

Section	Section Title	Level
7	Cryptographic Key Management	1
8	EMI/EMC[10]	1
9	Self-tests	1
10	Design Assurance	1
11	Mitigation of Other Attacks	N/A

2.2 Module Specification

The VMware Cryptographic Module is a software cryptographic module with a multi-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 an HP ProLiant DL380e Gen8 Server running an Intel Xeon E5-2430 processor executing VMware's own proprietary version of Linux and VMware vSphere Hypervisor (ESXi) 5.5. The VMware Linux OS[11] versions on which the module operates include:

- VMware vCloud Networking and Security 5.5.0a vShield Manager OS
- VMware vCloud Networking and Security 5.5.0a App Firewall OS
- VMware vCloud Networking and Security 5.5.0a Edge OS

VMware, Inc. affirms that the VMware 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 either of the VMware Operating Systems listed above.
- A general purpose computing platform with an Intel Core i3, Core i5, Core i7, and Xeon x86 Processor executing either of the VMware Operating Systems listed above.

Because the VMware Cryptographic Module is defined as a software cryptographic module, it possesses both a physical cryptographic boundary and a logical cryptographic boundary. The physical and logical boundaries are outlined in Section 2.2.1 and 2.2.2, respectively.

2.2.1 Physical Cryptographic Boundary

As a software cryptographic module, there are no physical protection mechanisms implemented. Therefore, 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. These interfaces include the integrated circuits of the system board, processor, network adapters, RAM[12], hard disk, device case, power supply, and fans. See Figure 2 for a block diagram of the HP ProLiant.

[10] EMI/EMC – Electromagnetic Interference / Electromagnetic Compatibility
[11] OS – Operating System
[12] RAM – Random Access Memory

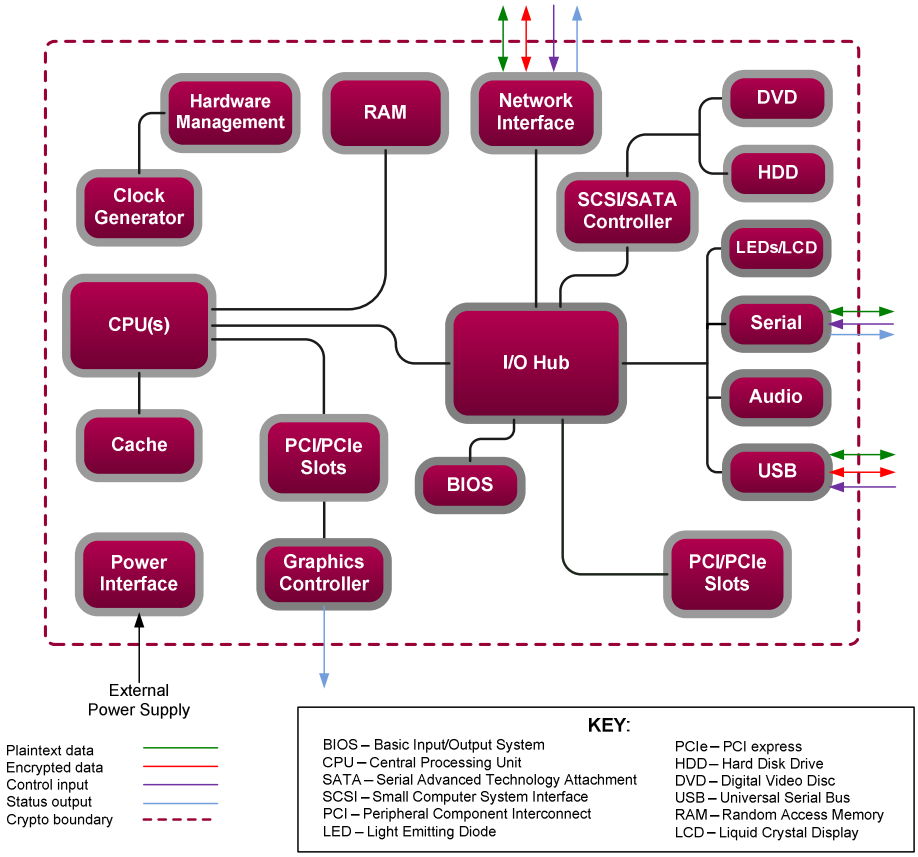

Figure 2 – HP ProLiant Server Block Diagram

2.2.2 Logical Cryptographic Boundary

Figure 3 shows a logical block diagram of the module executing in memory and its interactions with surrounding software components, as well as the module's logical cryptographic boundary. The files and binaries that make up the cryptographic module are shown as "VMware Cryptographic Module" in the diagram below. The module's services are designed to be called by applications such as the SSH server. 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.

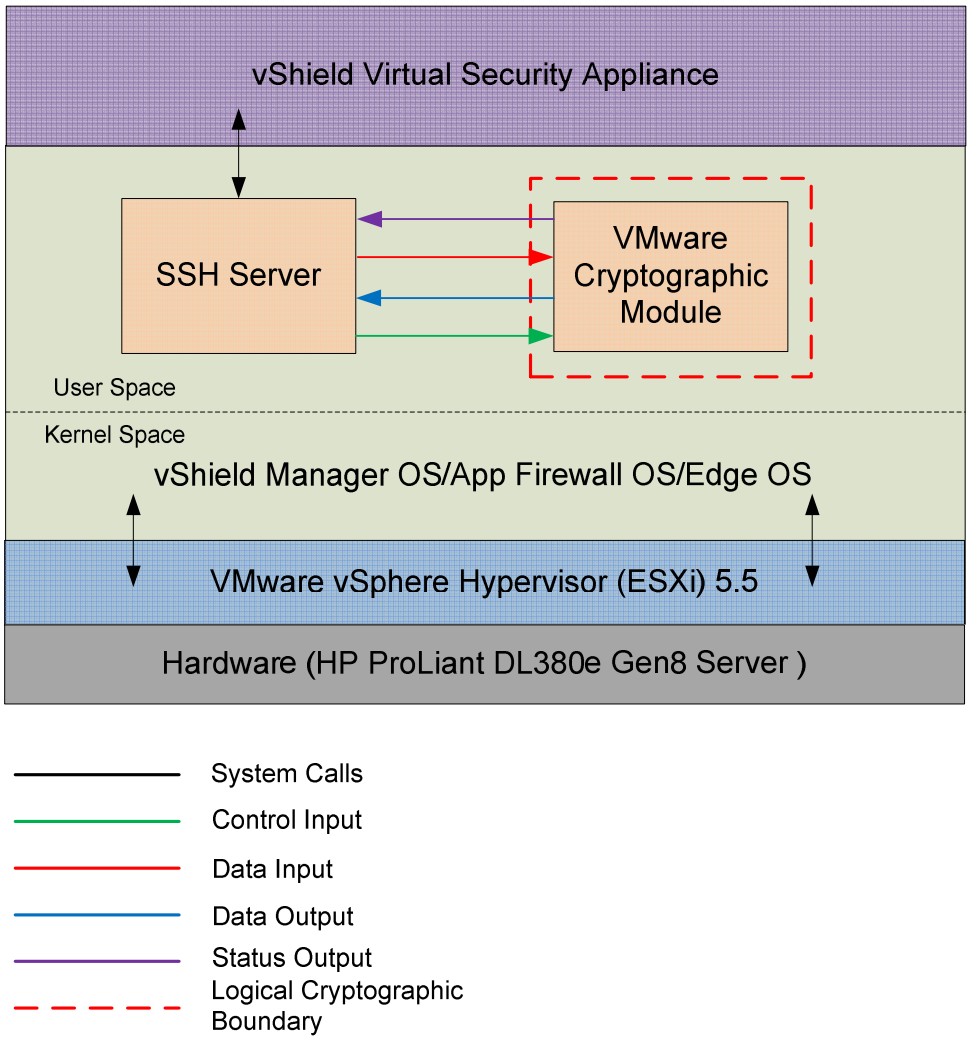

Figure 3 – VMware Cryptographic Module Logical Cryptographic Boundary

2.3 Module Interfaces

The module's logical interfaces exist at a low level in the software as an Application Programming Interface (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 has no physical characteristics. Thus, 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	Module Interface (API)
Data Input	Network port, Serial port, SCSI/SATA Controller, USB port	The function calls that accept input data for processing through their arguments.
Data Output	Network port, Serial port, SCSI/SATA Controller, USB port	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

The module does not support an authentication mechanism. There are two roles in the module (as required by FIPS 140-2) that operators may assume: a CO role and a User role. Roles are assumed implicitly through the execution of either a CO or User service. 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 and Table 4 below indicate the type 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 Approved or Allowed security function or authentication mechanism.

2.4.1 Crypto Officer Role

To assume the CO role, an operator of the module will perform one of the services listed in Table 3. The CO has the ability to enter and exit FIPS mode, run self-tests on demand, show status, and zeroize all keying material.

Table 3 – Crypto Officer Services

Service	Description	Key/CSP and Type of Access
Initialize module	Performs integrity check and power-up self-tests. Places the module into its validated FIPS-Approved mode.	None
Show status	Returns the current mode of the module	None
Run self-tests on demand	Performs power-up self-tests	None
Zeroize keys	Zeroizes and de-allocates memory containing sensitive data	All keys – W

2.4.2 User Role

To assume the User role, an operator of the module will perform one of the services listed in Table 4. The User has the ability to generate random numbers, symmetric and asymmetric keys, and digital signatures. Table 4 lists the module's non-Approved services.

Table 4 – Mapping User Services to Input, Output, CSPs, and Type of Access

Service	Description	Key/CSP and Type of Access
Generate random number	Returns the specified number of random bits to calling application	ANSI X9.31 RNG[13] seed – RWX ANSI X9.31 seed key – RX
Generate message digest (SHS[14])	Compute and return a message digest using SHS algorithms	None
Generate keyed hash	Compute and return a message authentication code	HMAC key – RX
Symmetric encryption	Encrypt plaintext using supplied key and algorithm specification	AES key – RX Triple-DES key – RX
Symmetric decryption	Decrypt ciphertext using supplied key and algorithm specification	AES key – RX Triple-DES key – RX
Generate Symmetric Key	Generate and return the specified symmetric key	AES Key – W Triple-DES Key – W
Generate asymmetric key pair	Generate and return the specified type of asymmetric key pair	RSA private key – W DSA private key – W
RSA key wrapping	Wrap plaintext using RSA public key (used for key transport)	None
RSA key unwrapping	Unwrap data using RSA private key (used for key transport)	RSA private key – RX
DH primitive	Perform Diffie-Hellman primitive[15]	DH[16] private keys – W
Signature Generation	Generate a signature for the supplied message using the specified key and algorithm	RSA private key – RX, DSA private key – RX
Signature Verification	Verify the signature on the supplied message using the specified key and algorithm	None

2.5 Physical Security

The VMware 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.

[13] RNG – Random Number Generator
[14] SHS – Secure Hash Standard
[15] Diffie-Hellman primitive is implemented to perform in accordance with scenario 6 in section D.8 of FIPS 140-2 Implementation Guidance. This service is provided for calling process use and is not used to establish keys into the module.
[16] DH – Diffie-Hellman

2.6 Operational Environment

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

- HP ProLiant DL380e Gen8 Server with an Intel Xeon E5-2430 processor running VMware vCloud Networking and Security 5.5.0a vShield Manager OS
- HP ProLiant DL380e Gen8 Server with an Intel Xeon E5-2430 processor running VMware vCloud Networking and Security 5.5.0a App Firewall OS
- HP ProLiant DL380e Gen8 Server with an Intel Xeon E5-2430 processor running VMware vCloud Networking and Security 5.5.0a Edge OS

All operating systems are executing on a VMware vSphere Hypervisor (ESXi) 5.5. All cryptographic keys and CSPs are under the control of the OS, which protects the CSPs against unauthorized disclosure, modification, and substitution. The module only allows access to CSPs through its well-defined API. The SSH server accessing the module is the single user of the VMware Cryptographic Module.

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 in ECB[17], CBC[18], OFB[19], CFB[20]1, CFB8, CFB128 modes with 128-, 192-, and 256-bit keys	2701
Triple-DES in ECB, CBC, CFB1, CFB8, CFB64, OFB modes (Keying Options 1, 2)	1620
RSA (ANSI X9.31, PKCS[21] #1 v1.5, PSS[22]) signature generation 2048- and 3072-bit keys	1399
RSA (ANSI X9.31, PKCS[23] #1 v1.5, PSS[24]) signature verification with 1024-, 1536-, 2048-, 3072-, 4096-bit keys	1399
RSA (ANSI X9.31) key generation with 2048 and 3072 bit keys	1399
DSA Signature Verification with 1024-bit key	822
DSA PQG Verification with 1024-bit key	822
SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	2268
HMAC-SHA-1, HMAC-SHA-224, HMAC-SHA-256, HMAC- SHA-384, HMAC-SHA-512	1682
ANSI X9.31PRNG Appendix A.2.4	1255

[17] ECB – Electronic Codebook
[18] CBC – Cipher Block Chaining
[19] OFB – Output Feedback
[20] CFB – Cipher Feedback
[21] PKCS – Public-Key Cryptography Standards
[22] PSS – Public Signature Scheme
[23] PKCS – Public-Key Cryptography Standards
[24] PSS – Public Signature Scheme

The module employs the following key establishment methodology, which is allowed for use in a FIPS-Approved mode of operation:

- RSA key wrapping (key establishment methodology provides 112 to 150[25] bits of encryption strength; non-compliant less than 112 bits of encryption strength)
- Diffie-Hellman (primitive implementation provides 112 to 219[25] bits of encryption strength; non-compliant less than 112 bits of encryption strength)
- EC Diffie-Hellman (key agreement; key establishment methodology provides between 112 and 256 bits of encryption strength; non-compliant less than 112 bits of encryption strength)

The module employs the methods listed in Table 6, which are not allowed for use in a FIPS-Approved mode. Their use will result in the module operating in a non-Approved mode.

Table 6 – VMware Cryptographic Module Non-Approved Services

Service	Description
Elliptic Curve DSA (non-compliant)	Perform Elliptic Curve DSA (ECDSA) key pair generation; ECDSA sign and verify
RSA and DSA Key Generation	Key-pair generation with RSA and DSA key sizes less than 2048-bits
RSA and DSA Signature Generation (key length)	Signature generation with RSA and DSA key sizes less than 2048-bits
RSA and DSA Signature Generation (hash size)	Signature generation with RSA and DSA (any key size) using SHA-1 hash

Caveats:

- Additional information concerning 2-key Triple-DES, SHA-1, DSA key and signature generation, Diffie-Hellman key agreement/key establishment, RSA key and signature generation, RSA key transport, 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 are modified by available entropy

[25] Computed using equation 1 in IG 7.5

The module supports the CSPs listed below in Table 7.

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

Key	Key Type	Generation[26] / Input	Output	Storage	Zeroization	Use
AES key	AES128-, 192-, 256-bit key	Internally Generated via approved PRNG; or Input via API in plaintext	Output in plaintext via Tested Platform's INT Path	Keys are not persistently stored by the module	Reboot OS; API call; Cycle host power	Encryption, decryption
Triple-DES key	Triple-DES 112-, 168- bit key	Internally Generated via approved PRNG; or Input via API in plaintext	Output in plaintext via Tested Platform's INT Path	Keys are not persistently stored by the module	Reboot OS; API call; Cycle host power	Encryption, decryption
HMAC key	HMAC key	Internally Generated via approved PRNG; or Input via API in plaintext	Output in plaintext via Tested Platform's INT Path	Keys are not persistently stored by the module	Reboot OS; API call; Cycle host power	Message Authentication with SHS
RSA private key	RSA 1024-, 1536-, 2048-, 3072-, 4096-bit key	Internally Generated via approved PRNG; or Input via API in plaintext	Output in plaintext via Tested Platform's INT Path	Keys are not persistently stored by the module	Reboot OS; API call; Cycle host power	Signature generation, key unwrapping
RSA public key	RSA 1024-, 1536-, 2048-, 3072-, 4096-bit key	Internally Generated via approved PRNG; or Input via API in plaintext	Output in plaintext via Tested Platform's INT Path	Keys are not persistently stored by the module	Reboot OS; API call; Cycle host power	Signature verification, key wrapping

[26] The module complies with IG 7.8 Scenario 1 for symmetric key generation as well as the seed supplied to the algorithm for generating asymmetric keys

Key	Key Type	Generation[26] / Input	Output	Storage	Zeroization	Use
DSA private key	DSA 160-bit key	Internally Generated via approved PRNG; or Input via API in plaintext	Output in plaintext via Tested Platform's INT Path	Keys are not persistently stored by the module	Reboot OS; API call; Cycle host power	Signature generation
DSA public key	DSA 1024-bit key	Internally Generated via approved PRNG; or Input via API in plaintext	Output in plaintext via Tested Platform's INT Path	Keys are not persistently stored by the module	Reboot OS; API call; Cycle host power	Signature verification
DH public keys	DH 1024- to 10000-bit keys	Internally Generated via approved RNG; or Input via API in plaintext	Output in plaintext via Tested Platform's INT Path	Keys are not persistently stored by the module	Reboot OS; API call; Cycle host power	Key exchange
DH private keys	DH 160- to 238-bit keys	Internally Generated via approved RNG; or Input via API in plaintext	Output in plaintext via Tested Platform's INT Path	Keys are not persistently stored by the module	Reboot OS; API call; Cycle host power	Key exchange
ANSI X9.31 PRNG seed	128-bit random value	Generated Within the Physical Boundary; Input Electronically	Never	The PRNG seed is not persistently stored by the module	Reboot OS; API call; Cycle host power	Generate random number
ANSI X9.31 PRNG seed key	AES 256-bit key	Generated Within the Physical Boundary; Input Electronically	Never	Keys are not persistently stored by the module	Reboot OS; API call; Cycle host power	Generate random number

2.8 Self-Tests

Cryptographic self-tests are performed by the module when the module begins operation in the FIPS-Approved mode as well as when a random number or asymmetric key pair is created. The following sections list the self-tests performed by the module, expected error status, and error resolution.

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 SSH server 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 Operating system. If the error persists, the module must be reinstalled.

The VMware Cryptographic Module performs the following Power-up Self-tests:

- Software integrity check (HMAC SHA-1)
- Known Answer Tests (KATs)
    - AES KAT (Encrypt)
    - AES KAT (Decrypt)
    - Triple-DES KAT (Encrypt)
    - Triple-DES KAT (Decrypt)
    - RSA KAT (Signature Generation)
    - RSA KAT (Signature Verification)
    - RSA KAT (Wrap)
    - RSA KAT (Unwrap)
    - SHA-1 KAT
    - HMAC with SHA-1 KAT
    - HMAC with SHA-224, SHA-256, SHA-384, SHA-512 KAT
    - ANSI X9.31 RNG KAT
- DSA Pairwise Consistency Test

2.8.2 Conditional Self-Tests

Conditional self-tests are performed by the module whenever a new random number is generated or when a new RSA or DSA key pair is generated. If an error is encountered, the module will return an error to the SSH server 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 Operating system. If the error persists, the module must be reinstalled.

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

- ANSI X9.31 Continuous RNG Test
- RSA PCT[27] for Key Pair Generation
- DSA PCT for Key Pair Generation

[27] PCT – Pairwise Consistency Test

2.9 Mitigation of Other Attacks

This section is not applicable. The modules do not claim to mitigate any attacks beyond the FIPS 140-2 Level 1 requirements for this validation.

3 Secure Operation

The VMware 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 Cryptographic Module requires the proper installation of the vShield Manager, vShield App, or vShield Edge. The sections below provide a brief summary of the installation procedures for these virtual appliances. For a more comprehensive instruction set, please refer to the *vShield Installation and Upgrade Guide* provided by VMware. The VMware Cryptographic Module is preconfigured to always operate in the FIPS-Approved mode of operation.

All guides mentioned within these instructions are freely available for download at http://www.vmware.com. These instructions assume that the CO is familiar with VMware vSphere 5.5 and VMware vShield 5.5 products.

3.1.1 Initial Setup

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

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 and Chapter 4 of *vShield Installation and Upgrade Guide* to securely install and configure the vShield Virtual Security Appliances. Successful installation of these virtual appliances is required for the installation of the VMware Cryptographic Module.

3.1.2 Secure Installation

In order to install the VMware Cryptographic Module, the CO shall follow the installation instructions provided in Chapter 3 and Chapter 4 of *vShield Installation and Upgrade Guide* in order to securely install and configure each of the vShield Virtual Security Appliances. A brief summary of the installation steps for each virtual appliance is provided:

vShield Manager (Must be installed first):

- Log into the vCenter Server using vSphere Client
- Install vShield Manager using OVA file obtained from VMware
- Configure network settings
- Log into vShield Manager directly
- Set up and configure for Operation

vShield Edge:

- 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

vShield App:

- Log into the vCenter Server using vSphere Client
- Determine which ESXi host the virtual appliance will be installed on
- Click the "vShield" tab after selecting the ESXi host
- Click "Install"
- Configure settings
- Click "Install"

Successful completion of installing the vShield Virtual Security Appliances will be indicated by the appearance of Virtual Appliances on the selected ESXi hosts specified by the CO. Using the vSphere Client, the CO can determine that the virtual appliances are operational. Troubleshooting instructions are available in *vShield Installation and Upgrade Guide*.

3.1.3 VMware Cryptographic Module Secure Operation

Following the successful installation of the vShield Virtual Security Appliances, the CO shall power on each of the virtual appliances. Enabling the SSH Server will initiate the VMware Cryptographic Module. The VCM is configured to always operate in the FIPS-Approved mode of operation. In the case that a non-Approved service is performed by the operator (see Section 2.7), the module will be operating in the non-Approved mode until the execution of that service is complete. The CO shall follow the guidelines offered in the *vShield Administration Guide* in order to securely operate the VMware Cryptographic Module.

3.2 User Guidance

The VMware Cryptographic Module is designed for use by VMware security products. 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 perform the services listed in Table 4. Users are responsible for reporting to the CO any irregular activity they notice. During operation, the User may check the status of the module by attempting to run any User service. If the service executes, the module is operating in FIPS mode.

4 Acronyms

Table 8 defines the acronyms used throughout this Security Policy.

Table 8 – Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
API	Application Programming Interface
BIOS	Basic Input/Output System
CBC	Cipher Block Chaining
CFB	Cipher Feedback
CLI	Command Line Interface
CMVP	Cryptographic Module Validation Program
CO	Cryptographic Officer
CPU	Central Processing Unit
CSE	Communications Security Establishment
CSP	Critical Security Parameter
DES	Data Encryption Standard
DH	Diffie-Hellman
DSA	Digital Signature Algorithm
DVD	Digital Video Disc
ECB	Electronic Code Book
ECDSA	Elliptic Curve Digital Signature Algorithm
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FIPS	Federal Information Processing Standard
HDD	Hard Disk Drive
HMAC	(Keyed-) Hash Message Authentication Code
KAT	Known Answer Test
LCD	Liquid Crystal Display
LED	Light Emitting Diode
NIS	Network Information Service
NIST	National Institute of Standards and Technology
NVLAP	National Voluntary Laboratory Accreditation Program
OFB	Output Feedback

Acronym	Definition
PCI(e)	Peripheral Component Interconnect (express)
PCT	Pairwise Consistency Test
PKCS	Public Key Cryptography Standard
PRNG	Psuedo-Random Number Generator
PSS	Public Signature Scheme
RNG	Random Number Generator
RAM	Random Access Memory
RC	Rivest Cipher
RSA	Rivest Shamir Adleman
SATA	Serial Advanced Technology Attachment
SCSI	Small Computer System Interface
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
SSH	Secure Shell
TDEA	Triple Data Encryption Algorithm
USB	Universal Serial Bus
vCNS	vCloud Networking and Security
VCM	VMware Cryptographic Module

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