VMware, Inc.

VMware Horizon JCE (Java Cryptographic Extension) Module

Software Version: 1.0

FIPS 140-2 Non-Proprietary Security Policy

FIPS SECURITY LEVEL 1
DOCUMENT VERSION: 1.1

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 Horizon JCE (Java Cryptographic Extension) Module from VMware, Inc. This Security Policy describes how the VMware Horizon JCE (Java Cryptographic Extension) 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 Security Policy was prepared as part of the Level 1 FIPS 140-2 validation of 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 (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) contains option to find 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 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 Horizon JCE (Java Cryptographic Extension) 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 and improving security and control.

2.1.1 Horizon 6

Horizon 6 leverages desktop virtualization with View and builds on these capabilities, allowing IT to deliver virtualized and remoted desktop and applications through a single platform and supports users with access to all their Windows and online resources through one unified workspace.

Horizon 6 supports the following key functionalities.

- Desktops and Applications Delivered through a Single Platform – Deliver virtual or remoted desktops and applications through a single platform to streamline management and easily entitle end users.
- Unified Workspace – Securely delivers desktops, applications, and online services to end users through a unified workspace, providing a consistent user experience across devices, locations, media, and connections.
- Closed Loop Management and Automation – Consolidated control, delivery and protection of user compute resources with cloud analytics and automation, cloud orchestration and self-service features.
- Optimization with the Software-Defined Data Center – Allocates resources dynamically with virtual storage, compute, and networking to manage and deliver desktop services on demand.
- Central Image Management – Central image management for physical, virtual, and BYO devices.
- Hybrid-cloud flexibility – Provides an architecture built for onsite and cloud-based deployment.

2.1.2 VMware Horizon JCE (Java Cryptographic Extension) Module

The VMware Horizon JCE (Java Cryptographic Extension) Module is a software cryptographic module containing a set of cryptographic functions available to the Horizon 6 View Connection Server, Security Server and View Agent via a well-defined Application Programming Interface (API). These functions facilitate the secure transfer of information between both View Components and external services where security is paramount. Within the context of this security policy, the VMware Horizon JCE (Java Cryptographic Extension) Module is also referred to as VMware Horizon JCE Module. The VMware Horizon JCE Module is a shared cryptographic library which provides the FIPS-Approved algorithms necessary for secure connections and services. The VMware Horizon JCE Module includes implementations of the following FIPS-Approved security functions:

- Symmetric key functions using AES[1] and Triple DES[2]
- Hashing functions using SHA[3]
- Asymmetric key functions using RSA[4] and DSA[5]
- Random number generation using NIST SP[6] 800-90A Hash-based DRBG[7]

[1] AES – Advanced Encryption Standard
[2] DES – Data Encryption Standard
[3] SHA – Secure Hash Algorithm
[4] RSA – Rivest, Shamir, Adleman
[5] DSA – Digital Signature Algorithm
[6] SP – Special Publication
[7] DRBG – Deterministic Random Bit Generator

Figure 1 provides an architectural overview of the components that interact with the VMware Horizon JCE Module. The module is deployed into a Java Virtual Machine (JVM) where it implements a cryptographic service provider within the Java Cryptography Architecture (JCA). The services it provides are made available to applications through the JCA framework. The indirection through the framework enables applications to be independent of the providers that implement the cryptographic services with the selection of the provider being made at run time on the basis of a provided configuration.

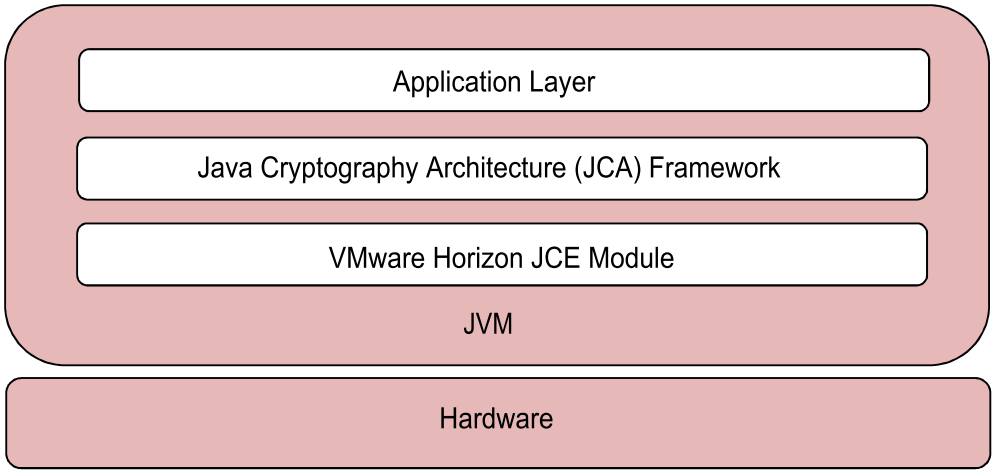


Figure 1 – Architectural Overview of the VMware JCE

Figure 2 illustrates how the three Horizon 6 View components leverage the VMware Horizon JCE Module. The View Security Server, View Connection Server and View Agent, interact with the VMware Horizon JCE Module by making cryptographic requests through the JCA framework. When these components have been configured to use FIPS cryptographic functionality, the configuration options are set such that the JCA Framework will route such requests to the VMware Horizon JCE.

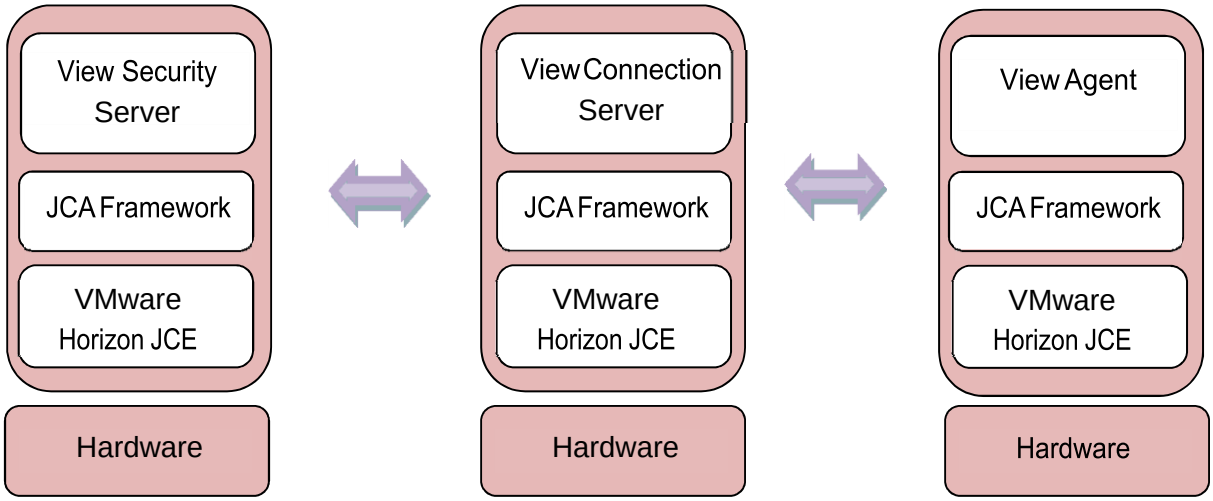


Figure 2 – Relationship of VMware Horizon JCE and View Components

The VMware Horizon JCE Module is validated at 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
9	Self-tests	1
10	Design Assurance	1
11	Mitigation of Other Attacks	N/A

2.2 Module Specification

The VMware Horizon JCE 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 the following platforms:

- Horizon 6, version 6.2 with Sun JRE 1.8 on Windows Server 2012R2 Datacenter hosted on VMware vSphere Hypervisor (ESXi) 6.0 running on Dell PowerEdge R630 with Intel(R) Xeon(R) E5-2630 CPU
- Horizon 6, version 6.2 with Sun JRE 1.8 on Windows 7 SP1 Enterprise (32 bit) hosted on VMware vSphere Hypervisor (ESXi) 6.0 running on Dell PowerEdge R630 with Intel(R) Xeon(R) E5-2630 CPU

VMware, Inc. affirms that the VMware Horizon JCE Module runs in its configured, Approved mode of operation on the following binary compatible platforms executing VMware vSphere Hypervisor (ESXi) 6.0:

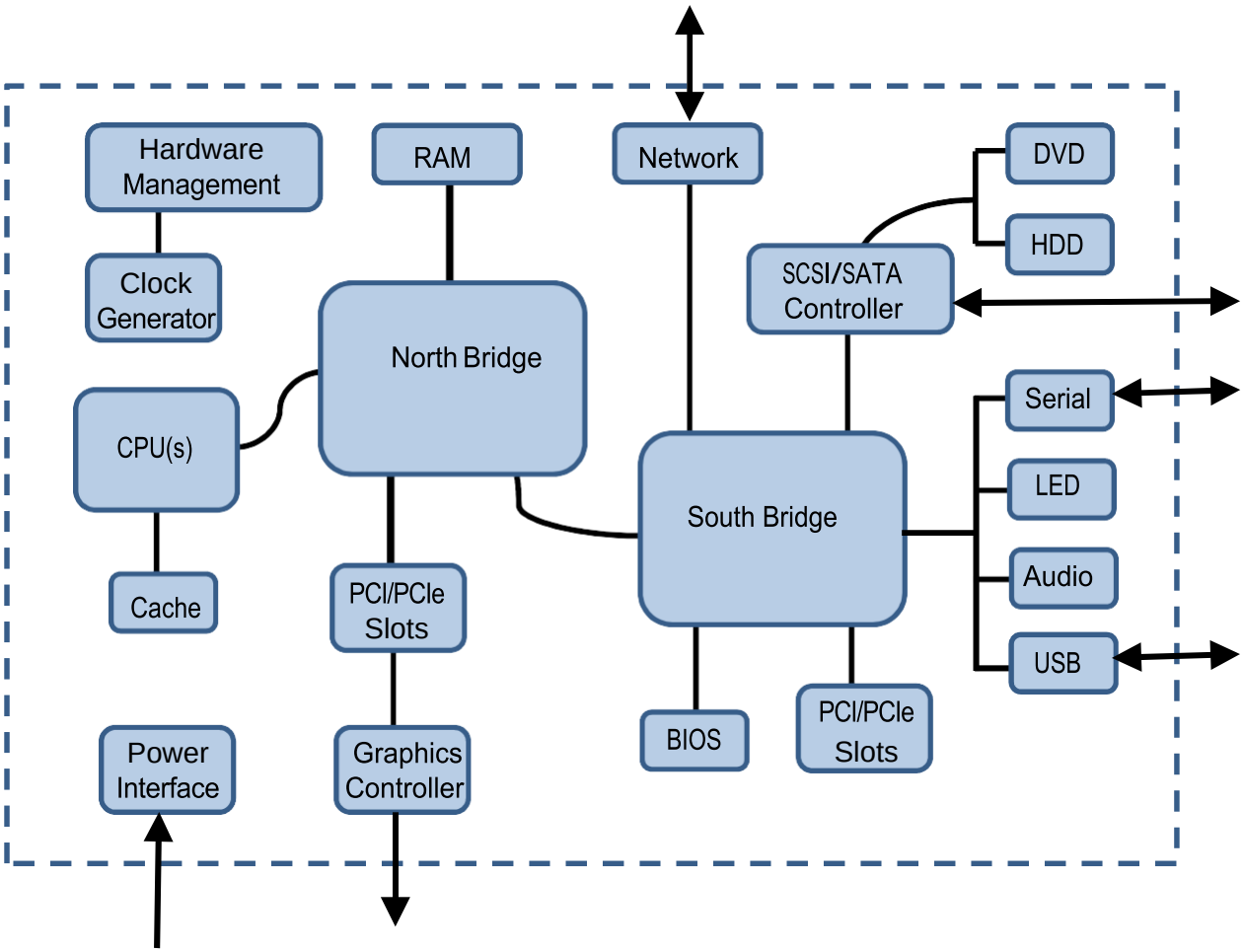
- A general-purpose computing platform with an AMD Opteron x86 Processor executing Horizon 6 on Windows Server 2008 R2 SP1 Standard, Windows Server 2008 R2 SP1 Enterprise, Windows Server 2008 R2 SP1 Datacenter, Windows Server 2012 Standard, Windows Server 2012 Datacenter, Windows Server 2012 R2 Standard, Windows Server 2012 R2 Datacenter.
- A general-purpose computing platform with an Intel Core i3, Core i5, Core i7, or Xeon x86 Processor executing Horizon 6 on Windows Server 2008 R2 SP1 Standard, Windows Server 2008 R2 SP1 Enterprise, Windows Server 2008 R2 SP1 Datacenter, Windows Server 2012 Standard, Windows 7 SP1 Professional and Windows 7 SP1 Enterprise.

Because the VMware Horizon JCE Module is defined as a software cryptographic module, it possesses both a physical cryptographic boundary and a logical cryptographic boundary. Sections 2.2.1 and 2.2.2 describe the physical and logical boundaries of the module.

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

2.2.1 Physical Cryptographic Boundary

As a software cryptographic 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 Dell PowerEdge R630. These interfaces include the integrated circuits of the system board, processor, network adapters, RAM[9], hard disk, device case, power supply, and fans. See Figure 3 for a block diagram of the Dell PowerEdge R630.



Key:

BIOS – Basic Input/Output System	PCIe – PCI express
CPU – Central Processing Unit	HDD – Hard Disk Driver
SATA – Serial Advanced Technology Attachment	DVD – Digital Video Disk
	USB – Universal Serial Bus
SCSI – Small Computer System Interface	RAM – Random Access Memory
PCI – Peripheral Component Interconnect	
LED – Light Emitting Diode	

Figure 3 – Dell R630 Server Block Diagram

[9] RAM – Random Access Memory

2.2.2 Logical Cryptographic Boundary

Figure 3 shows a logical block diagram of the module and its 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 the "VMware Horizon JCE Module" in Figure 4. The module is a cryptographic provider to the Java Runtime Environment (JRE). Java-based applications such as the Tomcat server call the module's services through the JRE. 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.

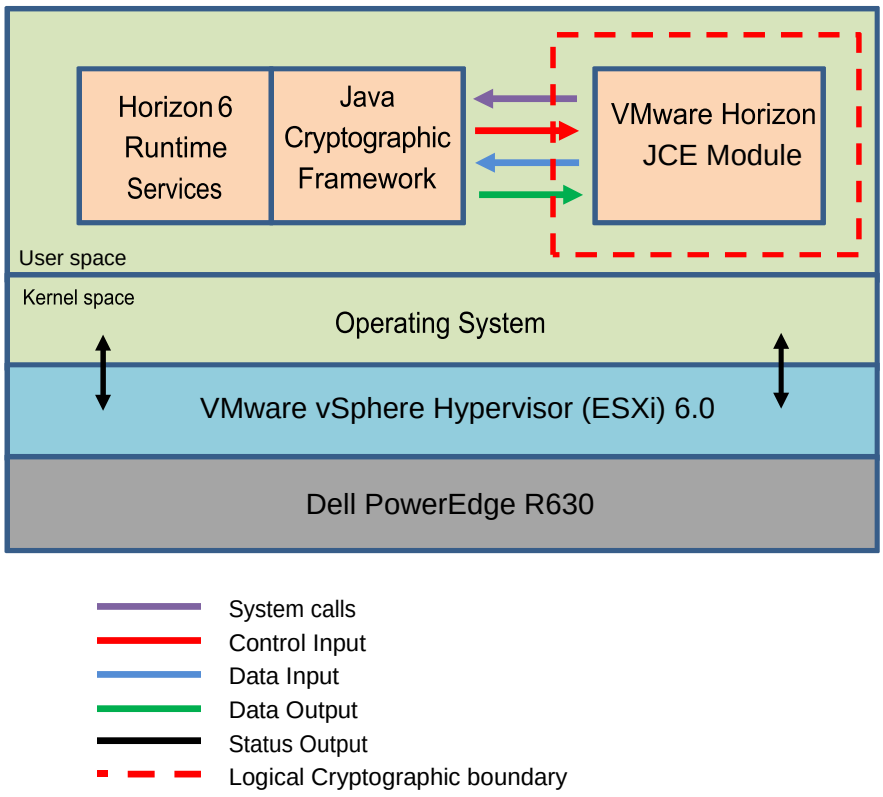


Figure 4 - VMware Horizon JCE Module Logical Cryptographic Boundary

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 has no physical characteristics. Thus, the module's manual controls, physical indicators, and physical and electrical characteristics are those of the host device. 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	Method calls that accept, as their arguments, data to be used or processed by the module
Data Output	Network port, Serial port, SCSI/SATA Controller, USB port	Arguments for a method that specify where the result of the method is stored
Control Input	Network port, Serial port, USB port, Power button	Method calls utilized to initiate the module and the method calls used to control the operation of the module
Status Output	Network port, Serial port, USB port, Graphics controller	Thrown exceptions for method calls
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 Crypto Officer (CO) role and a User role. As the module does not support an authentication mechanism, 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 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 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	CSP and Type of Access
Initialize module	Performs integrity check and power-up self-tests	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 - User Services

Service	Description	CSP and Type of Access
Generate random number	Returns the specified number of random bits to calling application	DRBG Seed – WRX DRBG C Value – WRX DRBG V Value – WRX DRBG Entropy – WRX
Generate message digest	Compute and return a message digest using SHS algorithms	None
Generate keyed hash (HMAC)	Compute and return a message authentication code	HMAC[10] key – RX
Generate Cipher Hash (CMAC[11])	Compute and return a cipher message authentication code	AES CMAC Key – RX Triple-DES CMAC Key – RX
Generate symmetric key	Generate and return the specified type of symmetric key	Triple-DES Key – W
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 asymmetric key pair	Generate and return the specified type of asymmetric key pair	RSA private/public key – W DSA private/public key – W
Key Wrapping	Perform key wrap with RSA public key	RSA Public Key – RX
Key Unwrapping	Perform key unwrap with RSA private key, AES key, and Triple-DES Key	RSA Private Key – RX AES Key – RX Triple-DES Key – RX
Key Transport	Perform key transport using AES key or Triple-DES Key, and HMAC Key	AES Key – RX Triple-DES Key – RX HMAC Key – RX
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	RSA public key – RX DSA public key – RX

[10] HMAC – (keyed-) Hash-based Message Authentication Code
[11] CMAC – Cipher-based Message Authentication Code

2.5 Physical Security

The VMware Horizon JCE 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 with Horizon 6, version 6.2 with Sun JRE 1.8 on Windows Server 2012R2 Datacenter hosted on VMware vSphere Hypervisor (ESXi) 6.0 running on Dell PowerEdge R630 with Intel(R) Xeon(R) E5-2630 CPU and also with Horizon 6, version 6.2 with Sun JRE 1.8 on Windows 7 SP1 Enterprise (32 bit) hosted on VMware vSphere Hypervisor (ESXi) 6.0 running on Dell PowerEdge R630 with Intel(R) Xeon(R) E5-2630 CPU. The cryptographic module will utilize the Java Virtual Machine (JVM) provided by Sun JRE v1.8. The JVM is responsible for relaying information from calling applications to the cryptographic module. All cryptographic keys and CSPs are under the control of the OS, which protects the module's 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 following sections highlight the module's cryptographic keys and critical security parameters.

2.7.1 Approved Cryptographic Algorithms

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

Table 5 - FIPS-Approved Algorithm Implementations

Algorithm	Certificate Number
AES in ECB[12], CBC[13], CFB[14]-128, OFB[15], and CMAC modes encrypt/decrypt with 128-, 192- and 256-bit keys	3554
Triple-DES in ECB, CBC, CFB-8, CFB-64, and CMAC modes encrypt/decrypt; KO[16] 1	1987
RSA (FIPS 186-4) Key Generation with 2048- and 3072-bit key range	1830
RSA (PKCS[17] #1 v1.5) Signature Generation and Verification	1830
RSA (PSS[18]) Signature Generation and Verification	1830
DSA (FIPS 186-4) Key Generation with 2048- and 3072-bit keys	992
DSA Signature Generation and Verification	992
SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 hash	2929
HMAC-SHA-1, HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512 keyed hash	2268
SP 800-90A Hash_DRBG	905
KTS using AES* or Triple-DES**, and HMAC	3554 (AES), or 1987 (Triple-DES), and 2268 (HMAC)

[12] ECB – Electronic Codebook
[13] CBC – Cipher Block Chaining
[14] CFB – Cipher Feedback
[15] OFB – Output Feedback
[16] KO – Keying Option
[17] PKCS – Public-Key Cryptography Standards
[18] PSS – Probabilistic Signature Scheme

- KTS (AES Cert. #3554 and HMAC Cert. #2268; key establishment methodology provides between 128 and 256 bits of encryption strength)
- KTS (Triple-DES Cert. #1987 and HMAC Cert. #2268; key wrapping; key establishment methodology provides 112 bits of encryption strength)

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

- RSA (key wrapping; key establishment methodology provides between 112 and 128 bits of encryption strength; non-compliant less than 112 bits of encryption strength)
- AES (Cert. #3554, key unwrapping; key establishment methodology provides between 128 and 256 bits of encryption strength)
- Triple-DES (Cert. #1987, key unwrapping; key establishment methodology provides 112 bits of encryption strength)

Caveats:

- Additional information concerning SHA-1, Diffie-Hellman key agreement/key establishment, RSA 1024-bit signature generation, RSA key transport, DSA key generation, DSA signature generation, 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; No assurance of the minimum strength of generated keys.

2.7.2 Non-Approved Algorithms

The module employs non-Approved cryptographic algorithms and services, which are accessible by the operator of the module. The use of these algorithms and services leads the module to operate in the non-Approved mode of operation. Their use, while operating in the FIPS-Approved mode, is strictly prohibited. Table 6 lists the non-Approved algorithms services provided by the module.

Table 6 - VMware Horizon JCE Module Non-Approved Algorithms and Services

Algorithm	Service
RC2[19]	Encryption; Decryption
RC4	Encryption; Decryption
TWOFISH	Encryption; Decryption
IES[20]/ECIES[21]	Encryption; Decryption
DES	Encryption; Decryption
Triple-DES (2-key)[22]	Encryption; Decryption
MD2[23]/MD5	Hashing
RIPE MD	Hashing
TIGER	Hashing
ISO9797[24] Alg3 MAC	Hash-based Message Authentication Code
RSA	Key Generation; Signature Generation; Key Wrapping (Key size < 2048)
DSA	Key Generation; Signature Generation (Key size < 2048)
SHA-1	Signature Generation
Non-compliant Key Wrapping Using AES or Triple-DES	Key Wrapping

[19] RC – Rivest Cipher
[20] IES – Integrated Encryption Scheme
[21] ECIES – Elliptic Curve IES
[22] 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
[23] MD – Message Digest
[24] ISO – International Organization for Standards

2.7.3 Critical Security Parameters

The module supports the CSPs listed below in Table 7.

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

CSP	CSP Type	Generation[25] / Input	Output	Storage	Zeroization	Use
AES key	AES 128-, 192-, 256-bit key	API call parameter	Output via GPC[26] INT path[27]	Plaintext in volatile memory	Reboot OS; Cycle host power	Encryption, Decryption
AES CMAC Key	AES CMAC 128-, 192, 256-bit key	API call parameter	Output via GPC INT path	Plaintext in volatile memory	Reboot OS; Cycle host power	Message Authentication with AES
Triple-DES key	Triple-DES 168-bit secure key	API call parameter or internally generated	Output via GPC INT path	Plaintext in volatile memory	Reboot OS; Cycle host power	Encryption, decryption
Triple-DES CMAC Key	Triple-DES CMAC 168-bit key	API call parameter	Output via GPC INT path	Plaintext in volatile memory	Reboot OS; Cycle host power	Message Authentication with Triple-DES
HMAC key	160- to 512-bit HMAC Key	API call parameter	Output via GPC INT path	Plaintext in volatile memory	Reboot OS; Cycle host power	Message Authentication with SHA-1 and SHA-2 family
RSA private key	RSA 2048-, 3072-bit key	API call parameter or internally generated	Output via GPC INT path	Plaintext in volatile memory	Reboot OS; Cycle host power	Signature generation, key unwrapping
RSA public key	RSA 2048-, 3072-bit key	API call parameter or internally generated	Output via GPC INT path	Plaintext in volatile memory	Reboot OS; Cycle host power	Signature verification, key wrapping
DSA private key	DSA 224-bit key	API call parameter or internally generated	Output via GPC INT path	Plaintext in volatile memory	Reboot OS; Cycle host power	Signature generation
DSA public key	DSA 2048-bit key	API call parameter or internally generated	Output via GPC INT path	Plaintext in volatile memory	Reboot OS; Cycle host power	Signature verification
DRBG Seed	880-bit random value	API call parameter or Internally generated	Never	Plaintext in volatile memory	Reboot OS; Cycle host power	Seed input to SP 800-90 Hash_DRBG
DRBG Entropy	440-bit random value	API call parameter or Internally generated	Never	Plaintext in volatile memory	Reboot OS; Cycle host power	Entropy input to SP 800-90 Hash_DRBG
Hash DRBG V value	Internal hash DRBG state value	Internally generated	Never	Plaintext in volatile memory	Reboot OS; Cycle host power	Used for SP 800-90 Hash_DRBG
Hash DRBG C value	Internal hash DRBG state value	Internally generated	Never	Plaintext in volatile memory	Reboot OS; Cycle host power	Used for SP 800-90 Hash_DRBG

2.8 Self-Tests

[25] 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
[26] GPC – General Purpose Computer
[27] GPC INT Path defined in Implementation Guidance Section 7.7

Cryptographic self-tests are performed by the module after the module begins normal operation as well as when a random number or asymmetric key pair is created. The following sections list the self-tests performed by the module, their expected error status, and 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 restarts the JRE or reboots the OS. 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 JRE and enter an error state. After entering the error state, all subsequent calls to the module requiring cryptographic operation or data output will be rejected, ensuring that these abilities of the module are inhibited. In order to resolve a cryptographic self-test error, the JRE must unload the module and then reload it. If the error persists, the module must be reinstalled.

The VMware Horizon JCE 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)
    - HMAC with SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 KAT
    - SP 800-90A Hash_DRBG
- DSA Pairwise Consistency Check

2.8.2 Conditional Self-Tests

Conditional self-tests are performed by the module whenever a new random number or a new asymmetric key pair is generated. If an error is encountered during an RSA or DSA pairwise consistency test, the module will return an error to the JRE and enter an error state. After entering the error state, all subsequent calls to the module requiring cryptographic operation or data output will be rejected. The JRE is responsible for resolving the error and returning the module to an operational state. This usually consists of unloading and reloading the module. No data will be returned by the module and the operation must be performed again. If the error persists, the module must be reinstalled.

The VMware Horizon JCE Module performs the following conditional self-tests:

- SP 800-90A Hash_DRBG Continuous RNG Test
- RSA Pairwise Consistency Test for key pair generation
- DSA Pairwise Consistency Test for key pair generation

2.8.3 Critical Functions Tests

The SP 800-90A Hash_DRBG employed by the cryptographic module includes four critical functions. These critical functions include instantiation, generation, reseed, and uninstantiation. Each function is tested by the module during the module's power-up self-tests. If any of these critical functions fail, the module will return an error to the JRE and will enter an error state. All subsequent calls to the module requiring cryptographic operation or data output will be rejected. The JRE will then proceed to unload and reload the module in order to reattempt these critical functions tests. If the error persists, the module must be reinstalled.

The VMware Horizon JCE Module performs the following critical functions tests:

- DRBG Instantiate Critical Function Test
- DRBG Generate Critical Function Test
- DRBG Reseed Critical Function Test
- DRBG Uninstantiate Critical Function Test

2.9 Mitigation of Other Attacks

This section is not applicable. The modules do not claim to mitigate any other attacks.

3 Secure Operation

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

3.1 Crypto Officer Guidance

Installation and operation of the VMware Horizon JCE Module requires the proper installation of Horizon 6 servers and agents. The sections below provide a brief summary of the installation procedures for Horizon 6. For a more comprehensive instruction set, please refer to the *Horizon 6 Installation Guide* provided by VMware. The VMware Horizon JCE Module operates in the FIPS-Approved mode of operation after the instructions for Initial Setup (3.1.1) and Secure Installation (3.1.2) are followed.

All guides mentioned within in these instructions are freely available for download at http://www.vmware.com. These instructions assume that the CO is familiar with VMware vSphere 6.0 and VMware Horizon 6 products.

3.1.1 Initial Setup

Prior to the secure installation of Horizon 6, the CO shall prepare the virtual environment required to securely operate the Horizon 6 services. This includes installing the latest version of VMware vSphere 6.0 (see *vSphere Installation and Setup*). Included in this installation is the VMware vSphere Hypervisor (ESXi) 6.0, the vSphere 6.0 vSphere Client, and the vSphere 6.0 vCenter Server, all of which are prerequisites to installing Horizon 6.

After installing the VMware vSphere 6.0 virtual environment, the CO shall log into the vCenter Server and create a Virtual Machine capable of running Windows 7 SP1 (32 bit) or Windows Server 2012. Once the VM has been provisioned the CO shall complete installation as described in section 3.1.2.

3.1.2 Secure Installation

In order to install the VMware Horizon JCE Module, the CO shall follow the installation instructions provided in the Horizon 6.2 installation guide in order to securely install and configure the relevant Horizon 6 component (Connection Server, Security Server or Agent) which utilizes the VMware Horizon JCE Module. A brief summary of the installation steps is provided:

- Log into the Windows Operating System using an account with appropriate administrative rights
- Ensure the Windows Operating System has been configured to take advantage of FIPS based cryptography
- Run the relevant Horizon 6 installer (Connection Server and Security Server share the same install binary but the agent is separate package)
- When prompted select the option for FIPS based cryptography
- Complete the installation

Successful completion of installing a Connection Server can be established by accessing the View Administrator UI. A Security Server is successfully installed when it can be used to connect from a client to a Connection Server. Successful agent installs can be verified by ensuring the desktop or RDSH server is shown as "Available" when added to a farm (for RDSH) or a pool (for desktops).

3.1.3 VMware Horizon JCE Module Secure Operation

Following the successful installation of the Horizon 6 components the CO shall ensure the relevant Horizon 6 services are running. After following the steps outlined in Sections 3.1.1 and 3.1.2, the Horizon components will use the VMware Horizon JCE Module for operation in the FIPS-Approved mode. The CO shall follow the guidelines in the *View Security Guide* in order to securely configure and operate the VMware Horizon JCE Module. Additionally, the CO shall ensure the module is operated in accordance with the transition rules specified in SP 800-131A. Furthermore, the transition tables available at the CMVP Web site (http://csrc.nist.gov/groups/STM/cmvp/) can be referenced to inform users of the risks associated with using a particular algorithm and a given key length.

When the module swaps between using approved and non-approved services the operator shall re-initialize the module so that cryptographic keys and CSPs are destroyed in the volatile memory.

3.2 User Guidance

The VMware Horizon JCE Module is designed for use by VMware Horizon. 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 4. The user is responsible for reporting to the CO if any irregular activity is noticed.

4 Acronyms

Table 8 describes the acronyms used in this Security Policy.

Table 8 – Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
API	Application Programming Interface
BIOS	Basic Input/Output System
CBC	Cipher Block Chaining
CCM	Counter with CBC-MAC
CFB	Cipher Feedback
CMAC	Cipher-based Message Authentication Code
CMVP	Cryptographic Module Validation Program
CO	Cryptographic Officer
CPU	Central Processing Unit
CSE	Communications Security Establishment
CSP	Critical Security Parameter
DES	Data Encryption Standard
DRBG	Deterministic Random Bit Generator
DSA	Digital Signature Algorithm
DVD	Digital Video Disk
ECB	Electronic Code Bank
ECIED	Elliptic Curve IES
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FIPS	Federal Information Processing Standard
GPC	General Purpose Computer
GUI	Graphical User Interface
HDD	Hard Disk Drive
HMAC	(keyed-) Hash Message Authentication Code
HTTPS	Secure Hyper-Text Transfer Protocol
IES	Internet Key Exchange
ISO	International Organization for Standards

Acronym	Definition
JCE	Java Crypto Extension
JVM	Java Virtual Machine
KAT	Known Answer Test
KO	Keying Option
LCD	Liquid Crystal Display
LED	Light Emitting Diode
MD	Message Digest
NIST	National Institute of Standards and Technology
OFB	Output Feedback
OS	Operating System
OVA	Open Virtual Appliance
OVF	Open Virtualization Format
PCI	Peripheral Component Interconnect
PCI(e)	Peripheral Component Interconnect (express)
PCT	Pairwise Consistency Test
PKCS	Public Key Cryptography Standard
PSS	Probabilistic Signature Scheme
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
SP	Security Policy
USB	Universal Serial Bus
VPN	Virtual Private Network

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