VMware, Inc.

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

VMware's ESXboot Cryptographic Module

Software Version: 1.0

FIPS 140-3 Non-Proprietary Security Policy

FIPS Security Level: 1
Document Version: 0.8

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1 General

1.1 Security level

The cryptographic module meets the overall requirements applicable to Level 1 security of FIPS 140-3.

Table 1 – Security Levels

	Security Level	
ISO/IEC 24759 Section 6.	**FIPS 140-3 Section Title**	**Security Level**
1	General	1
2	Cryptographic Module Specification	1
3	Cryptographic Module Interfaces	1
4	Roles, Services, and Authentication	1
5	Software/Firmware Security	1
6	Operational Environment	1
7	Physical Security	N/A
8	Non-Invasive Security	N/A
9	Sensitive Security Parameters Management	1
10	Self-Tests	1
11	Life-Cycle Assurance	1
12	Mitigation of Other Attacks	N/A

1.2 Glossary

Table 2 – Glossary

Term/Acronym	Description
AES	Advanced Encryption Standard
API	Application Programming Interface
CMVP	Cryptographic Module Validation Program (FIPS 140)
CO	Crypto Officer
CPU	Central Processing Unit
CSP	Critical Security Parameter
DEP	Default Entry Point
EFI	Extensible Firmware Interface
ESX	Elastic Sky X
ESXi	Elastic Sky X Integrated
FIPS	Federal Information Processing Standard
HMAC	Hash-based Message Authentication Code
IEC	International Electrotechnical Commission
INCITS	InterNational Committee for Information Technology Standards
ISO	International Organization for Standardization
MPI	Multiple Precision Integer
OS	Operating System
PKCS	Public Key Cryptography Standards
PSP	Public Security Parameter
RAM	Random Access Memory

RSA	Rivest–Shamir–Adleman
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
SSP	Sensitive Security Parameter
UEFI	Unified Extensible Firmware Interface
USA	United States of America

2 Cryptographic Module Specification

2.1 Purpose

The purpose of this document is to describe the secure operation of VMware's ESXboot Cryptographic Module including the initialization, roles, and responsibilities of operating the product in an Approved mode of operation.

VMware's ESXboot Cryptographic Module is a FIPS 140-3 Security Level 1 validated software cryptographic module. This module is used by the ESXi Bootloader to aid in the UEFI Secure Boot process. The bootloader checks that the OS has been properly signed and checks the integrity of the OS before passing control over to it. VMware's ESXboot Cryptographic Module is what provides the cryptographic functions to accomplish this.

2.2 Cryptographic Boundary

For FIPS 140-3 purposes, VMware's ESXboot Cryptographic Module, version 1.0, is classified as a Level 1 multi-chip standalone cryptographic module running on UEFI firmware version 2.x. The cryptographic boundary of the module is defined as the binary `crypto64.efi`. The physical perimeter of the module is defined as the enclosure of a general-purpose computing device on which it runs.

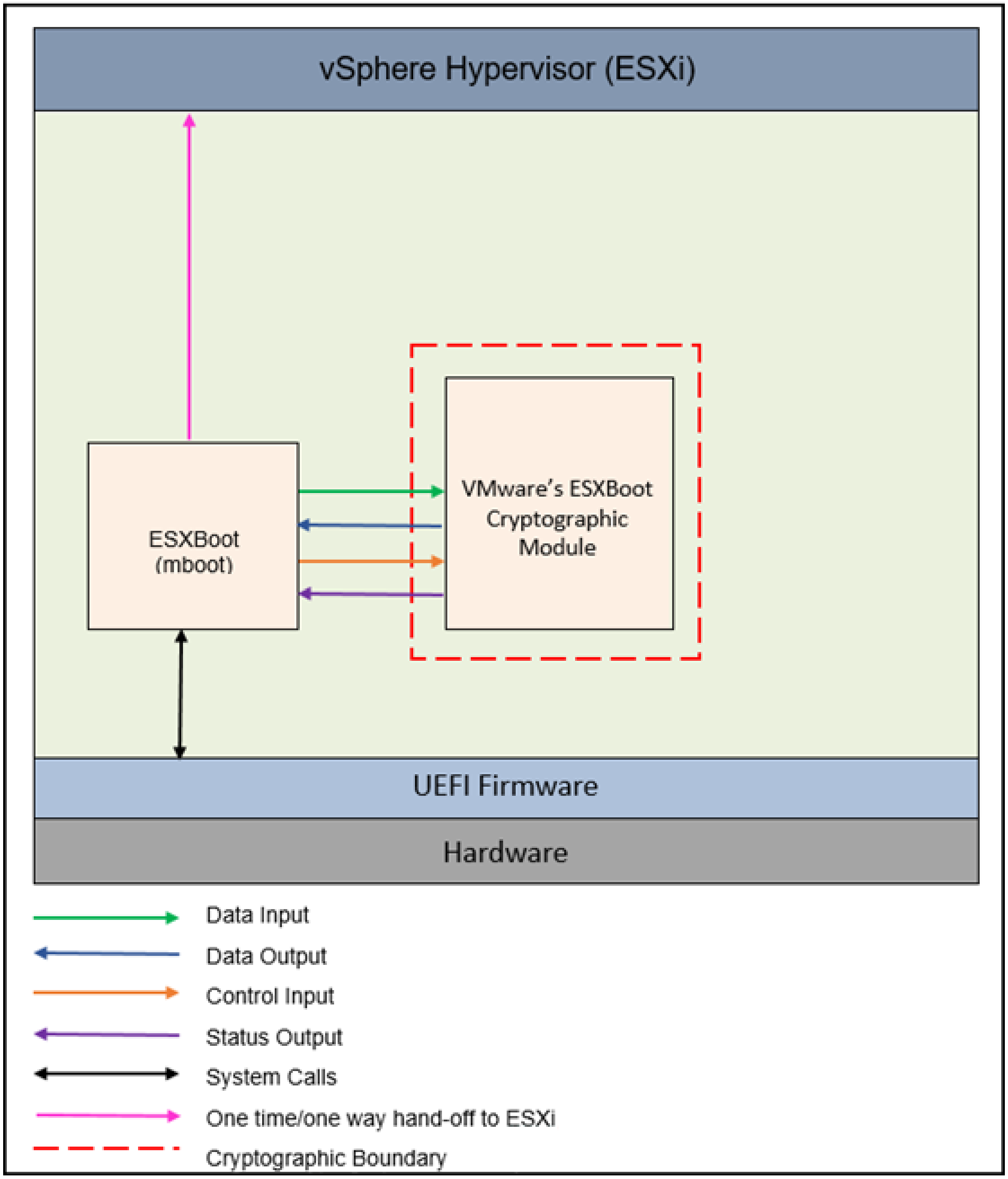

Figure 1 - VMware's ESXboot Cryptographic Module Cryptographic Boundary and Block Diagram

2.3 Tested Platforms

VMware's ESXboot Cryptographic Module has been tested for validation on the following platforms:

Table 3 – Tested Operational Environments

#	Operating System	Hardware Platform	Processor	PAA/Acceleration

1	UEFI firmware version 2.5	Dell PowerEdge R740	Intel Xeon Gold 6126	None
2	UEFI firmware version 2.7	Dell PowerEdge R740	Intel Xeon Gold 6230R	None
3	UEFI firmware version 2.7	Lenovo ThinkSystem HR350A	Ampere Computing eMAG	None

VMware is claiming the following Vendor Affirmed operational environments:

Table 4 – Vendor Affirmed[1] Operational Environment

#	Operating System	Hardware Platform
1	UEFI firmware version 2.x	Dell PowerEdge R650 with Intel Xeon Gold 6330

2.4 Modes of Operation

The module only operates in an Approved mode of operation. Please refer to Section 11 for details on this.

2.5 FIPS Approved Algorithms

VMware's ESXboot Cryptographic Module implements the following FIPS-approved algorithms:

Table 5 – Approved Algorithms

CAVP Cert.	Algorithm and Standard	Mode / Method	Description / Key Size(s) / Key Strength(s)	Use / Function
A1357	RSA FIPS 186-4	PKCS #1 v1.5 Signature Verification	1024, 2048, 3072 and 4096 bit keys	RSA Signature Verification service
A1357	HMAC FIPS 198-1	HMAC-SHA-224, SHA-256, SHA-384, SHA-512	112 - 524288 bit keys (byte-oriented)	Generate Keyed Hash service Software Integrity Test
A1357	SHS FIPS 180-4	SHA-224, SHA-256, SHA-384, SHA-512	BYTE only	Generate Hash service Prerequisite for RSA and HMAC

The module does not implement any algorithms that fall under any of the following categories:

[1] The CMVP makes no statement as to the correct operation of the module or the security strengths of the generated keys when ported and executed in an operational environment not listed on the validation certificate

- Non-Approved Algorithms Allowed in the Approved Mode of Operation
- Non-Approved Algorithms Allowed in the Approved Mode of Operation with No Security Claimed
- Non-Approved Algorithms Not Allowed in the Approved Mode of Operation

3 Cryptographic Module Interfaces

As a software-only module, VMware's ESXboot Cryptographic Module provides an API logical interface for invocation of FIPS 140-3 approved cryptographic functions. The functions shall be called by the referencing application, which assumes the operator role during application execution. The API, using input parameters, output parameters, and function return values, defines the five FIPS 140-3 logical interfaces: data input, data output, control input, control output and status output.

Table 6 – Ports and Interfaces

Physical Port	Logical Interface	Data that passes over port / interface
All information travels through the module's API; with the module's process memory being physically in RAM and executing on the platform's CPU. No information is transmitted by the module over a physical port on the platform.	Data Input	The data read from memory area(s) provided to the invoked API functions via parameters that point to the memory area(s).
	Data Output	The data written to memory area(s) provided to the invoked API functions via parameters that point to the memory area(s).
	Control Input	The API function invoked and API function parameters designated as control inputs.
	Control Output	The module does not output any commands, signals, or control data used to control another module.
	Status Output	The return value of the invoked API function.

4 Roles, Services and Authentication

VMware's ESXboot Cryptographic Module supports the *Crypto Officer* role. The operator of the module will assume this role. The Crypto Officer role is assumed implicitly for all module services. The module does not support concurrent operators and does not authenticate the Crypto Officer role.

4.1 Services and SSP Access

The Crypto Officer role can perform all the services offered by the module. Note, as the module always operates in an Approved mode of operation, all the module's services are approved services. The module does not support any Non-Approved Services.

The module allows controlled access to the SSPs contained within it. The following tables define the access that an operator or an application has to each SSP while operating VMware's ESXboot Cryptographic Module in a given role performing a specific service (command). The permissions are categorized as a set of five separate permissions: generate [G] (The SSP is generated or derived by this operation), read [R] (the SSP can be output by this operation), write [W] (the SSP can be updated, imported, or written by this operation), execute [E] (the SSP is used in performing a cryptographic operation) and Zeroise [Z] (the SSP will be zeroised by this operation). If no permission is listed, then an operator outside VMware's ESXboot Cryptographic Module has no access to the SSP.

Table 7 – Roles, Service Commands, Input and Output

Role	Service	Input	Output
Crypto Officer	Show Module Version (ApiVersion, ModuleVersion)	N/A	Status
Crypto Officer	Show Status[2]	API call parameters	Status
Crypto Officer	Perform Self-Tests[3]	Manually power-cycle or reboot host device	Status
Crypto Officer	RSA Signature Verification (RsaInit, RsaPkcs1Verify)	API call parameters, key, signed data	Status, result
Crypto Officer	Generate Hash (Sha256Ret, Sha512Ret)	API call parameters, plaintext	Status, hash
Crypto Officer	Generate Keyed Hash (HmacRet)	API call parameters, key, plaintext	Status, hash
Crypto Officer	MPI (Multiple Precision Integer) Management Functions (MpiLset, MpiReadBinary, MpiReadString)	API call parameters	Status

[2] As noted in section 3, the status output is the return value of the invoked API function, so there is no separate "Show Status" API.

[3] In order to perform the self-tests on-demand, the CO should power-cycle or reboot the host device.

Crypto Officer	Zeroisation[4]	Manually power down or power-cycle host device	Status

Table 8 – Approved Services

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys and/or SSPs	Indicator
Show Module Version	ApiVersion, ModuleVersion API parameters	None	None	Crypto Officer	None	N/A – These are just parameters
Show Status	Return value of each API function	None	None	Crypto Officer	None	Zero (0) indicates success
Perform Self-Tests	On-demand self-tests are performed by power-cycling or rebooting the host device	HMAC, RSA, SHS	HMAC Key (CSP) RSA Verification Key (PSP)	Crypto Officer	E	Protocol interface structure is installed, Status >= 0 indicates success
RSA Signature Verification	RsaInit, RsaPkcs1Verify API functions	RSA, SHS	RSA Verification Key (PSP)	Crypto Officer	WE	Zero (0) indicates success
Generate Hash	Sha256Ret, Sha512Ret API functions	SHS	None	Crypto Officer	None	Zero (0) indicates success
Generate Keyed Hash	HmacRet API function	HMAC, SHS	HMAC Key (CSP)	Crypto Officer	WE	Zero (0) indicates success
MPI (Multiple Precision Integer) Management Functions	MpiLset, MpiReadBinary, MpiReadString API functions	None	None	Crypto Officer	None	Zero (0) indicates success

[4] In order to perform the zeroisation service, the CO should either power down or power-cycle the host device. The zeroisation shall be performed while the host device and module are under the control of the operator.

Zeroisation	Power down or power-cycle the host device	None	HMAC Key (CSP) RSA Verification Key (PSP)	Crypto Officer	Z	Protocol interface structure is installed, Status >= 0 indicates success

4.2 Authentication Mechanisms and Strength

FIPS 140-3 Security Level 1 does not require *role-based* or *identity-based* operator authentication. VMware's ESXboot Cryptographic Module will not authenticate the operator. As a result, the 'Roles and Authentication' table from SP 800-140B is not included.

5 Software/Firmware Security

VMware's ESXboot Cryptographic Module implements an HMAC-SHA2-512 Software Integrity Test. The test is conducted over the whole module binary, `crypto64.efi`, and can be initiated on-demand by rebooting the module's host platform. Please refer to Section 10.1 for details about when an error occurs during the integrity test.

6 Operational Environment

The operational environment is modifiable, and there are no specific security rules, settings or restrictions required to configure the operational environment. Since this is a Level 1 module, the requirements AS06.02 through AS06.08 from ISO/IEC 24759 are applicable. The OE does not require any specific configuration to load the module in an Approved mode of operation. The module is installed by the manufacturer to initialize and run in the Approved mode.

Additionally, the UEFI operational environment does not have multiple concurrent application processes. It is a single-process system. It is also single processor: all but one hardware CPU thread is halted while UEFI is in control of the machine. The module does not spawn any processes or threads.

7 Physical Security

VMware's ESXboot 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 140-3 requirements for physical security are not applicable and the tables for ‘Physical Security Inspection Guidelines’ from SP 800-140B has been excluded from this document.

The host platform contains production-grade components which have industry-standard passivation techniques applied to them. Additionally, the enclosure of the device is a metal enclosure made of production-grade materials.

8 NON-INVASIVE SECURITY

This section is not applicable as the module does not implement any non-invasive mitigation techniques.

9 Sensitive Security Parameters Management

The table below lists the SSPs contained in and used by VMware's ESXboot Cryptographic Module. The CAVP certificate number for each algorithm is #A1357. **Note**: SSPs cannot be output from the module.

Table 9 – SSPs

Key/SSP Name/Type	Strength	Security Function and Cert. Number	Generation	Import / Export	Establishment	Storage	Zeroisation	Use & Related Keys
HMAC Key (CSP)	Variable, greater than or equal to 112 bits	HMAC-SHA2-224, HMAC-SHA2-256, HMAC-SHA2-384, HMAC-SHA2-512 Cert. #A1357	N/A	Input in plaintext via API call within GPC INT pathways.	N/A	Plaintext in RAM	Power-off/Power-cycle	Key used for the purpose of generating and verifying HMAC authentication codes.
RSA Verification Key (PSP)	Variable, modulus size greater than or equal to 1024 bits (80 bits of security strength)	RSA Signature Verification (PKCS1 v1.5) Cert. #A1357	N/A	Input in plaintext via API call within GPC INT pathways.	N/A	Plaintext in RAM	Power-off/Power-cycle	Public key used for the purpose of verifying signed data using RSA with PKCS #1 v1.5 padding.

All the cryptographic keys and other security relevant materials handled by the module can be zeroised by powering down or power-cycling the host device. Since the module does not support any random number generation, the SP 800-140B table 'Non-Deterministic Random Number Generation Specification' has been excluded from this document.

10 SELF-TESTS

10.1 Pre-Operational Self-Tests

VMware's ESXboot Cryptographic Module includes the following Pre-Operational self-test:

- Software Integrity Test (using HMAC-SHA2-512)

10.2 Conditional Self-Tests

VMware's ESXboot Cryptographic Module includes the following Conditional Self-Tests:

- KAT test for HMAC SHA2-512
- KAT for RSA Signature Verification (2048-bit, PKCS #1 v1.5)

10.3 Notes about Self-Tests

- All the above self-tests are invoked automatically upon loading VMware's ESXboot Cryptographic Module via the DEP (default entry point), or by rebooting the host platform.

- VMware's ESXboot Cryptographic Module defines an error state. The module enters this state when any of the self-tests or the installation of the protocol interface fails. After entering the error state, the module returns an error to the operator in the form of a log message with the prefix ‘Crypto module failure:’ and the status code ‘EFI_SECURITY_VIOLATION’ and terminates execution of the EFI image, passing control back to the application. The only way to resume normal operation is to load the module again and pass the preoperational self-tests.

- In accordance with INCITS/ISO/IEC 19790 Section “Pre-operational software/firmware integrity test”, both conditional self-tests are executed before the Software Integrity Test as the HMAC algorithm is used to perform the integrity test. When ESXBoot is finished using the module's services, ESXboot passes control over to ESXi, and control cannot be passed back to either ESXboot or the ESXBoot cryptographic module unless the host device is power-cycled or rebooted. Thus the conditional self-tests will only be run one time during execution of the module.

11 LIFE-CYCLE ASSURANCE

VMware's ESXboot Cryptographic Module is provided to the end-user via the ESXi installer media. There are no specific procedures that need to be followed to ensure the secure operation of the module apart from using the installer to install ESXi and verifying that Secure boot is enabled. There are no specific steps or instructions that need to be followed during the ESXi installation to ensure the module is installed and initialized correctly. Once ESXi is installed on a host device where Secure boot has been enabled, the module will be installed and initialized, and will always operate in the Approved mode.

VMware's ESXboot Cryptographic Module does not support operator authentication and thus does not require any authentication itself.

12 Mitigation of Other Attacks

The module does not mitigate other attacks outside the scope of FIPS 140-3.