Symantec Corporation

Symantec Cryptographic Module

Software Version: 1.1

FIPS 140-2 Non-Proprietary Security Policy

FIPS Security Level: 1
Document Version: 0.6

Prepared for:

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043
United States of America

Phone: +1 408-517-8000
Email: info@symantec.com
http://www.symantec.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 Symantec Cryptographic Module from Symantec Corporation. This Security Policy describes how the Symantec 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 Symantec Cryptographic Module is referred to in this document as SymCrypt Module, 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 Symantec website (www.symantec.com) contains information on the full line of products from Symantec.
- 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 Symantec. With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Submission Package is proprietary to Symantec and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Symantec.

2 Symantec Cryptographic Module

2.1 Overview

As one of the world's largest software companies, Symantec offers a comprehensive portfolio of security, storage, and systems management solutions. Symantec has a broad range of product offerings that range from consumer virus protection to enterprise-class Security Operation Centers (SOCs). One solution that Symantec offers is the Symantec Security Information Manager (SSIM), which utilizes the Symantec Cryptographic Module.

2.1.1 Symantec Security Information Manager

The Symantec Security Information Manager is a high-availability enterprise-class software solution, whose primary purpose is to preempt or detect security incidents while providing the framework to demonstrate compliance. SSIM accomplishes this through its integrated log management, distributed architecture, and automated updates from Symantec's Global Information Network (GIN), which offers real-time intelligence on the latest vulnerabilities and threats from around the world.

As shown in Figure 1 below, SSIM collects security information, called events, from a broad range of applications, services, and security products. It then converts that information into actionable intelligence by using its built-in asset management function for prioritization, and then applying its sophisticated rule-based correlation engine on a normalized event stream. Event data is easily managed and quickly retrieved using SSIM's specialized form of event detail storage, which uses proprietary indexing and compression. Large amounts of diverse event data can be centralized in online or archived event stores using direct-attached storage (DAS), network-attached storage (NAS) or storage area network (SAN). SSIM also embeds a high-performance relational database to store summarized events and data pertaining to incidents, tickets, assets, rules, vulnerabilities, workflow, and reports. This allows for trend reporting and custom SQL[1] queries, with drill down capability into the appropriate event archives.

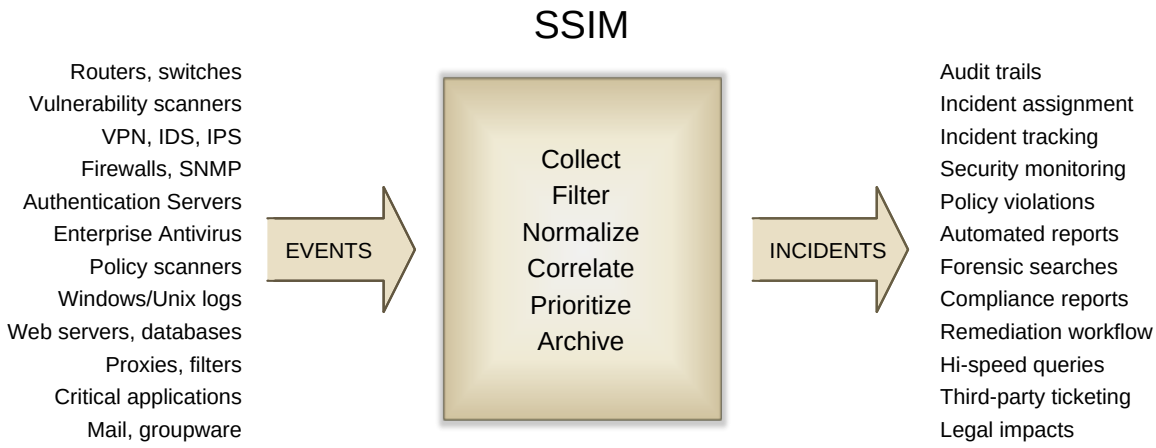

Figure 1 – Symantec Security Information Manager Workflow

The SSIM solution consists of the following major components:

- **Information Manager** – comprises the core functionality of a SSIM deployment. It installs on a standard server platform that supports RHEL (Red Hat Enterprise Linux). It aggregates and

[1] SQL – Structured Query Language

processes event data for correlation, incident management, and archival. It also consists of a comprehensive report engine and an embedded LDAP (Lightweight Directory Access Protocol) directory for centralized access control and multi-domain management. The various roles of the Information Manager (Collection, Correlation, Archival, and Service Provider) can be distributed in local clusters and then federated for fail safety, higher scalability, and global deployments. The Web Configuration Interface and OpenSSH provide administrative access to the Information Manager server via a web browser or a remote secure shell (SSH) connection.

- **Event Collector** – gathers and filters events from event sources. Collectors are installed directly on a security point product or in strategic locations with access to security events. They use application specific *sensors* that retrieve events from a file, database, or syslog. SSIM provides multi-vendor support with over 200 predefined collectors for popular products. It also has universal collectors that can be customized for unique event sources.
- **Event Agent** – handles the communication path between event collectors and the Information Manager. It is a Java-based application that is installed alongside each collector on standard server platforms that support Windows 2012 and Solaris. The agent forwards both raw event data and events that have been filtered and aggregated.
- **Information Manager Console** – provides a bidirectional administrative GUI[2] to the Information Manager. It is a Java-based application used by administrators, analysts, and service desk systems to perform security monitoring functions, such as incident management, reports, and rule definition. It presents both high-level and detailed views of critical security information.

See Figure 2 below for a diagram of the SSIM solution architecture.

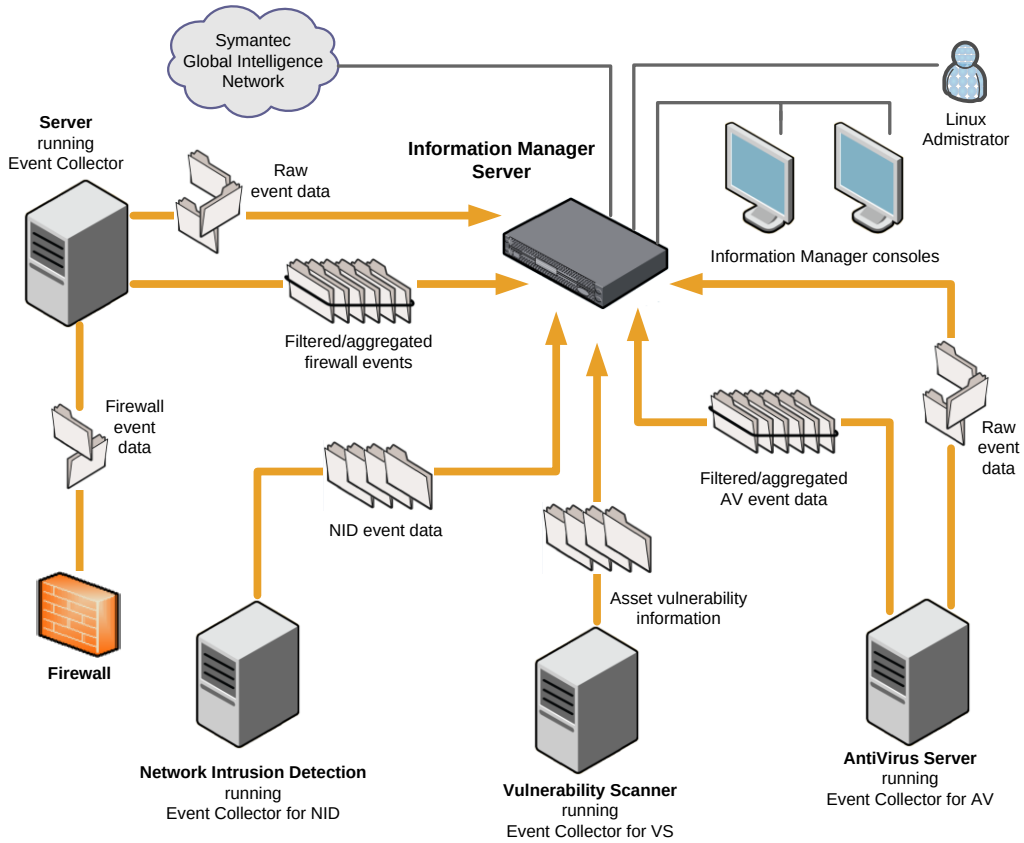

Figure 2 – SSIM Deployment Scenario

[2] GUI – Graphical User Interface

2.1.2 Symantec Cryptographic Module Security

The Symantec Cryptographic Module is a software shared library that resides on various Symantec application components, including the Information Manager server in SSIM. The module includes implementations of the following FIPS-Approved algorithms:

- Advanced Encryption Standard (AES)
- Triple Data Encryption Algorithm (TDEA or Triple-DES[3])
- Secure Hash Algorithm (SHA)
- (Keyed-) Hash Message Authentication Code (HMAC)
- Digital Signature Algorithm (DSA)
- RSA[4] signature generation and verification
- NIST SP800-90A Deterministic Random Bit Generator (DRBG)

The Symantec Cryptographic Module is configured to operate in a FIPS-Approved mode of operation. The Symantec 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 and Services	1
4	Finite State Model	1
5	Physical Security	N/A
6	Operational Environment	1
7	Cryptographic Key Management	1
8	EMI/EMC[5]	1
9	Self-tests	1
10	Design Assurance	1
11	Mitigation of Other Attacks	N/A

2.2 Module Specification

The Symantec Cryptographic Module is a software module with a multi-chip standalone embodiment. The overall security level of the module is 1. The SymCrypt Module is used by calling applications to provide symmetric/asymmetric cipher operation, signature generation/verification, hashing, cryptographic key generation, random number generation, and message authentication functions. The cryptographic boundary of the SymCrypt Module consists of the shared object file "libcrypto.so.1.0.1.e" that is linked with the calling application. The module was tested and found compliant on a Dell Optiplex 755 with an Intel Core 2 Duo processor.

The SymCrypt Module is defined as a software cryptographic module and therefore has a logical boundary in addition to a physical boundary. The physical and logical boundaries are outlined in section 2.2.1 and 2.2.2 respectively.

[3] DES – Data Encryption Standard
[4] RSA – Rivest, Shamir, Adleman
[5] 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. Therefore, the physical boundary of the cryptographic module is defined by the hard enclosure around the host system on which it runs.

The host system consists of a motherboard, a Central Processing Unit (CPU), random access memory (RAM), read-only memory (ROM), hard disk(s), hardware case, power supply, and fans. Other devices may be attached to the hardware appliance such as a monitor, keyboard, mouse, floppy drive, DVD[6] drive, fixed disk drive, printer, video adapter, audio adapter, or network adapter.

Please see Figure 3 for the layout of the physical structure of the host system. The physical cryptographic boundary contains the processor(s) and other hardware components that store and protect the module. The module is stored on the hard disk of the Dell Optiplex 755 with an Intel Core 2 Duo processor and is loaded into RAM by the OS for execution after the host system is powered on. The module remains in RAM while executing until the host system is powered off or until is it unloaded by the OS.

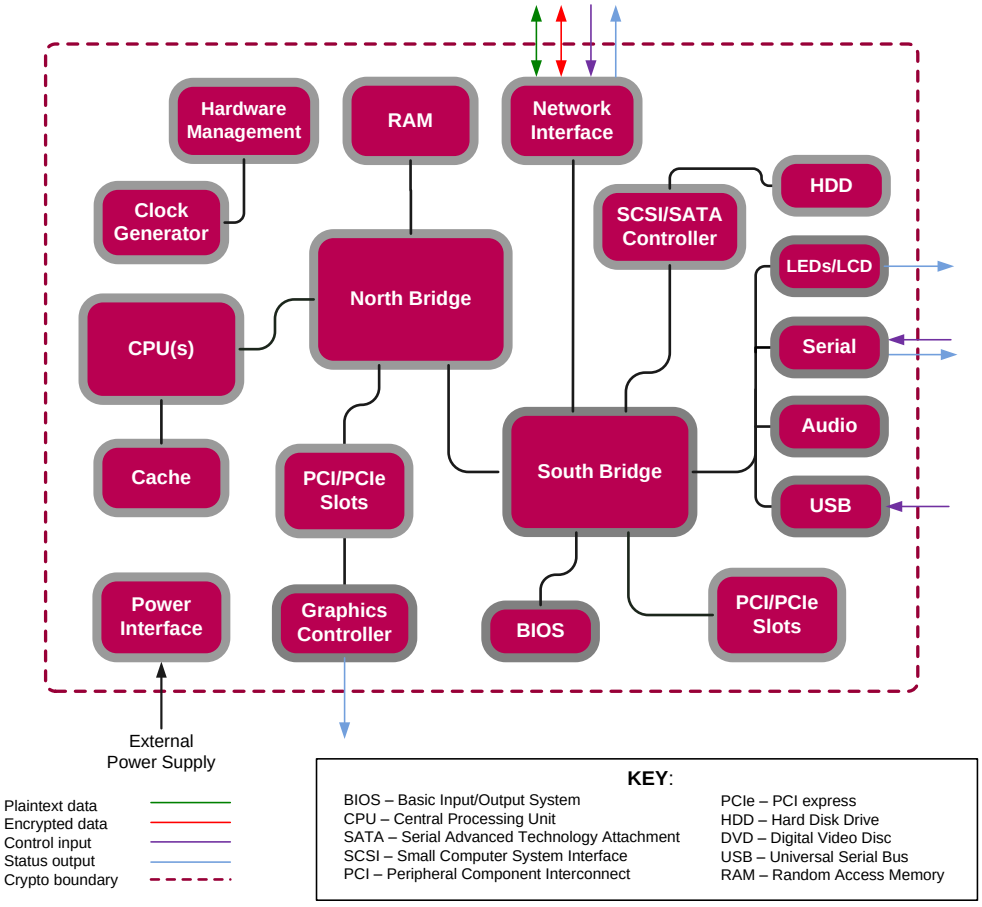

Figure 3 – SymCrypt Module Hardware Platform Physical Block Diagram

[6] DVD – Digital Video Disk

2.2.2 Logical Cryptographic Boundary

Figure 4 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 module is a cryptographic library that provides cryptographic services for other software applications developed by Symantec. In this document, those applications will be referred to collectively as the calling applications. The module is used by the calling application to provide symmetric and asymmetric cipher operation, signature generation and verification, hashing, cryptographic key generation, random number generation, message authentication functions, and secure key agreement/key exchange protocols. The module is entirely contained within the physical cryptographic boundary described in Figure 3.

The module's logical cryptographic boundary is shown below in Figure 4.

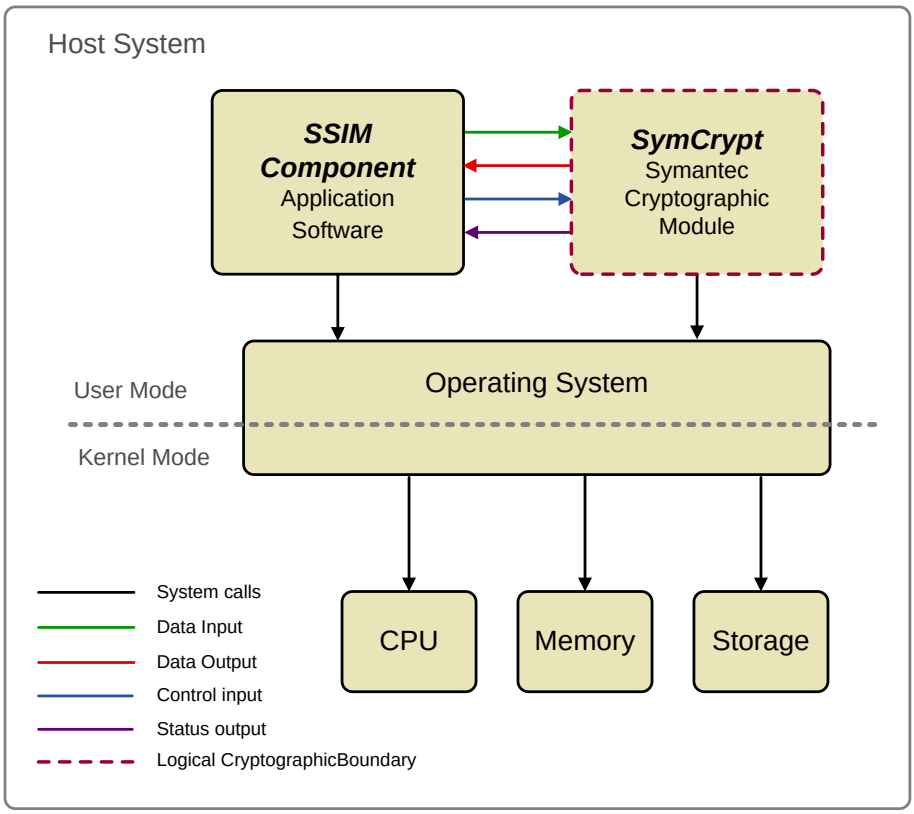

Figure 4 – SymCrypt Module Logical Block Diagram

2.3 Module Interfaces

Communications with the module are isolated to logical interfaces that are defined in the software as an API[7]. The API interface is mapped to the following four logical interfaces:

- Data Input
- Data Output
- Control Input

[7] API – Application Programming Interface

- Status Output

The module features the physical ports of a Dell Optiplex 755. The module's manual controls, physical indicators, and physical, logical, and electrical characteristics are those of the host Dell Optiplex 755. The module's logical interfaces are at a lower level in the software. The physical interfaces supporting input and output are translated into the logical inputs and outputs for the software module. All of these physical interfaces are separated into logical interfaces defined by FIPS 140-2, as described in Table 2.

Table 2 – Symantec Cryptographic Module Interface Mappings

FIPS 140-2 Interface	Physical Interface	Module Interface (API)
Data Input	Network port, Serial port, USB[8] port	Method calls that accept, as their arguments, data to be used or processed by the module
Data Output	Network port, Serial port, 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, Audio port	Thrown exceptions for method calls
Power Input	AC[9] 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. The Crypto Officer is responsible for installing & initializing the module, running self-tests on demand, zeroizing keys, and checking the status. The User is able to perform cryptographic services as depicted in
Table 3 below. The module does not allow multiple concurrent operators in the FIPS-Approved mode of operation. Per section 6.1 of the NIST FIPS 140-2 Implementation Guidance, the calling application that loaded the module is the only operator.

Descriptions of the services available to the Crypto Officer and User role alike are provided in
Table 3 below. Please note that the keys and CSPs[10] listed in the table indicate the type of access required using the following notation:

- R – Read: The plaintext CSP is read by the service.
- W – Write: The CSP is established, generated, modified, or zeroized by the service.
- X – Execute: The CSP is used within an Approved or Allowed security function

[8] USB – Universal Serial Bus
[9] AC – Alternating Current
[10] CSPs – Critical Security Parameters

.

Table 3 – Mapping of CO Services to CSPs and Type of Access

Service	Description	CSP and Type of Access
Initialize module	Perform integrity check and power-up self-tests	Integrity check HMAC[11] key – RX
Run self-test on demand	Performs power-up self-tests	None
Show status	Returns the current mode of the module	None
Zeroize keys	Zeroizes and de-allocates memory containing sensitive data	AES key – W Triple-DES key – W HMAC key – W RSA private/public key – W DSA[12] public key – W DRBG Seed – W DRBG Entropy – W

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

Service	Description	CSP and Type of Access
Generate random number	Returns the specified number of random bits to the calling application	DRBG Seed – WRX DRBG Entropy – RX
Generate message digest	Compute and return a message digest using SHS[13] algorithms	None
Generate keyed hash (HMAC)	Compute and return a message authentication code	HMAC key – RX
Generate symmetric key	Generate and return the specified type of symmetric key (Triple-DES or AES)	AES key – W Triple-DES Key – W
Symmetric encryption	Encrypt plaintext using supplied key and algorithm specification (Triple-DES or AES)	AES key – RX Triple-DES key – RX
Symmetric decryption	Decrypt ciphertext using supplied key and algorithm specification (Triple-DES or AES)	AES key – RX Triple-DES key – RX
Generate asymmetric key pair	Generate and return the specified type of asymmetric key pair (RSA)	RSA private/public key – W

[11] HMAC – (Keyed-)Hash Message Authentication Code
[12] DSA – Digital Signature Algorithm
[13] SHS – Secure Hash Standard

.

Service	Description	CSP and Type of Access
Key Wrapping	Perform key wrap with RSA public key, AES key, and Triple-DES Key	RSA Public Key – RX AES Key – RX Triple-DES Key – RX
Signature Generation	Generate a signature for the supplied message using the specified key and algorithm (RSA)	RSA private key – RX
Signature Verification	Verify the signature on the supplied message using the specified key and algorithm (RSA or DSA)	RSA public key – RX DSA public key – RX

2.5 Physical Security

The Symantec Cryptographic Module is a software 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 Symantec Cryptographic Module was tested and found compliant with the FIPS 140-2 requirements on the following operating system (OS) and platform:

- Dell Optiplex 755 with an Intel Core 2 Duo processor running RHEL 6.4 64-bit.

All cryptographic keys and CSPs are under the control of the host OS, which protects the keys and CSPs against unauthorized disclosure, modification, and substitution. The module only allows access to keys and CSPs through its APIs. The module performs a Software Integrity Test using a FIPS-Approved message authentication code (HMAC SHA[14]-1).

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[15] Encryption and Decryption in ECB[16], CBC[17], CFB8, CFB128, and OFB[18] modes with 128-,192-, and 256-bit key sizes	#2646
Triple DES[19]: ECB, CBC, CFB8, CFB64, and OFB mode for keying option 1, 2^{20}	#1587
RSA[21] (ANSI[22] X9.31) Key Generation with 2048-, 3072-, and 4096-bit key range	#1355

[14] SHA – Secure Hash Algorithm
[15] AES – Advance Encryption Service
[16] ECB – Electronic Code Book
[17] CBC – Cipher Block Chaining
[18] OFB – Output Feedback
[19] DES – Data Encryption Standard
[20] Until December 31st, 2015, two-key Triple-DES is allowed with the restriction that at most 2^{20} blocks of data can be encrypted with the same key.
[21] RSA – Rivest, Shamir, Adleman

Algorithm	Certificate Number
RSA (ANSI X9.31) Signature Generation with 2048-, 3072-, and 4096-bit key range	#1355
RSA (ANSI X9.31) Signature Verification with 1024-, 1536-, 2048-, 3072-, and 4096-bit key range	#1355
RSA (PKCS #1 v1.5) Signature Generation with 2048-, 3072-, and 4096-bit key range	#1355
RSA (PKCS #1 v1.5) Signature Verification with 1024-, 1536-, 2048-, 3072-, and 4096-bit key range	#1355
RSA (PSS[23]) Signature Generation with 2048-, 3072-, and 4096-bit key range	#1355
RSA (PSS) Signature Verification with 1024-, 1536-, 2048-, 3072-, and 4096-bit key range	#1355
DSA[24] (FIPS 186-2) Signature Verification with 1024-bit keys	#797
SHA[25]-1, SHA-224, SHA-256, SHA-384, SHA-512	#2219
HMAC[26] SHA-1, HMAC SHA-224, HMAC SHA-256, HMAC SHA-384, HMAC SHA-512	#1637
NIST SP800-90A DRBG[27] (CTR)	#413

Additionally, the module utilizes the following non-FIPS-Approved algorithm implementation which are allowed for use in the FIPS-Approved mode of operation:

- RSA (2048 bit keys; key wrapping; key establishment methodology provides 112 bits of encryption strength)
- Diffie-Hellman (2048 to 3072 bit keys; key agreement; key establishment methodology provides between 112 and 128 bits of encryption strength)
- EC[28] Diffie-Hellman (curves with |n| >= 224; key agreement; key establishment methodology provides between 112 and 256 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 – SymCrypt Module Non-Approved Algorithm Implementations and Services

Algorithm	Service
RSA	Key Generation; Signature Generation (Key size < 2048)
DSA	Key Generation; Signature Generation (Key size < 2048)

Caveat: No assurance of the minimum strength of generated keys is inside the boundary.

[22] ANSI – American National Standards Institute
[23] PSS – Probabilistic Signature Scheme
[24] DSA – Digital Signature Algorithm
[25] SHA – Secure Hash Algorithm
[26] HMAC – (Keyed-)Hash Message Authentication Code
[27] DRBG – Deterministic Random Bit Generator
[28] EC – Elliptic Curve

.

The module supports the critical security parameters listed below in Table 7.

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

CSP	CSP Type	Generation / Input	Output	Storage	Zeroization	Use
AES key	AES128, 192, 256 bit key	Internally generated via Approved DRBG; or Input via API call parameter	Output in plaintext via Hardware Platform's INT[29] Path	Keys are not persistently stored by the module	Unload module; Remove Power	Encryption, decryption
Triple-DES key	Triple-DES 168 bit key (keying option 1, 2)	Internally generated via Approved DRBG; or Input via API call parameter	Output in plaintext via Hardware Platform's INT Path	Keys are not persistently stored by the module	Unload module; Remove Power	Encryption, decryption
HMAC key	HMAC 160, 224, 256, 384, or 512 – bit key	Internally generated via Approved DRBG; or Input via API call parameter	Output in plaintext via Hardware Platform's INT Path	Keys are not persistently stored by the module	Unload module; Remove Power	Message Authentication with SHS
RSA private key	RSA 2048, 3072, or 4096 bit key	Internally generated via Approved DRBG; or Input via API call parameter	Output in plaintext via Hardware Platform's INT Path	Keys are not persistently stored by the module	Unload module; Remove Power	Signature generation, decapsulation
RSA public key	RSA 1024, 1536, 2048, 3072, or 4096 bit key	Internally generated via Approved DRBG; or Input via API call parameter	Output in plaintext via Hardware Platform's INT Path	Keys are not persistently stored by the module	Unload module; Remove Power	Signature verification, encapsulation

[29] INT – Internal

.

CSP	CSP Type	Generation / Input	Output	Storage	Zeroization	Use
DSA public key	DSA 1024 bit key	Internally generated via Approved DRBG; or Input via API call parameter	Output in plaintext via Hardware Platform's INT Path	Keys are not persistently stored by the module	Unload module; Remove Power	Signature verification
DRBG Seed	Random data – 440 or 880 bits	Generated internally using nonce along with DRBG entropy input.	Never	Keys are not persistently stored by the module	Unload module; API call; Remove Power	Seeding material for SP 800-90A CTR DRBG
DRBG Entropy	256 bit value	Externally Generated[30]; Input via API	Never	Plaintext in volatile memory	Unload module; API call; Remove Power	Entropy material for SP 800-90A CTR DRBG
DRBG 'V' Value	Internal state value	Internally Generated	Never	Plaintext in volatile memory	Unload module; API call; Remove Power	Used for SP 800-90A CTR DRBG
DRBG 'Key' Value	Internal state value	Internally Generated	Never	Plaintext in volatile memory	Unload module; API call; Remove Power	Used for SP 800-90A CTR DRBG

[30] The module employs the non-deterministic random number generator (/dev/random) of the RHEL 6.4 64-bit host operating system, which is outside of the logical cryptographic boundary.

2.8 EMC/EMI

The Symantec Cryptographic Module is a software module. Therefore, the only electromagnetic interference produced is that of the host system on which the module resides and executes. FIPS 140-2 requires that the host systems on which FIPS 140-2 testing is performed meet the Federal Communications Commission (FCC) EMI and EMC requirements for business use as defined in Subpart B, Class A of FCC 47 Code of Federal Regulations Part 15. However, all systems sold in the United States must meet these applicable FCC requirements.

2.9 Self-Tests

Errors encountered during the power-up or conditional self-tests will cause the module to enter the Critical Error state. The module's running process is aborted and the Crypto Officer must power down or restart the host system to clear the error state.

2.9.1 Power-Up Self-Tests

The Symantec Cryptographic Module performs the following self-tests at power-up:

- Software integrity check using a FIPS-Approved MAC[31] (HMAC SHA-1)
- Known Answer Tests (KATs)
  - AES encrypt KAT
  - AES decrypt KAT
  - Triple-DES encrypt KAT
  - Triple-DES decrypt KAT
  - Hash KAT (SHA-1)
  - HMAC KAT with SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512
  - RSA signature generation KAT
  - RSA signature verification KAT
  - DSA PCT[32]
  - NIST SP 800-90A CTR DRBG KAT

2.9.2 Conditional Self-Tests

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

- Continuous RNG Test for the SP 800-90A CTR DRBG
- RSA pairwise consistency test for key pair generation
- DSA pairwise consistency test for key pair generation

2.9.3 Critical Functions Self-Tests

The Symantec Cryptographic Module implements the SP 800-90A CTR DRBG. The DRBG employs four critical functions which must also be tested on a regular basis to ensure the security of the SP 800-90A DRBG. Therefore, the following critical function tests are also implemented by the crypto module:

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

By default, the module performs heatlh checks on the DRBG automatically every 2^{24} DRBG-generate operations; this count can be modified (up or down) by the calling application via the FIPS_drbg_set_check_interval() function. If a DRBG health check fails, the DRBG is placed in an error state that can only be cleared by uninstantiating and reinstantiating the DRBG. The Crypto Officer must

[31] MAC – Message Authentication Code
[32] PCT – Pairwise consistency test

clear the error state by rebooting or unloading the module, which will call the FIPS_drbg_uninstantiate() and FIPS_drbg_instantiate functions respectively.

2.10 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 Symantec 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 Secure Management

FIPS 140-2 mandates that a software cryptographic module at Security Level 1 be restricted to a single operator mode of operation. Prior to installing the module, the Crypto Officer must ensure the host system's OS is configured for single-user mode.

The SymCrypt module is installed as part of the installation of a Symantec product. For SSIM, the CO should follow the installation procedures found in *Symantec Security Information Manager Installation Guide*. These instructions install both server and client components. The Information Manager, which is installed on a server platform, comes with RHEL 6.4 already configured for single-user mode.

3.1.1 Initialization

When the SSIM is initialized, the module runs its power-up self-tests, including the software integrity test that checks the integrity of the module using an HMAC SHA-1 digest. If the integrity check succeeds, then the module performs power-up cryptographic algorithm self-tests. When the module passes all of the power-up self-tests, the module is in its FIPS-Approved mode of operation. If any power-up self-test fails, the module enters a critical error state, ceases all cryptographic functionality, and throws an exception. To leave the critical error state, the Crypto Officer must reboot the host device, remove the power or unload the software.

The Crypto Officer may perform power-up self-tests on demand by invoking the FIPS_selftest() command or through power-cycling the GPC on which the module resides.

3.1.2 Zeroization

The SymCrypt Module module is designed for use by Symantec software applications. Since SymCrypt is a software module, it does not provide a method to persistently store any keys or CSPs. All ephemeral keys used by the module are zeroized upon rebooting, powering down, or unloading the module.

3.2 User Guidance

Only security functions that are FIPS-Approved or allowed for use in the FIPS mode of operation are available when configured for FIPS mode. Should an application attempt to use a non-Approved security function, SymCrypt will give an error message stating the function is non-Approved and will lock the module from further use. SymCrypt must then be reinitialized by the Crypto Officer.

.

Acronyms

Table 8 provides definitions for the acronyms used in this document.

Table 8 – Acronyms

Acronym	Definition
AC	Alternating Current
AES	Advanced Encryption Service
ANSI	American National Standards Institute
API	Application Programming Interface
BIOS	Basic Input Output System
CBC	Cipher-Block Chaining
CFB	Cipher Feedback
CMVP	Cryptographic Module Validation Program
CO	Crypto Officer
CPU	Central Processing Unit
CSE	Communications Security Establishment
CSP	Critical Security Parameter
CTR	Counter
DAS	Direct-attached storage
DRBG	Deterministic Random Bit Generator
DES	Data Encryption Standard
DSA	Digital Signature Algorithm
DVD	Digital Video Disc
EC	Elliptic Curve
ECB	Electronic Codebook
ECC	Elliptic Curve Cryptography
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FCC	Federal Communications Commission
FIPS	Federal Information Processing Standard
GIN	Global Information Network
GUI	Graphical User Interface
HDD	Hard Disk Drive
HMAC	(Keyed-) Hash Message Authentication Code
INT	Internal

.

Acronym	Definition
KAT	Known Answer Test
LCD	Liquid Crystal Display
LDAP	Lightweight Directory Access Protocol
LED	Light Emitting Diodes
MAC	Message Authentication Code
NAS	Network-attached storage
NIST	National Institute of Standards and Technology
OFB	Output Feedback
OS	Operating System
PCI	Peripheral Component Interconnect
PCIe	Peripheral Component Interconnect Express
PCT	Pairwise consistency test
PKCS	Public Key Cryptography Standard
PRNG	Pseudo Random Number Generator
PSS	Probabilistic Signature Scheme
RAM	Random Access Memory
RHEL	Red Hat Enterprise Linux
RNG	Random Number Generator
ROM	Read-Only Memory
RSA	Rivest Shamir and Adleman
SAN	Storage Area Network
SATA	Serial Advanced Technology Attachment
SCSI	Small Computer System Interface
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
SOC	Security Operation Center
SP	Special Publication
SQL	Structured Query Language
SSIM	Symantec Security Information Manager
TDEA	Triple Data Encryption Algorithm
USB	Universal Serial Bus
XEX	XOR-Encrypt-XOR
XOR	Exclusive OR
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