Symantec Corporation

Symantec Enterprise Vault Cryptographic Module

SW Version: 1.0

FIPS 140–2 Non–Proprietary Security Policy

FIPS Security Level: 1
Document Version: 1

Prepared for:

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

Phone: +1 (650) 527-8000
http://www.symantec.com

Prepared by:

Corsec Security, Inc.
10340 Democracy Lane, Suite 201
Fairfax, VA 22030
United States of America

Phone: +1 (703) 267–6050
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 Enterprise Vault (EV) Cryptographic Module from Symantec Corporation. This Security Policy describes how the Symantec Enterprise Vault 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 Canada (CSEC) Cryptographic Module Validation Program (CMVP) website at http://csrc.nist.gov/groups/STM/cmvp.

The Symantec Enterprise Vault Cryptographic Module is referred to in this document as the Enterprise Vault Cryptographic Module, the cryptographic module, or the module. This 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 Symantec website (http://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
- 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 EV Cryptographic Module

This section describes the Symantec Enterprise Vault (EV) Cryptographic Module from Symantec Corporation.

2.1 Overview

Symantec provides a broad range of Information Technology (IT) products and services that help organizations to efficiently manage resources, maximize performance, and minimize security risks. Symantec's product offerings are classified into the following product categories: Security; Information Risk and Compliance; Storage; Infrastructure Operations; and Business Continuity. Symantec, one of the largest makers of security and storage management software, has received recognition as a global leader by a number of research organizations including Gartner and Forrester.

2.1.1 Symantec Enterprise Vault

Symantec Enterprise Vault is a content archiving platform that enables automatic archival of less frequently accessed information into centrally held archives. Using Enterprise Vault, organizations can archive infrequently accessed data from a wide variety of platforms including Exchange Servers; Domino Mail Servers; SharePoint Servers; Simple Mail Transfer Protocol (SMTP) message Servers; and file systems. Enterprise Vault also provides users with the ability to search and retrieve archived information. The Discovery and Compliance Accelerator components provided with Enterprise Vault enable compliance monitoring and legal discovery activities.

2.1.1.1 Enterprise Vault Core Components

Enterprise Vault enables information archival and retrieval through the following core components which are a part of the Enterprise Vault system as shown in Figure 1 below:

- The Enterprise Vault Server– includes services and tasks that perform the tasks of archiving items from target servers, creating indexes of archived items, storing items in the archives, and retrieving archived information.
- The Enterprise Vault Administration Console – configures and manages services, tasks and archives.
- Active Server Page (ASP) Web Access Components – enable users to search and retrieve items in archives.
- SQL Databases – store information related to the Enterprise Vault archives. Services and tasks retrieve information, such as the location of a particular archive, from these databases. The various databases installed as a part of Enterprise Vault include:
    - Enterprise Vault directory database – Enterprise Vault holds configuration data and information about the archives in this database.
    - Vault Store database – Enterprise Vault organizes archived items in entities called Vault Stores. Each Vault Store has a Vault Store database associated with it.
    - Vault Store Group Fingerprinting database – Enterprise Vault creates a fingerprint of parts of an item, referred to as Single Instance Storage (SIS) parts, which are suitable for sharing across Vault Stores. For every SIS part, Enterprise Vault checks the fingerprint database to determine if a fingerprint of the SIS part already exists. If a match is found, Enterprise Vault only references the stored SIS part instead of storing it again, allowing for efficient storage and de–duplication of data.
    - Monitoring and Reporting databases – Perform Enterprise Vault monitoring and reporting functions.

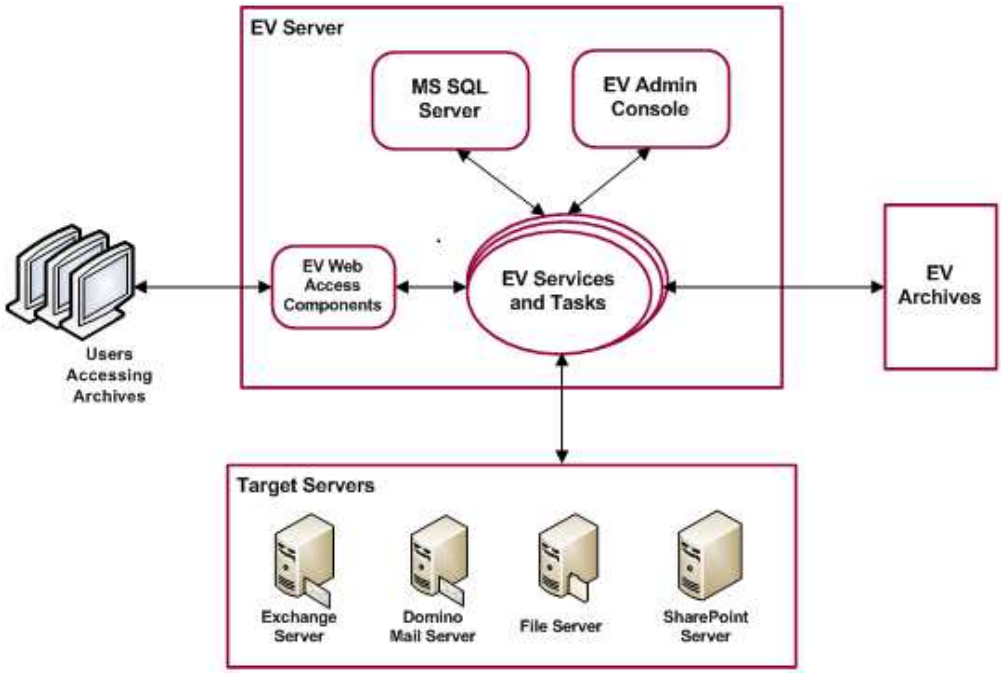

Figure 1 – Symantec Enterprise Vault System Overview

The core Enterprise Vault components can be installed on the same or different computers as required.

2.1.1.2 Enterprise Vault Archiving

In order to archive information, Enterprise Vault archiving tasks check target servers at scheduled times. Relevant items are then stored in Enterprise Vault archives. In order to enable fast search and retrieval, Enterprise Vault creates an index of all the archived items. The Enterprise Vault (EV) archiving process is shown in Figure 2 below.

Figure 2 – EV Archiving Process

2.1.1.3 Accessing Enterprise Vault Archives

Any time a user wants to access an archived item, the web access component passes the user request on to the Enterprise Vault services and tasks. Enterprise Vault services and tasks then look up the archives, and return the requested information to the user. Additionally, users may be allowed to restore archived items to their original location. If permitted, users can also delete archived items. The process of accessing Enterprise Vault archives is shown in Figure 3 below.

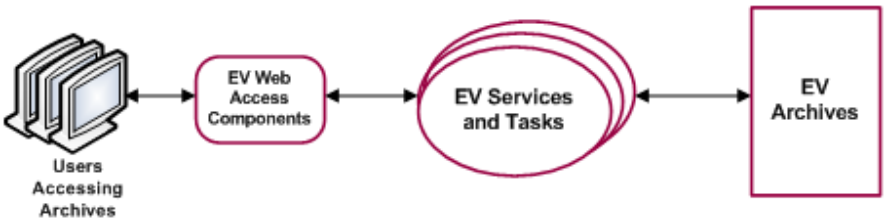

Figure 3 – Users Accessing EV Archives

2.1.2 Enterprise Vault Cryptographic Module

Symantec Enterprise Vault Cryptographic Module is a multi–chip standalone physical embodiment. The module consists of a DLL[1] which interfaces with the Microsoft Cryptographic API[2] to provide the required cryptographic functionality. The Enterprise Vault Cryptographic Module may be used for encryption/decryption of Enterprise Vault passwords, hashing of indexes, and random number generation.

When running on Windows Server 2003 SP2, 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 Standard (SHS)
- (Keyed–) Hash Message Authentication Code (HMAC)
- RSA[4] signature generation
- FIPS 186–2 General Purpose Pseudo Random Number Generator (PRNG)

When running on Windows Server 2008 R2, the module includes implementations of the following FIPS-Approved algorithms:

- Advanced Encryption Standard (AES)
- Triple Data Encryption Algorithm (TDEA or Triple–DES[5])
- Secure Hash Algorithm (SHA)
- (Keyed–) Hash Message Authentication Code (HMAC)
- RSA[6] signature generation and verification
- SP[7] 800-90 AES-256 based counter mode Deterministic Random Bit Generator (DRBG)

The Symantec Enterprise Vault Cryptographic Module is validated at the FIPS 140–2 Section levels shown in Table 1 below:

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

[1] DLL – Dynamic–Link Library
[2] API – Application Programming Interface
[3] DES – Data Encryption Standard
[4] RSA – Rivest, Shamir, Adleman
[5] DES – Data Encryption Standard
[6] RSA – Rivest, Shamir, Adleman
[7] SP – Special Publication

Section	Section Title	Level
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 Symantec Enterprise Vault Cryptographic Module is a software module with a multi–chip standalone embodiment. The overall security level of the module is 1. The physical and logical cryptographic boundaries of the Enterprise Vault Cryptographic Module are defined in the following sections.

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 host system, including the integrated circuits of the system board, the CPU, network adapters, RAM, hard disk, device case, power supply, and fans. Other devices may be attached to the General Purpose Computer (GPC), such as a display monitor, keyboard, mouse, printer, or storage media. See Figure 4 below for a standard host system block diagram.

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

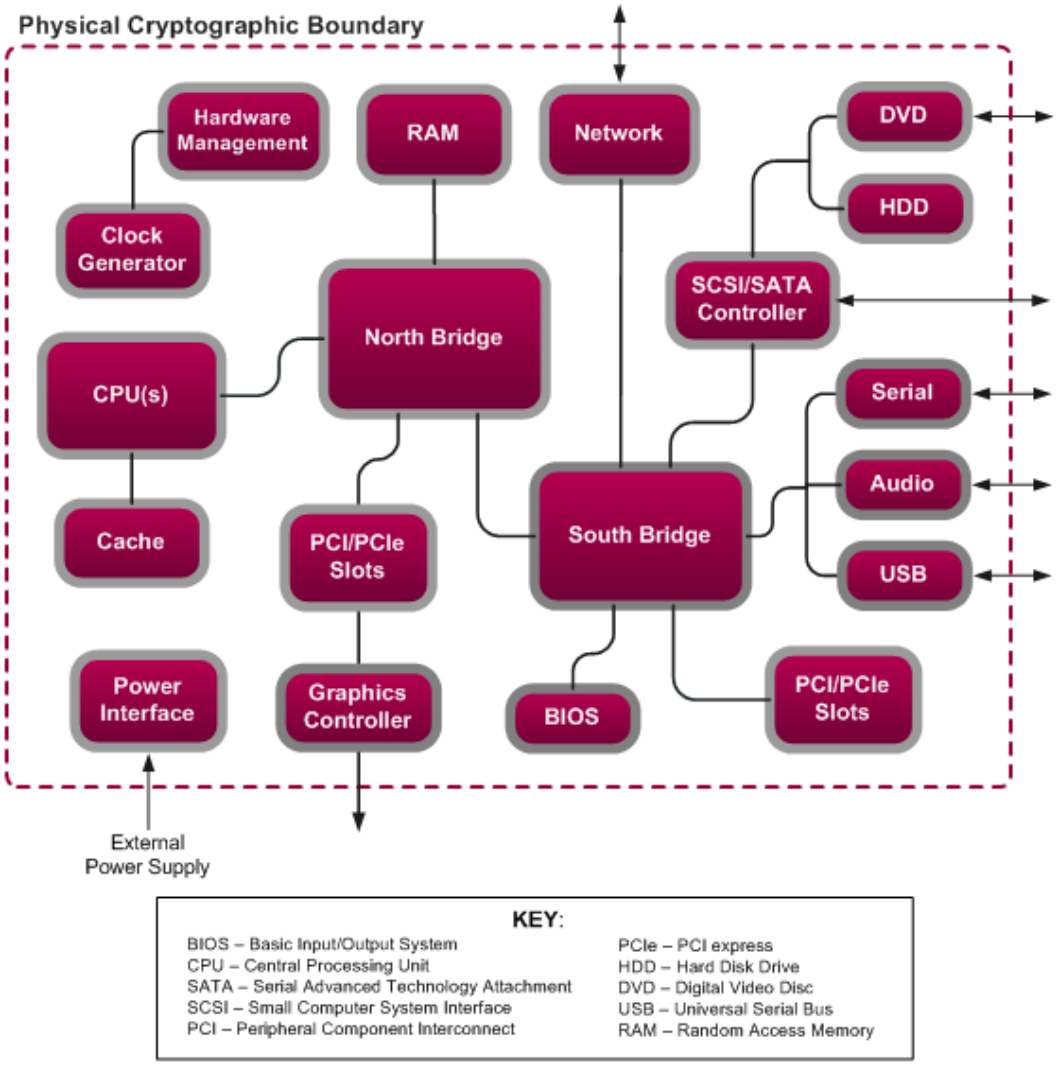

Figure 4 – Standard GPC Block Diagram

2.2.2 Logical Cryptographic Boundary

The logical cryptographic boundary of the module executing in memory is shown in Figure 4. The module's services can be called by the Symantec Enterprise Vault components. The module is utilized by every component of Enterprise Vault that uses the encryption/decryption, hashing, and random number generation functionality.

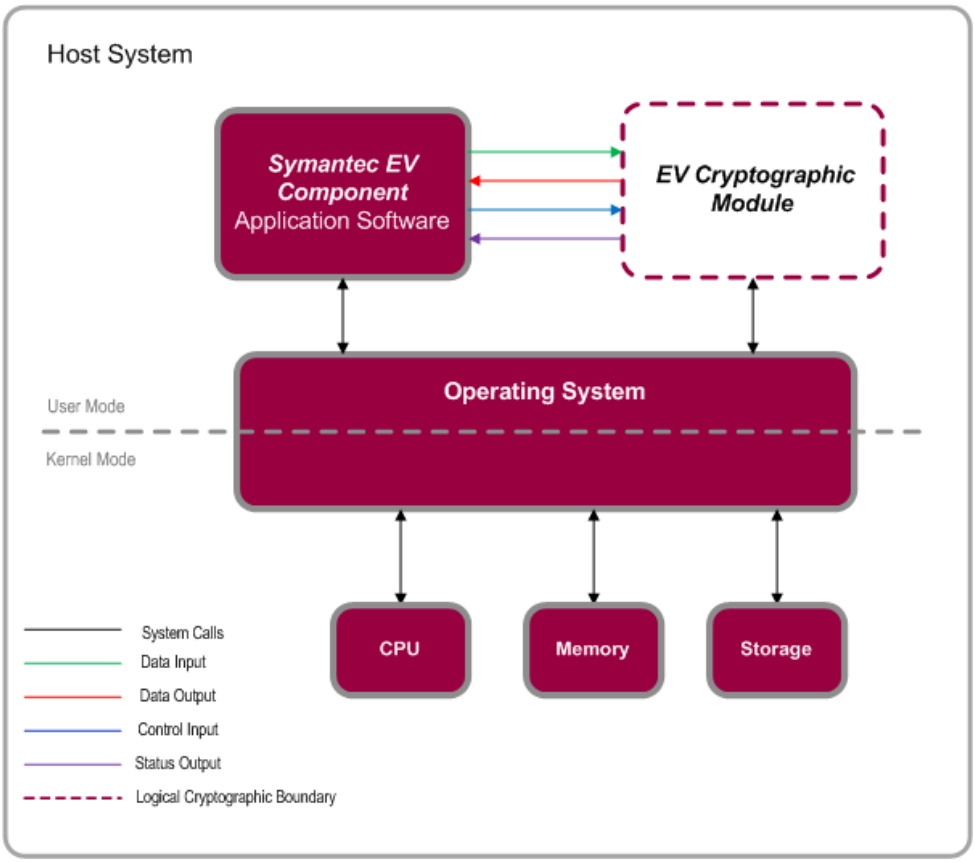

Figure 5 – Logical Block Diagram and Cryptographic Boundary

The cryptographic module was tested and found compliant on the following platforms:

- Windows Server 2003 SP2, 32–bit
- Windows Server 2008 R2, 64-bit

Additionally, the vendor affirms that the cryptographic module is also fully supported on the following platforms:

- Windows Server 2003 SP2, 64–bit
- Windows Server 2008, 32-bit
- Windows Server 2008, 64-bit

2.3 Module Interfaces

The module's logical interfaces exist in the software as an API. Physically, ports and interfaces are those of the host server. The API and physical interfaces can be categorized into following interfaces defined by FIPS 140–2:

- Data Input
- Data Output
- Control Input
- Status Output
- Power Input

A mapping of the FIPS 140–2 logical interfaces, the physical interfaces, and the module can be found in the following table:

Table 2 – FIPS 140–2 Interface Mappings

FIPS Interface	Physical Interface	Logical Interface
Data Input	USB ports, network ports, serial ports, SCSI/SATA ports, DVD/CD drive, audio ports	Arguments for API calls that contain data to be used or processed by the module
Data Output	Display port (e.g. VGA, HDMI, DVI, etc.),, USB ports, network ports, serial ports, SCSI/SATA ports, audio ports, DVD/CD drive	Arguments for API calls that contain or point to where the result of the function is stored
Control Input	USB ports, network ports, serial ports, power switch	API Function calls and parameters that initiate and control the operation of the module
Status Output	Display port (e.g. VGA, HDMI, DVI, etc.), serial ports, network ports	Return values from API function calls and error messages
Power Input	AC Power Ports	N/A

2.4 Roles and Services

Symantec Enterprise Vault Cryptographic Module is validated at FIPS 140–2 Level 1. Therefore, it does not perform authentication of any operators. The module supports the following two roles for operators, as required by FIPS 140–2: Crypto–Officer (CO) role and User role. Both roles are implicitly assumed when the services are utilized.

Note 1: Table 3 and Table 4 use the following definitions for CSP[9]access.

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 or authentication mechanism.*

Note 2: Input parameters of an API call that are not specifically a signature, hash, message, plaintext, ciphertext, or a key are NOT itemized in the "Input" column, since it is assumed that most API calls will have such parameters.

Note 3: The "Input" and "Output" columns are with respect to the module's logical boundary.

2.4.1 Crypto–Officer Role

The operator in the Crypto–Officer role installs, uninstalls, and administers the module via the host platform's Operating System (OS) interfaces.

[9] CSP – Critical Security Parameter

An operator assumes the CO role by invoking one of the following services:

Table 3 – Crypto–Officer Services

Service	Input	Output	CSP and Type of Access
Initialize module	API call parameters	Status	None
Show status	None	Status	None
Run self–tests on demand	None	Status	None

2.4.2 User Role

The operator in the User role is a consumer of the module's security services. The role is assumed by invoking one of the following cryptographic services:

Table 4 – User Services

Service	Input	Output	CSP and Type of Access
Generate random number (Windows Server 2003 SP2 – FIPS 186–2)	API call parameters	Status, random bits	FIPS 186–2 RNG seed – RX FIPS 186–2 seed key – RX
Generate random number (Windows Server 2008 R2 – SP 800-90)	API call parameters	Status, random bits	SP 800-90 RNG seed – RX
Generate message digest (SHS)	API call parameters, message	Status, hash	None
Generate keyed hash (HMAC)	API call parameters, key, message	Status, hash	HMAC key – RWX
Zeroize key	API call parameters	Status	AES key – W TDES key – W HMAC key – W RSA private/public key – W
Symmetric encryption	API call parameters, key, plaintext	Status, ciphertext	AES key – RWX TDES key – RWX
Symmetric decryption	API call parameters, key, ciphertext	Status, plaintext	AES key – RWX TDES key – RWX
Generate asymmetric key pair	API call parameters	Status, key pair	RSA private/public key – W
RSA encryption	API call parameters, plaintext	Status, ciphertext	RSA public key – RWX
RSA decryption	API call parameters, ciphertext	Status, plaintext	RSA private key – RWX
Signature Generation	API call parameters, key, message	Status, signature	RSA private key – WX
Signature Verification	API call parameters, key, signature, message	Status	RSA public key – WX

2.5 Physical Security

The Symantec Enterprise Vault Cryptographic Module is a software module, which FIPS defines as a multi–chip standalone cryptographic module. As such, it does not include physical security mechanisms. Thus, the FIPS 140–2 requirements for physical security are not applicable.

2.6 Operational Environment

The module was tested and found to be compliant with FIPS 140–2 requirements on the following platforms:

- GPC with an Intel Celeron processor running Windows Server 2003 SP2, 32–bit
- GPC with an Intel Core 2 Duo processor running Windows Server 2008 R2, 64-bit

Symantec affirms that the module also executes in its FIPS–Approved manner (as described in this Security Policy) on the following other Operating Systems:

- Windows Server 2003 SP2, 64–bit
- Windows Server 2008, 32-bit
- Windows Server 2008, 64-bit

The Crypto–Officer shall ensure that the Operating System (OS) is configured to a Single User mode of operation. All cryptographic keys and CSPs are under the control of the operating system, which protects the CSPs against unauthorized disclosure, modification, and substitution. The module only allows access to CSPs through its well–defined API.

2.7 Cryptographic Key Management

When running on Windows Server 2003 SP2, the module implements the FIPS–Approved algorithms listed in Table 5 – FIPS–Approved Algorithm Implementations (Windows Server 2003 SP2) below.

Table 5 – FIPS–Approved Algorithm Implementations (Windows Server 2003 SP2)

Algorithm	Certificate Number
AES in ECB[10], CBC[11] modes with 128, 192, and 256 bit keys	818
Triple–DES in ECB, CBC modes with 112 and 168 bit keys	691
RSA (ANSI[12] X9.31, PKCS[13] #1.5, PSS) sign with 1024, 1536, 2048, 3072, 4096 bit keys	395
SHA[14]–1, SHA–256, SHA–384, SHA–512	816
HMAC–SHA–1, HMAC–SHA–256, HMAC– SHA–384, HMAC–SHA–512	452
FIPS 186–2 General Purpose PRNG	470

[10] ECB – Electronic Codebook
[11] CBC – Cipher Block Chaining
[12] ANSI – American National Standards Institute
[13] PKCS – Public–Key Cryptography Standards
[14] SHA – Secure Hash Algorithm

When running on Windows Server 2008 R2, the module implements the FIPS–Approved algorithms listed in Table 6 above.

Table 6 – FIPS–Approved Algorithm Implementations (Windows Server 2008 R2)

Algorithm	Certificate Number
AES in ECB, CBC, CFB8[15] modes with 128, 192, and 256 bit keys	1168
Triple–DES in ECB, CBC, CFB8 modes with 112 and 168 bit keys	846
RSA (ANSI X9.31, PKCS #1.5) sign/verify with 1024, 1536, 2048, 3072, 4096 bit keys	568
RSA (ANSI X9.31) key generation with 1024, 1536, 2048, 3072, 4096 bit keys	559
SHA–1, SHA–256, SHA–384, SHA–512	1081
HMAC–SHA–1, HMAC–SHA–256, HMAC– SHA–384, HMAC–SHA–512	687
SP[16] 800-90 AES-256 based counter mode DRBG	23

The module implements the following non-Approved algorithm allowed in FIPS mode:

- RSA Key Transport (key establishment methodology provides between 80 and 150 bits of encryption strength)

When running on Windows Server 2003 SP2, the module supports the following non–FIPS approved algorithms which are only available in a non–FIPS mode of operation:

- ANSI X9.31RSA key-pair generation
- ANSI X9.31 RSA signature verification
- RC[17]2
- RC4
- MD[18]5
- MD2
- MD4
- DES

When running on Windows Server 2008 R2, the module supports the following non–FIPS approved algorithms which are only available in a non–FIPS mode of operation:

- RC2
- RC4
- MD5
- MD2
- MD4
- DES

[15] CFB8 – Cipher Feedback (8-bit)
[16] SP – Special Publication
[17] RC – Rivest Cipher
[18] MD – Message Digest

The CSPs supported by the module are shown in Table 7 below. Please note that the "Input" and "Output" columns are in reference to the module's logical boundary. Keys that enter and exit the module via an API call parameter are in plaintext.

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

CSP/Key	Input	Output	Storage	Zeroization	Use
AES key	API call parameter	Never	Plaintext in volatile memory	By API call, power cycle	Encryption, decryption
TDES key	API call parameter	Never	Plaintext in volatile memory	By API call, power cycle	Encryption, decryption
HMAC key	API call parameter	Never	Plaintext in volatile memory	By API call, power cycle	Message Authentication with SHA–1 and SHA–2s
RSA private key	API call parameter	Never	Plaintext in volatile memory	By API call, power cycle	Signature generation, decryption
RSA public key	API call parameter	Never	Plaintext in volatile memory	By API call, power cycle	Signature verification, encryption
FIPS 186–2 PRNG seed (Windows Server 2003 SP2)	Internally generated	Never	Plaintext in volatile memory	By API call, power cycle	Generate random number
FIPS186–2 PRNG seed key (Windows Server 2003 SP2)	Internally generated	Never	Plaintext in volatile memory	By API call, power cycle	Generate random number
SP 800-90 DRBG seed (Windows Server 2008 R2)	Internally generated	Never	Plaintext in volatile memory	By API call, power cycle	Generate random number

2.7.1 Key Generation

When running on Windows Server 2003 SP2, the module uses a FIPS–Approved FIPS 186–2 General Purpose PRNG implementation to generate cryptographic keys. When operating on Windows Server 2008 R2, the module uses a FIPS-Approved SP 800-90 AES-256 based counter mode DRBG for the generation of cryptographic keys.

2.7.2 Key Entry and Output

The cryptographic module itself does not support key entry or key output from its physical boundary. However, keys are passed to the module as parameters from the applications resident on the host platform via the exposed APIs. Similarly, keys and CSPs exit the module in plaintext via the well–defined exported APIs.

2.7.3 Key/CSP Storage and Zeroization

The module does not persistently store any keys or CSPs. Symmetric keys are either provided by or delivered to the calling process, and are subsequently destroyed by the module at the completion of the API function call.

2.8 EMI/EMC

Enterprise Vault Cryptographic Module is a software module. Therefore, the only electromagnetic interference produced is that of the host platform 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

2.9.1 Power–Up Self–Tests

The Symantec Enterprise Vault Cryptographic Module performs the following self–tests at power–up when running on Windows Server 2003 SP2:

- Software integrity test
- Known Answer Tests (KATs)
  - Triple–DES 168 ECB encrypt/decrypt
  - Triple–DES 168 CBC encrypt/decrypt
  - Triple–DES 112 ECB encrypt/decrypt
  - Triple–DES 112 CBC encrypt/decrypt
  - AES 128 ECB encrypt/decrypt
  - AES 192 ECB encrypt/decrypt
  - AES 256 ECB encrypt/decrypt
  - AES 128 CBC encrypt/decrypt
  - AES 192 CBC encrypt/decrypt
  - AES 256 CBC encrypt/decrypt
  - SHA–1
  - SHA–256
  - SHA–384
  - SHA–512
  - HMAC SHA–1
  - HMAC SHA–256
  - HMAC SHA–384
  - HMAC SHA–512
- RSA sign/verify test
- FIPS 186–2 RNG

The Symantec Enterprise Vault Cryptographic Module performs the following self–tests at power–up when running on Windows Server 2008 R2:

- Software integrity test
- Known Answer Tests (KATs)
  - Triple–DES 168 ECB encrypt/decrypt
  - AES 128 ECB encrypt/decrypt
  - SHA–384
  - SHA–512
  - HMAC SHA–1
  - HMAC SHA–256
  - SP 800-90 CTR[19]_DRBG KAT
- RSA sign/verify

2.9.2 Conditional Self–Tests

The Symantec Enterprise Vault Cryptographic Module performs the following conditional self–tests:

- RSA pairwise consistency test
- Continuous RNG test

2.10 Mitigation of Other Attacks

This section is not applicable. The module does not claim to mitigate any attacks beyond the FIPS 140–2 Level 1 requirements for this validation.

[19] CTR – Counter mode

3 Secure Operation

The Symantec Enterprise Vault 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 Initial Setup

When the module is loaded by the host Symantec Enterprise Vault software application, the module assumes a FIPS–Approved mode if a FIPS–Approved algorithm is requested. Immediately after the module is loaded, it performs a self–integrity test. If the integrity test succeeds, the module performs all other required FIPS power–up self–tests. If the module passes all self–tests, then the module enters a FIPS–Approved mode of operation. The module implicitly assumes a non–FIPS mode if a non–FIPS approved algorithm is requested. The only way to cause the module to return to a FIPS mode is to reload the module, cycle the power, or reboot the host OS.

3.2 Crypto–Officer Guidance

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 OS is configured for single–user mode.

To configure the Windows OS for single–user mode, the Crypto–Officer must ensure that all remote guest accounts are disabled in order to ensure that only one operator can log into the Windows OS at a time. The services that need to be turned off for Windows are:

- Fast–user switching (irrelevant if server is a domain member)
- Terminal services
- Remote registry service
- Secondary logon service
- Telnet service
- Remote desktop and remote assistance service

3.3 User Guidance

The Enterprise Vault Cryptographic Module is designed for use by the Symantec Enterprise Vault application. The module does not input, output, or persistently store CSPs with respect to the physical boundary. The user is responsible for providing persistent storage of the cryptographic keys and CSPs, and to ensure that keys are transmitted outside the physical cryptographic boundary in a secure manner.

4 Acronyms

Table 8 – Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
API	Application Programming Interface
ANSI	American National Standards Institute
ASP	Active Server Page
CBC	Cipher Block Chaining
CMVP	Cryptographic Module Validation Program
CPU	Central Processing Unit
CSEC	Communications Security Establishment Canada
CSP	Critical Security Parameter
CTR	Counter Mode
DES	Data Encryption Standard
DLL	Dynamic–Link Library
DRBG	Deterministic Random Bit Generator
ECB	Electronic Codebook
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
EV	Enterprise Vault
FCC	Federal Communications Commission
FIPS	Federal Information Processing Standard
GPC	General Purpose Computer
HMAC	(Keyed–) Hash Message Authentication Code
IT	Information Technology
KAT	Known Answer Test
LED	Light Emitting Diode
MD	Message Digest
NIST	National Institute of Standards and Technology
NVLAP	National Voluntary Laboratory Accreditation Program
OS	Operating System
PKCS	Public Key Cryptography Standards
PRNG	Pseudo Random Number Generator

Acronym	Definition
RAM	Random Access Memory
RC	Rivest Cipher
RNG	Random Number Generator
RSA	Rivest Shamir and Adleman
SATA	Serial Advanced Technology Attachment
SCSI	Small Computer System Interface
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
SIS	Single Instance Storage
SMTP	Simple Mail Transfer Protocol
SP	Special Publication
TDES	Triple Data Encryption Standard
USB	Universal Serial Bus

Prepared by:
Corsec Security, Inc.

10340 Democracy Lane, Suite 201
Fairfax, VA 22030

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