Vormetric, Inc

Vormetric Encryption Expert Cryptographic Module
Software Version 5.1.3

FIPS 140-2 Non-Proprietary Security Policy Level 1 Validation

02 March 2015

Table of Contents

1 INTRODUCTION

1.1 Purpose

This is a non-proprietary FIPS 140-2 Security Policy for the version 5.1.3 Vormetric Encryption Expert Cryptographic Module. It describes how this module meets all the requirements as specified in the FIPS 140-2 Level 1 requirements. This Policy forms a part of the submission package to the validating lab.

FIPS 140-2 (Federal Information Processing Standards Publication 140-2) specifies the security requirements for a cryptographic module protecting sensitive information. Based on four security levels for cryptographic modules this standard identifies requirements in eleven sections.

1.2 References

This Security Policy describes how this module complies with the eleven sections of the Standard:

- For more information on the FIPS 140-2 standard and validation program please refer to the NIST website at csrc.nist.gov/groups/STM/cmvp/index.html
- For more information about Vormetric, please visit www.vormetric.com

1.3 Document History

Authors	***Date***	***Version***	***Comment***
Mike Yoder	18 June 2013	0.1	First Draft
Mike Yoder	9 August 2013	0.2	Second Draft
Mike Yoder	12 February 2014	0.3	Changed version 5.1.2 -> 5.1.3
Mike Yoder	26 March 2014	0.4	Added algorithm numbers
Peter Henscheid	25 August 2014	0.5	Changed software module to software-hybrid module
Peter Henscheid	19 December 2014	0.6	Added encryption hardware documentation
Peter Henscheid	4 February 2015	0.7	Third Draft
Jonathan Smith	13 February 2015	0.8	Fourth Draft
Jonathan Smith	2 March 2015	0.9	Fifth Draft

2 PRODUCT DESCRIPTION

The Vormetric Encryption Expert Cryptographic Module is a Level 1 FIPS 140-2 module of type *Software-Hybrid* with an embodiment classified as *Multi-chip Standalone*. This module is a subset of the Vormetric Encryption Expert Agent, which in turn is part of the Vormetric Data Security solution. The Vormetric Encryption Expert Cryptographic Module interacts with the Vormetric Data Security Manager, which is itself a cryptographic hardware module. It has been validated separately from this module.

The Vormetric Encryption Expert Cryptographic Module is a loadable kernel module also known as "SECFS" (SECure File System). This module is a file system layer that enforces an access and encryption policy upon selected data on end-user systems. The policy specifies a key to be used when writing data to disk and while reading data from disk. This module contains the Vormetric Encryption Expert Cryptographic Library, which provides all cryptographic services.

The Vormetric Encryption Expert Cryptographic Module implements Triple-DES, AES, SHA-1, SHA-256, and HMAC-SHA-256.

The product meets the overall requirements applicable to Level 1 security for FIPS 140-2.

Security Requirements Section	***Level***
Cryptographic Module Specification	1
Cryptographic Module Ports and Interfaces	1
Roles and Services and Authentication	1
Finite State Machine Model	1
Physical Security	1
Operational Environment	1
Cryptographic Key Management	1
EMI/EMC	1
Self-Tests	1
Design Assurance	1
Mitigation of Other Attacks	N/A
Cryptographic Module Security Policy	1
Overall Level of Certification	1

Table 1 - Module Compliance Table

2.1 Cryptographic Boundary

The Vormetric Encryption Expert Cryptographic Module's boundary is illustrated in **red** in the figure below:

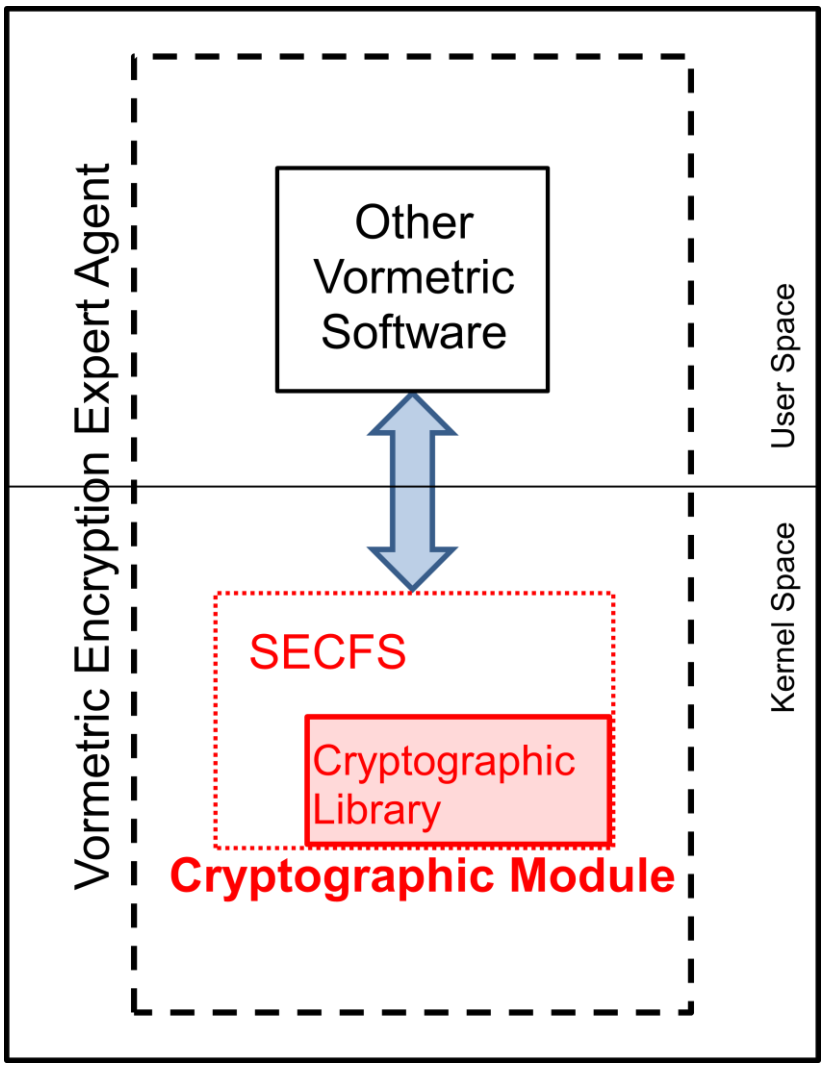

Figure 1 – Logical Cryptographic Boundary

The loadable kernel module for all Linux platforms (“SECFS” in the diagram above) is named “secfs2.ko”.

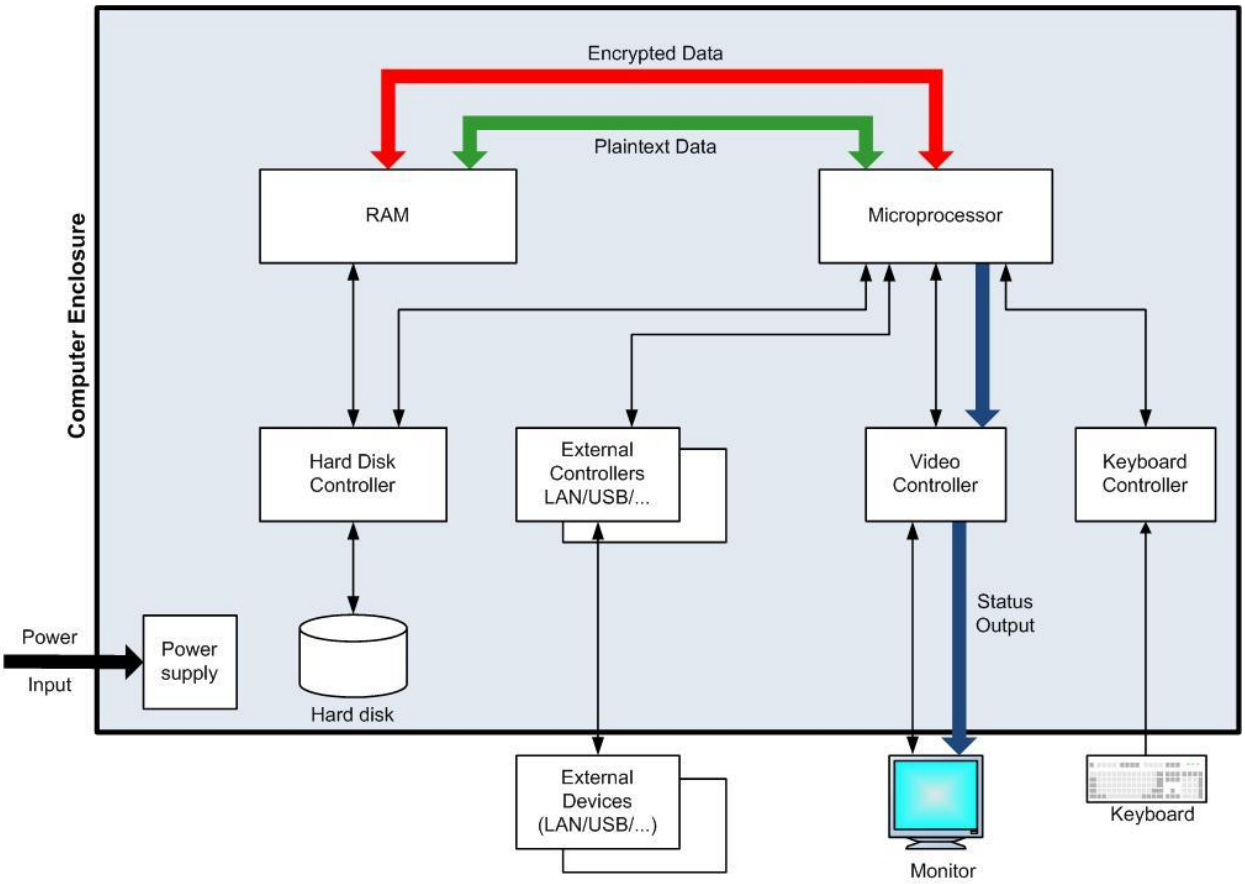

Figure 2 – Physical Cryptographic Boundary

2.2 Platform Considerations

This module is validated on Red Hat Enterprise Linux (RHEL 6.3), running on a Supermicro X9DR7 and SUSE Linux Enterprise Server (SLES 11 SP 2), running on a Supermicro X9DR7. This module utilizes the "AES-NI" instruction set for AES cryptographic operations. All other cryptographic operations are performed in software inside the module boundary.

3 MODULE PORTS AND INTERFACES

The module is software based and designed to meet FIPS 140-2 Level 1 requirements.

FIPS 140-2 Interface	*Physical Interface*	*Logical Interface*
Data Input interface	External Devices (LAN/USB/…), Keyboard	File System write() function calls
Data Output interface	External Devices (LAN/USB/…), Monitor	File System read() function calls
Control Input interface	External Devices (LAN/USB/…), Keyboard	Input parameters to ioctl() calls into the module
Status Output interface	External Devices (LAN/USB/…), Monitor	Output parameters from ioctl() calls into the module

Table 2 – Mapping FIPS 140-2 Interfaces and Logical Interfaces

4 ROLES, SERVICES AND AUTHENTICATION

4.1 Roles and Services

The User and Crypto Officer roles are implicitly assumed by the entities that can access the interfaces to the cryptographic module. These entities do so implicitly through the file system read() and write() interfaces, and control through the ioctl() interfaces of the module.

4.2 Authentication

The module does not provide identification or authentication mechanisms that would distinguish between the two supported roles. Each process or thread accessing the module is logically separated by the operating system into independent contexts of execution, and hence the FIPS 140-2 requirement for a single user mode of operation is upheld.

4.3 Authorized Services

The Vormetric Encryption Expert Agent supports the services listed in the following tables. Each table shows the privileges of each role on a per-service basis. The privileges are divided into:

R - The item is **read** or referenced by the service.
W -The item is **written** or updated by the service.
E - The item is **executed** by the service. (The item is used as part of a cryptographic function.)

The cryptographic module is a loadable kernel module. This module utilizes the “AES-NI” instruction set, if available, for AES cryptographic operations. It intercepts file system calls, evaluates a policy, and encrypts or decrypts data according to the rules in the policy. There are several control interfaces for this component, all of which have to do with either initialization or with policy and key configuration. These are accessed in the “Crypto Officer” role. The data input/output interfaces are done through intercepting file system calls, and are accessed in the “User” role. The keys used in the Authorized Services are described in Section 7, “Key Management”, in Table 5.

Authorized Services	Cryptographic Key/CSP	*Roles*	*Access*
Run Power-On Self Test	HMAC Integrity Key	Crypto Officer	E
Initialization (Also known as “registration”)	SECFS Private Key SECFS Wrapping Key SECFS HMAC Key	Crypto Officer	WE
Configuration Update (New configuration / policy / key information is given to the kernel module)	All keys in Table 5	Crypto Officer	WE
Status Query	N/A	Crypto Officer	R
Rekey (converting data from being encrypted with one key to being encrypted with another)	File System Keys	Crypto Officer	RWE
Zeroization	All	Crypto Officer	WE
File System interfaces: read(), write(), etc	File System Keys (Triple-DES, AES 128-bit and 256-bit)	User	RWE
non-Approved Service: File System interfaces: read(), write(), etc	File System Keys (ARIA 128-bit and 256-bit)	User	RWE

Table 3 – Authorized Services

Note: The module utilizes the AES-NI instructions when the module runs on processors that implement these instructions. The AES-NI instructions accelerate the AES algorithm.

5 PHYSICAL SECURITY

This software-hybrid module meets the level 1 physical security requirements. The module runs on a general purpose computer.

6 Operational Environment

The Vormetric Encryption Expert Agent operates in a “modifiable operational environment”. It exists as software executed in a commercially available operating system. The specifically tested platforms are

Operating System	*Bits*	*Processor / System*	*Cryptographic Hardware*
Red Hat Enterprise Linux 6.3	64	Intel Xeon – Supermicro X9DR7	Type: Intel® Xeon® Part/Version: E5-2670 @ 2.60Ghz
SUSE Linux Enterprise Server 11 SP 2	64	Intel Xeon – Supermicro X9DR7	Type: Intel® Xeon® Part/Version: E5-2670 @ 2.60Ghz

Table 4 – Tested Platforms

Figure 3 – Physical Cryptographic Hardware for AES-NI

All other platforms supported by Vormetric are "Vendor Affirmed" to be FIPS 140-2 compliant as per FIPS Implementation Guidance section G.5. The CMVP allows vendor porting of a validated level 1 software-hybrid cryptographic module running on a CPU supporting the AES-NI instruction set from the GPC(s) specified on the validation certificate to a GPC that was not included as part of the validation status, as long as no source code modifications are required. The validation status is maintained on the new GPC without re-testing the cryptographic module on the new GPC. The CMVP makes no statement as to the correct operation of the module when so ported if the specific operational environment is not listed on the validation certificate.

7 CRYPTOGRAPHIC KEY MANAGEMENT

The cryptographic library manages keys. All of the keys and CSPs are generated externally.

7.1 Cryptographic Keys and CSPs

Key	Generation	Storage	Use	Input/Output
HMAC Integrity Key (HMAC-SHA 256-bit, key size 256-bit)	At vendor facility	Incorporated into binary	Protects the integrity of the module	Hardcoded Cannot be exported
SECFS HMAC Key (HMAC-SHA 256-bit, key size 256-bit)	At vendor facility	Incorporated into binary	Protects the integrity of keys when stored.	Hardcoded Cannot be exported
SECFS Wrapping Key (AES 256-bit)	At vendor facility	Incorporated into binary	Protects storage of keys	Hardcoded Cannot be exported
SECFS Private Key (RSA 2048-bit)	Generated externally to the module	Stored in encrypted form with AES	Protects the File System Key Encrypting Key for key transport	Input only, Cannot be exported

Key	Generation	Storage	Use	Input/Output
File System Key Encrypting Key (AES 256-bit)	Generated externally by the Vormetric Data Security Server Module (NIST 800-90A DRBG)	Stored in encrypted form with AES	Protects the File System Keys	Input only, Cannot be exported
File System Keys (Triple-DES, AES 128-bit and 256-bit)	Generated externally by the Vormetric Data Security Server Module (NIST 800-90A DRBG)	Stored in encrypted form with AES	Encrypts and decrypts file system data	Input only, Cannot be exported
File System Keys (ARIA 128-bit and 256-bit)	Generated externally by the Vormetric Data Security Server Module (NIST 800-90A DRBG)	Stored in encrypted form with AES	Obfuscates and unobfuscates file system data. This is a **non-approved** security function	Input only, Cannot be exported

Table 5 – Keys and CSPs

7.2 Approved Security Algorithms

The module keys map to the following algorithms certificates. On the Windows 2008 R2 platform the certificates from the Microsoft Kernel Mode Cryptographic Primitives Library (FIPS certificate #1335) are referenced. For AES encryption, Linux platforms have an algorithm certificate which utilizes AES-NI. All others are implemented in software inside the module boundary.

Approved or Allowed Security Functions	Vormetric Encryption Expert Agent Certificate
Symmetric Encryption/Decryption	
AES: (CBC Mode; Encrypt/Decrypt; 128 and 256 bit)	2807
Triple-DES (3-key) (CBC Mode, Encrypt/Decrypt)	1685
Secure Hash Standard (SHS)	
SHA-1, SHA-256	2355
Data Authentication Code	
HMAC-SHA-256	1758
Allowed Security Function	
RSA (key wrapping; key establishment methodology provides 112 bits of encryption strength)	
Non-Approved Security Function	
ARIA: Obfuscate/Unobfuscate, Key Size = 128, 256	

Table 6 - Algorithms Table

8 EMI/EMC

The general purpose computers that this module was tested on meet the FCC Code of Federal Regulations, Title 47, Part 15, Subpart B as a class B unintentional radiator.

9 SELF-TEST

The module performs power-up self-tests and conditional self tests.

9.1 Power-up Self-Tests

Any other processing and data input/output is inhibited while the tests are in progress. If any test fails, an error status such as “FIPS Algorithm Known Answer Test/Integrity test failed” is displayed and the module will cease operation. When each of the five tests run to completion, a “FIPS <testname> Test passed” message is written to the log. When all five tests pass, the module is operating in FIPS mode. While running the non-Approved security function ARIA the module is in non-FIPS mode. To run these self-tests on demand, restart the module.

Cryptographic Algorithm KATs:
Known Answer Tests (KATs) are run at power-up for:

- AES (CBC mode for Encrypt/Decrypt)
- Triple-DES (3-key) (CBC mode for Encrypt/Decrypt)
- SHA-1, SHA-256
- HMAC-SHA-256

Software Integrity Tests:
The module checks the integrity of its object code when it is initialized. It performs an HMAC-SHA-256 of itself when it is loaded into the kernel; this is compared to an HMAC-SHA-256 digest generated during

build time. If the results are not the same, an error message is written to the output interface, and the kernel module will cease further operation.

9.2 Conditional Self-Tests

The module performs no conditional self-tests.

10 Crypto-Officer and User Guidance

This section shall describe the configuration, maintenance, and administration of the cryptographic module.

10.1 Secure Setup, Initialization, and Operation

It is the operator's responsibility to operate the module according to the security policy rules described in the following section. To configure the module, the Crypto-Officer should

- Install the Vormetric Encryption Expert Agent software package
- Register with a Vormetric Data Security Server
- Verify that the fingerprints of the generated certificates match those shown on the Vormetric Data Security Server
- Verify that the message described in section 9.1 is emitted to ensure that the module is operating in a FIPS approved mode.

Zeroization is performed by uninstalling the module. The platform's hard drive must be reformatted or overwritten after uninstallation.

To show the status of the module, run the command "vmsec status".

10.2 Module Security Policy Rules

The module operates in FIPS mode after all the power-up self tests have passed and the message described in section 9.1 has been displayed. However when using the non-Approved Security Function ARIA the module is in a non-FIPS mode. To operate in FIPS mode use only FIPS Approved security functions.

11 Design Assurance

Vormetric utilizes Concurrent Versioning System (CVS) for configuration management of product source code. Vormetric also utilizes Confluence, an internal wiki for configuration management of functional specifications and documentation. Both support authentication, access control, and logging. A high-level programming language is used for all software components within the module. Software is distributed either in person or via a secure https-based web site.

12 Mitigation of Other Attacks

The module does not mitigate against any specific attacks.