*Vormetric, Inc*

# Vormetric Encryption Expert Cryptographic Module
# Software Version 4.4.1

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

**April 9th, 2012**

## Table of Contents

# 1 INTRODUCTION

## *1.1 Purpose*

This is a non-proprietary FIPS 140-2 Security Policy for the version 4.4.1 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 | August 27th, 2010 | 0.1 | First Draft |
| Mike Yoder | September 27th, 2010 | 0.2 | Second Draft |
| Mike Yoder | October 27th, 2010 | 0.3 | Third Draft |
| | | | |

# 2 PRODUCT DESCRIPTION

The Vormetric Encryption Expert Cryptographic Module is a Level 1 FIPS 140-2 module of type *Software* 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 Server, 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 in the approved mode. It also implements ARIA encryption in the non approved mode.

The product meets the overall requirements applicable to Level 1 security for FIPS 140-2, with Design Assurance meeting the Level 3 requirement.

| ***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 | N/A |
| Operational Environment | 1 |
| Cryptographic Key Management | 1 |
| EMI/EMC | 1 |
| Self-Tests | 1 |
| Design Assurance | 3 |
| 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:

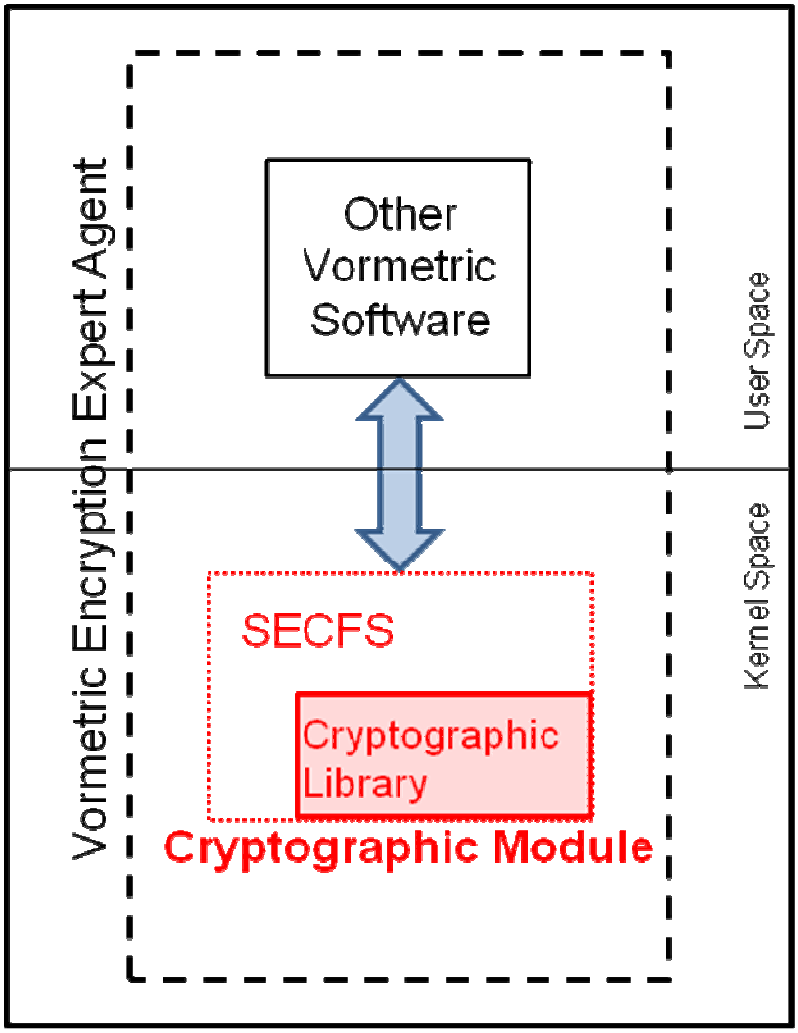


**Figure 1 – Logical Cryptographic Boundary**

The loadable kernel module ("SECFS" in the diagram above) has different names on different operating systems. On 32-bit and 64-bit Windows it is called "vmmgmt.sys". On Solaris it is "secfs2". On Linux it is "secfs2.ko". On HPUX the name is "vormetric".

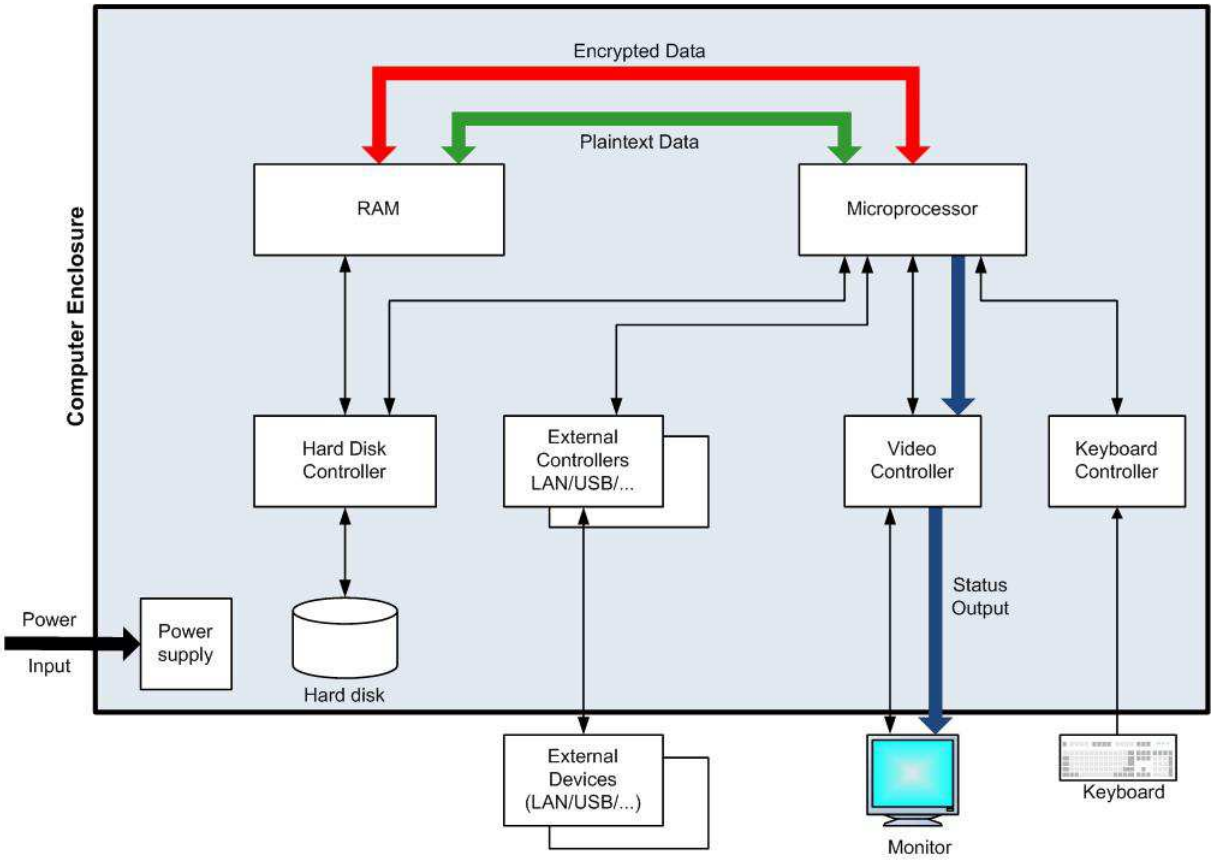


**Figure 2 – Physical Cryptographic Boundary**

# 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. 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 6.

| ***Authorized Services*** | **Cryptographic Key/CSP** | ***Roles*** | ***Access*** |
|---|---|---|---|
| Run Power-On Self Test | HMAC Integrity Key | Crypto Officer | W |
| Initialization (Also known as “registration”) | SECFS Private Key<br>SECFS Wrapping Key | Crypto Officer | WE |
| Configuration Update (New configuration / policy / key information is given to the kernel module) | All keys in Table 6 | 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 | User | RWE |

**Table 3 – Authorized Services**

The following services may also operate in a non-FIPS-approved mode. This occurs only when ARIA keys are used.

| *Non-FIPS-Approved Services When ARIA Keys Used* | **Cryptographic Key/CSP** |
|---|---|
| Configuration Update (New configuration / policy / key information is given to the kernel module) | ARIA File System Keys |
| Rekey (converting data from being encrypted with one key to being encrypted with another) | ARIA File System Keys |
| File System interfaces: read(), write(), etc | ARIA File System Keys |

**Table 4 – Services in non-FIPS mode**

# 5 PHYSICAL SECURITY

This module does not claim to enforce any physical security as it is implemented entirely in software. 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* |
|---|---|---|
| Microsoft Windows 2003 | 32 | Intel Xeon |
| Microsoft Windows 2008 | 64 | Intel Xeon |
| Solaris 10 | 64 | Sun UltraSPARC II |
| Redhat 5.7 | 64 | Intel Xeon |
| HPUX 11i v3 | 64 | Intel Itanium |

**Table 5 – Tested Platforms**

All other platforms supported by Vormetric are "Vendor Affirmed" to be FIPS 140-2 compliant.

# 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 |
|---|---|---|---|
| **HMAC Integrity Key** (HMAC-SHA 256-bit) | At vendor facility | Incorporated into binary | Protects the integrity of the module |
| **SECFS Wrapping Key** (AES 256-bit) | At vendor facility | Incorporated into binary | Protects storage of keys |
| **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 |

| Key | Generation | Storage | Use |
|---|---|---|---|
| **File System Key Encrypting Key** (AES 256-bit) | Generated externally by the Vormetric Data Security Server Module (ANSI X9.31) | Stored in encrypted form with AES | Protects the File System Keys |
| **File System Keys** (Triple DES, AES 128-bit and 256-bit) | Generated externally by the Vormetric Data Security Server Module (ANSI X9.31) | Stored in encrypted form with AES | Encrypts and decrypts file system data |

**Table 6 – Keys and CSPs**

None of the above keys can be output or exported from the module.

## *7.2 Approved Security Algorithms*

The module keys map to the following algorithms certificates:

| Approved or Allowed Security Functions | Certificate |
|---|---|
| ***Symmetric Encryption/Decryption*** | |
| AES: (CBC Mode; Encrypt/Decrypt; 128 and 256 bit) | 1820 |
| Triple-DES (3-key) (CBC Mode, Encrypt/Decrypt) | 1173 |
| ***Secure Hash Standard (SHS)*** | |
| SHA-1, SHA-256 | 1596 |
| ***Data Authentication Code*** | |
| HMAC-SHA-256 | 1075 |
| ***Non-Approved Security Function*** | |
| ARIA: Encrypt/Decrypt, Key Size = 128, 256 | |
| RSA (key wrapping; key establishment methodology provides 112 bits of encryption strength) | |

**Table 7 - FIPS Approved 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 all tests run to completion, a “FIPS Algorithm Known Answer Test/Integrity test passed” message is displayed and the module is operating in FIPS mode.

**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.

## *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. The module remains operating in FIPS mode when using FIPS Approved cryptography. If ARIA keys are used, the module will not be operating in a FIPS Approved mode. The use of ARIA keys occurs only when the Vormetric Data Security Server instructs the module to apply an encryption policy that uses an ARIA key.

# 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.