Vormetric, Inc

Vormetric Application Encryption Module
Software Version 5.2.5

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

09 March 2017

Table of Contents

1 INTRODUCTION

1.1 Purpose

This is a non-proprietary FIPS 140-2 Security Policy for the version 5.2.5 Vormetric Application Encryption (VAE) software 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***
Janice Cheng	24 May 2016	0.1	First Draft
Janice Cheng	09 March 2017	1.0	Updated as per CMVP comments

2 PRODUCT DESCRIPTION

The Vormetric Application Encryption software module is classified as a multi-chip standalone module embodiment for FIPS 140-2 purposes.. This module is part of the Vormetric Data Security solution. The Vormetric Application Encryption software module interacts with the Vormetric Data Security Manager (DSM), which is itself a cryptographic hardware module. It has been validated separately from this module.

The Vormetric Application Encryption software module is a user space library. This module is a shared object (.so) in Linux and a dynamic link library (.dll) on Windows. The application encryption software module provides a set of documented standard based APIs used to perform cryptographic and encryption key management operations.

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	N/A
Operational Environment	1
Cryptographic Key Management	1
EMI/EMC	1
Self-Tests	1
Design Assurance	1
Mitigation of Other Attacks	N/A
Overall Level of Validation	1

Table 1 - Module Compliance Table

2.1 Cryptographic Boundary

The Vormetric Application Encryption software module's boundary is illustrated in **red** in the figure below:

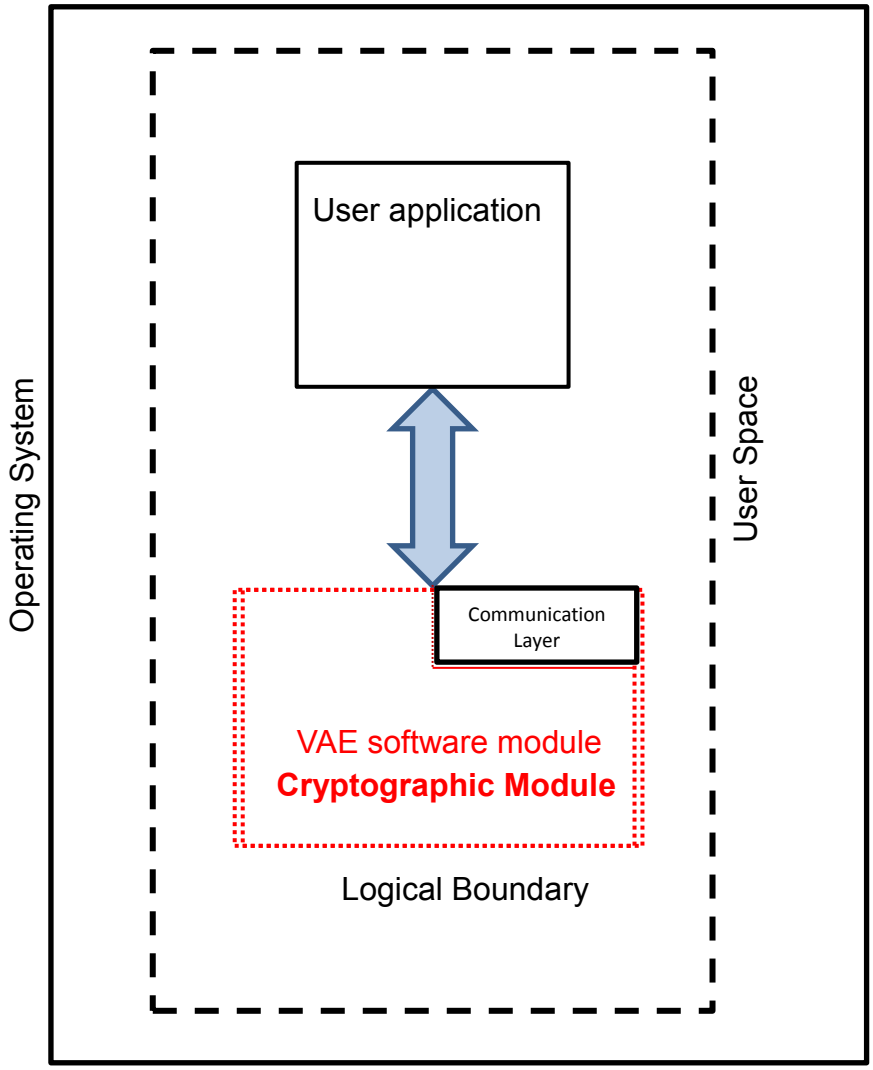

Figure 1 – Logical Cryptographic Boundary

The VAE software module in the diagram above is a shared object (.so) on Linux and dynamic link library (dll) on Windows. It is named libvorpkcs11.so on Linux and vorpkcs11.dll on Windows.

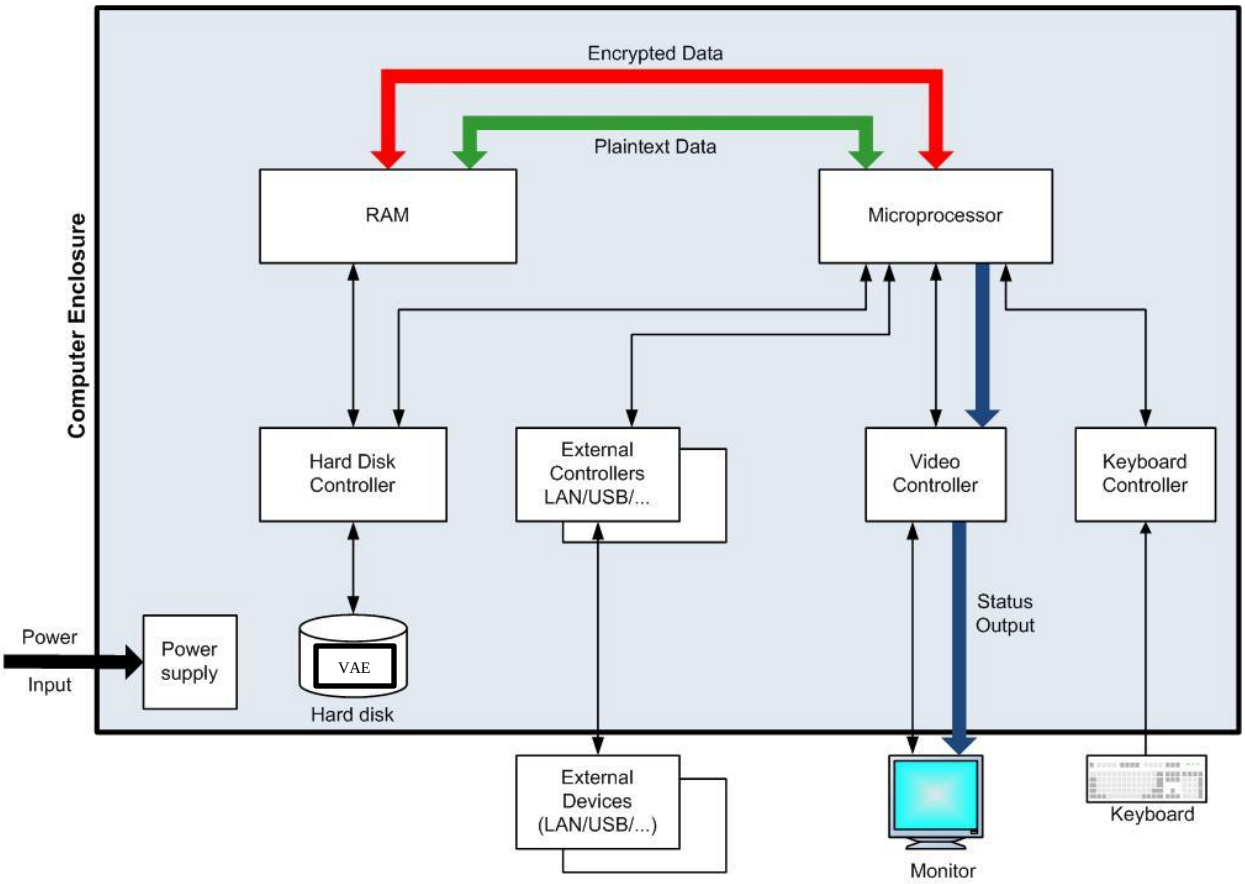

Figure 2 – Physical Cryptographic Boundary

2.2 Platform Considerations

This module is validated on Red Hat Enterprise Linux (RHEL) and Windows. All 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 or hard disk	Input parameters to VAE software module function calls
Data Output interface	External Devices (LAN/USB/…), Monitor or hard disk	Output parameters from VAE software module function calls
Control Input interface	External Devices (LAN/USB/…), Keyboard	Input parameters to VAE software module function calls
Status Output interface	External Devices (LAN/USB/…), Monitor or hard disk	Output parameters from VAE software module function calls Log message to VAE log file
Power Interface	Computer Power Supply Port	N/A Power interface provided by the computer

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

4 ROLES, SERVICES AND AUTHENTICATION

4.1 Roles and Services

The cryptographic officer role installs and uninstalls the Vormetric Application Encryption agents. It is implicitly assumed. The user role has access to VAE module function calls.

Role	Type of Authentication	Authentication Data
Crypto Officer	none	none
User	Username and password	8-character minimum/maximum 64

4.2 Authentication

The module provides username and password authentication for the user role.

Authentication Mechanism	Strength of Mechanism
Username and password	The module enforces at minimum 8-character passwords chosen from 76 human readable ASCII characters. The maximum password length is 64 characters. Taking into account that the password policy requires minimum 1 uppercase, 1 number, and 1 special character; thus for 8-character password the probability of a successful random attempt is 1/558,215,611,185,664. This is derived by taking the full set of available 8 character combinations and then excluding invalid passwords. The full set of 8 character combinations is: 76 ^8 = 1.11303E+15 Exclude the following invalid passwords: No numbers: 66^8 = 3.60041E+14 No uppercase: 50^8 = 3.90625E+13 No special 62^8 = 2.1834E+14 Exclude the following invalid passwords: All uppercase: 26^8 = 2.08827E+11 All numbers: 10^8 = 100000000 All special 14^8 = 1475789056 And include the following valid combinations because some excluded passwords are counted twice from the calculation above: No number and no uppercase = 40^8 = 6.5536E+12 No number and no special = 52^8 = 5.34597E+13 No upper and no special = 36^8 = 2.82111E+12 This gives us a total of 558,215,611,185,664 possible valid passwords.

4.3 Authorized Services

The Vormetric Application Encryption software module 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 Cryptographic Key/CSP is **read** or referenced by the service.
W -The Cryptographic Key/CSP is **written** or updated by the service.
E - The Cryptographic Key/CSP is **executed** by the service. (The item is used as part of a cryptographic function.)

The cryptographic module is a user space dynamically loaded shared library. It provides various APIs (application programming interfaces) that a user can call and encrypts or decrypts data according to the function that is called. The data input/output interfaces are done through the user making API function 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.

Services	Cryptographic Key/CSP	*Roles*	*Access*
Run Power-On Self Test	HMAC Integrity Key	No role	E
Initialization (Also known as "registration")	none	Crypto Officer	N/A
Cryptographic API calls (encrypt/decrypt) etc.	symmetric keys HMAC keys	User	RWE
Show Status	none	User	N/A
Authentication Service	password	Crypto Officer	R
Password Change	password	Crypto Officer	W
Key Zeroization	symmetric keys, HMAC keys	User	W

Table 3 – Authorized Services

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 Application Encryption software module 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*	*Platform/Processor*
Red Hat Enterprise Linux 7.1	64	Intel core i7-4770 CPU, ASUS Desktop PC M51AC-US002S
Windows Server 2012 R2	64	Intel core i7-4770 CPU, ASUS Desktop PC M51AC-US002S

Table 4 – Tested Platforms

Per section G.5 of the Implementation Guidance for FIPS 140-2, the CMVP allows vendor porting of a validated level 1 software cryptographic module 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 Vormetric Application Encryption software modules performs cryptographic operations. 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, key size 256-bit)	At vendor facility	Incorporated into binary	Protects the integrity of the module
VAE symmetric keys (AES 128-bit and 256-bit)	Generated externally by the Vormetric Data Security Server Module (NIST 800-90A DRBG)	Stored in obfuscated form in RAM only. Keys are zeroized before API returns.	Encrypts and decrypts user data
password	Crypto Officer types in password during installation	Password is hashed with SHA-384 and stored in a file on disk Password can be reset by re-registering the VAE module. To zeroize the password, the VAE module must be uninstalled.	To authenticate the user
VAE HMAC keys (256-bit)	Generated externally by the Vormetric Data Security Server Module (NIST 800-90A DRBG)	Stored in obfuscated form in RAM only. An obfuscation key is derived by using a SHA-384 hash of machine specific configuration. The cache is then x-or'ed with the obfuscation key. Keys are zeroized before API returns	Message authentication

Table 5 – Keys and CSPs

7.2 Approved Security Algorithms

The module keys map to the following algorithms certificates. All cryptographic functions are implemented in software inside the module boundary.

CAVP Cert	Algorithm	Standard	Mode/Method	Key Lengths, Curves or Moduli	Use
#4088	AES	FIPS 197, SP 800-38A	CBC,ECB,CTR	128, 256	Data Encryption/Decryption
		SP 800-38G	FF3 (Vendor Affirmed)	256	Format Preserving Encryption/Decryption radix = 2 - 65535 bytes minlen = 2 bytes, maxlen = 128k bytes
#3364	SHS	FIPS 180-4	SHA-256, SHA-384, SHA-512		Message digest
#2668	HMAC	FIPS 198	HMAC-SHA-256	256	Integrity check Message Authentication

Table 6 - 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 automatically.

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 “selftest failed!” or “integrity check failed!” is written to the log file and the module will cease operation. When each of the tests run to completion, the “selftest passed!” message and “integrity check passed!” message are written to the log. When all tests pass, the module is operating in FIPS mode. To run these on demand, re-initialize the module.

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

- AES CBC mode Encrypt KAT
- AES CBC mode Decrypt KAT
- AES CTR mode Encrypt KAT
- AES CTR mode Decrypt KAT
- AES ECB mode Encrypt KAT
- AES ECB mode Decrypt KAT

- SHA-256 KAT
- SHA-384 KAT
- SHA-512 KAT
- HMAC-SHA-256 KAT

Software Integrity Test:
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; 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 software 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

To configure the module, the Crypto Officer should:

- Install the Vormetric Application Encryption software package
- Register with a Vormetric Data Security Server
- Configure user name and password for the User role. Refer to the user guide for installation instructions.

User name and password can be zeroized by uninstalling the module. The platform's hard drive must be reformatted or overwritten after uninstallation.

After installation the User should verify that the message described in section 9.1 is emitted to ensure that the module is operating in the FIPS approved mode.
When the self-tests or integrity tests fail, the library exits. The user looks in the log which will state whether self-tests or integrity tests failed.

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. No special configurations or practices are required.

11 Design Assurance

Vormetric utilizes Apache Subversion (SVN) 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.