Vormetric, Inc

Vormetric Data Security Server Module

Firmware Version 4.4.1
Hardware Version 1.0

FIPS 140-2 Non-Proprietary Security Policy

Level 2 Validation

May 24th, 2012

Table Of Contents

1 INTRODUCTION

1.1 Purpose

This is a non-proprietary FIPS 140-2 Security Policy for the Vormetric Data Security Server firmware version 4.4.1 cryptographic module. It describes how this module meets all the requirements as specified in the FIPS 140-2 Level 2 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 19th, 2010	0.1	First Draft
Mike Yoder	September 27th, 2010	0.2	Second Draft
Mike Yoder	October 27th, 2011	0.3	Third Draft
Mike Yoder	May 24th, 2012	1.0	Final Version

2 PRODUCT DESCRIPTION

The Vormetric Data Security Server is a multi-chip standalone cryptographic module. The Vormetric Data Security Server is the central point of management for the Vormetric Data Security product. It manages keys and policies, and controls Vormetric Encryption Expert Agents. These agents contain the Vormetric Encryption Expert Cryptographic Module, which has been validated separately from this module.

The module implements AES, Triple DES, RSA, an X9.31 PRNG, SHA-1, SHA-256, HMAC-SHA-1, and HMAC-SHA-256 algorithms in the approved mode. The module also implements the non-approved SSL_RSA_WITH_3DES_EDE_CBC_SHA cipher mode.

The product meets the overall requirements applicable to Level 2 security for FIPS 140-2, with Key Management, Roles, Services and Authentication, and Design Assurance meeting the Level 3 requirements.

Security Requirements Section	***Level***
Cryptographic Module Specification	2
Cryptographic Module Ports and Interfaces	2
Roles and Services and Authentication	3
Finite State Machine Model	2
Physical Security	2
Operational Environment	N/A
Cryptographic Key Management	3
EMI/EMC	2
Self-Tests	2
Design Assurance	3
Mitigation of Other Attacks	N/A
Cryptographic Module Security Policy	2
Overall Level of Certification	2

Table 1 - Module Compliance

2.1 Cryptographic Boundary

The Vormetric Data Security Server is a 2U rack-mount hardware module. The cryptographic boundary is the physical boundary of the hardware module, the removable power supplies and power connectors are excluded from the cryptographic boundary. The physical design of the module is shown in the following two graphics:

Figure 1 – Hardware Module Cryptographic Boundary (with power supplies removed)

3 MODULE PORTS AND INTERFACES

The module is considered to be a multi chip standalone module designed to meet FIPS 140-2 Level 2 requirements. The module has the following interfaces

Data Input interface: The network interface cards are defined as the data input interface through which data is input to the module.
Data Output Interface: The network interface cards are defined as the data output interface through which data is output from the module.
Control input interface: The network interface cards and serial port are interfaces by which the module can be controlled.

Status output interface: The network interface cards, serial port, the LCD on the front panel, LEDs, and an audible power alarm are status output interfaces. The LEDs are located as follows: two status LEDs for each of the two Ethernet ports on the front panel, and two LEDs in the rear, one for each power supply.
Power Interface: Two removable redundant 110 volt external power supplies.

The table below describes the relationship between the logical and physical interfaces.

FIPS 140-2 Interface	*Logical Interface*	*Physical Interface*
Data Input interface	Data input parameters of API function calls	Ethernet
Data Output interface	Data output parameters of API function calls	Ethernet
Control Input interface	Control input parameters of API function calls that command the module	Ethernet, Serial Port
Status Output interface	Status output parameters of API function calls that show the status of the module	Ethernet, Serial Port, LED, LCD, audible power alarm
Power Interface		110v power interface

Table 2 – Mapping Physical and Logical Interfaces

4 ROLES, SERVICES AND AUTHENTICATION

The Vormetric Data Security Server module supports five distinct roles: System Administrator, Network Administrator, Domain Administrator, Security Administrator, and Network user. Within the Security Administrator role there are four sub-roles: audit, key, policy, and host. The module implements identity based authentication using passwords for the Crypto-Officer accounts. 2048 bit RSA certificates are used for the "Network user" account – these correspond to a Vormetric Encryption Expert Agent instance, which is a separately validated product.

4.1 Identification and Authentication

Role	*Group*	*Type of Authentication*	*Authentication Data*
System Administrator	Crypto-Officer	Identity Based	8-20 character alpha/numeric password
Network Administrator	Crypto-Officer	Identity Based	8-20 character alpha/numeric password
Domain Administrator	Crypto-Officer	Identity Based	8-20 character alpha/numeric password
Security Administrator	Crypto-Officer	Identity Based	8-20 character alpha/numeric password
Network User	User	Identity Based	2048 bit RSA Certificate

Table 3 - Authentication Types

4.2 Strengths of Authentication Mechanisms

Authentication Mechanism	*Strength of Mechanism*
Username and password	The module enforces at minimum 8-character passwords chosen from 78 human readable ASCII characters. The maximum password length is 20 characters. The module enforces an account lockout after a certain number of failed login attempts. This is configurable by a System Administrator; the default is that after 3 failed login attempts the account is locked for 30 minutes. The most lenient that it can be configured is to lock the account for 1 minute after 10 failed login attempts. This leads to a theoretical maximum for an attacker to attempt password entry 10 times per minute. Thus the probability of a successful random attempt is $1/78^8$, which is less than 1 in 1 million. The probability of success with multiple consecutive attempts in a one minute period is $10/(78^8)$, which is less than 1 in 100,000.
RSA Certificate	The module supports RSA 2048-bit certificates, which have a minimum equivalent computational resistance to attack of 2^{112}. There is no programmatic limit to the number of attempts in a given time frame, but it is limited to hardware and network latency. We can use an unrealistically high rate of one million attempts per second (60 million per minute) for our purposes in this calculation. Thus the probability of a successful random attempt is 2^{112}, which is less than 1 in 1 million. The probability of success with multiple consecutive attempts in a one minute period is $60{,}000{,}000/2^{112}$, which is less than 1/100,000.

Table 4 – Strengths of Authentication Mechanisms

4.3 Roles and Services

Roles in the Vormetric Data Security Server apply to *Administrative Domains*. An administrative domain is a logical partition that is used to separate administrators, and the data they access, from other administrators. Administrative tasks are performed in each domain based upon each administrator's assigned role.

- The **System Administrator** role operates outside of domains. It creates domains and assigns administrators of the Domain Administrator role to the domains.
- The **Domain Administrator** role primarily serves to assign administrators into a domain.
- **Security Administrators** exist inside a domain, and are responsible for managing hosts, policies, keys, and audit settings.
- The **Network Administrator** role is used for network and system configuration only. It is a special, low-level type of administrator that does not interact with the other roles.
- The **Network User** corresponds to an instance of a Vormetric Encryption Expert Agent.

The Vormetric Data Security Server supports the services listed in the following table. The 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 mapping between Authorized Services and Keys can be found in Table 8.

Authorized Services	*System Administrator*	*Network Administrator*	*Domain Administrator*	*Security Administrator*	*Network User*
Run Power-On Self Test		W			
Show basic status on dashboard	R		R	R	
Create and delete administrator accounts; reset passwords	RWE				
Backup and restore	RWE				
Firmware upgrade	RWE	RWE			
Shutdown, reboot, restart Security Server		RW			
Generate CA certificate		RWE			
Generate server certificate		RWE			
Configure High Availability	RWE	RWE			
Zeroize all data and all key material		WE			
Create File System Keys				RWE	
Create Database Backup Keys				RWE	
Create, modify, and delete file system policies				RW	
Create, modify, and delete database backup policies				RW	
Import and export keys				RWE	
Apply guard points using policies (and remove them)				RW	
Submit a CSR and obtain a certificate					RWE
Obtain host/policy/key info					RE

Table 5 - Privileges of each role

5 PHYSICAL SECURITY

The module is a “multiple-chip standalone cryptographic module”. The module consists of production grade components which include standard passivation techniques. The module is enclosed in an opaque production-grade enclosure with tamper-evident seals placed on both sides of the module to indicate attempts at removing the cryptographic module’s cover.

Physical Security Mechanism	*Recommended Frequency of Inspection / Test*	*Inspection / Test Guidance Details*
Tamper Evident Seals	3 months	The tamper evident seals are only installed by the module manufacturer. A System or Network Administrator is required to inspect the tamper evident seals for visible signs of malice. Upon viewing any signs of tampering, the administrator must assume that the device has been fully compromised. The administrator is required to zeroize the cryptographic module and shall return the device to the factory.

Table 6 – Inspection/Testing of Physical Security Mechanisms

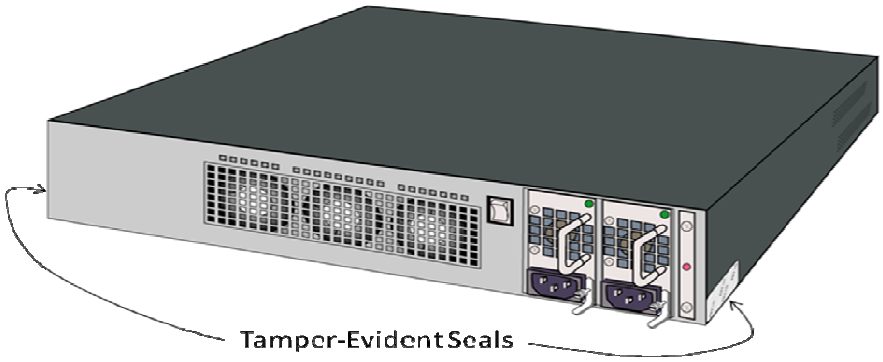

Figure 2 – Location of Tamper-Evident Seals

6 Operational Environment

The Vormetric Data Security Server is a limited operational environment. Since the operational environment is not modifiable, this section is not applicable.

7 CRYPTOGRAPHIC KEY MANAGEMENT

7.1 Cryptographic Keys and CSPs

The following table summarizes the module's keys and CSPs (Critical Security Parameters):

Key	Generation / Input	Storage	Use
Seed	Internally gathered	-	PRNG initialization
Seed Key	Internally gathered	-	PRNG initialization
Keystore Key	Internally gathered	Non-volatile	Protects the keystore using Triple DES.
Certificate Authority Key 2048-bit RSA	Generated internally using a PRNG compliant to ANSI X9.31	Keystore	Signs certificates
Server Key 2048-bit RSA	Generated internally using a PRNG compliant to ANSI X9.31	Keystore	Identifies the server in a TLS session; wraps the Master Key when transported to a failover server. Key establishment methodology provides 112 bits of encryption strength.
Master Key Encrypting Key AES 256	Generated internally using a PRNG compliant to ANSI X9.31	Keystore	Protects the Master Key
TLS Session Keys AES 256	Generated internally using a PRNG compliant to ANSI X9.31	None	Negotiated as part of the TLS handshake
Master Key AES 256	Generated internally using a PRNG compliant to ANSI X9.31	Database	Protects symmetric filesystem keys, RSA keys for database backups, password hashes, backup wrapper keys
Administrator Passwords	At least 8-character alphanumeric	Database	Authentication of administrators; stored as a SHA-256 hash encrypted by the Master Key

Key	Generation / Input	Storage	Use
File System Keys Triple DES, AES 128, AES 256	Generated internally using a PRNG compliant to ANSI X9.31	Database	Protects data inside a guard point in a Vormetric Encryption Expert Agent. Stored encrypted by the Master Key
Database Agent Backup Keys RSA 2048, 4096 bits	Generated internally using a PRNG compliant to ANSI X9.31	Database	Protects data inside a database backup protected by a Vormetric Encryption Expert Agent. Stored encrypted by the Master Key
Server Backup Key AES 256	Generated internally using a PRNG compliant to ANSI X9.31	Non-volatile	Protects backup information and key import/export. Also known as the "wrapper key".
Vormetric Upgrade Verification Key RSA 2048	At vendor facility	Non-volatile	Ensures that security server patches, upgrades, and licenses originate only from Vormetric.
Agent Public Key RSA 2048	Externally input to the module	Database	Vormetric Encryption Expert Agents create a 2048-bit RSA key pair. This is the public part. The private part is known as the "SECFS private key" in the Vormetric Encryption Expert Cryptographic Module. Usage: key wrapping; key establishment methodology provides 112 bits of encryption strength.
File System Key Encrypting Key AES 256	Generated internally using a PRNG compliant to ANSI X9.31	None. This is a one-time-use key	Encrypts file system keys when output to a Vormetric Encryption Expert Cryptographic Module.

Table 7 – Keys and CSPs

All of the keys in the above table can be input/output to/from the module except the TLS Session Keys and the Server Backup Key.

The following table shows the keys that are used in the Authorized Services from table 5. Note that the TLS Session Key is used implicitly in all Authorized Services because TLS is used to connect to the cryptographic module. Note also that Administrator Passwords are used implicitly in all Authorized Services because the administrators have to enter their passwords in order to perform actions.

Authorized Service	Cryptographic Key/CSP	Modes of Access
Show basic status on dashboard	N/A	N/A
Create and delete administrator accounts; reset passwords	Administrator Passwords Master Key	Account passwords are created by human entry, and are at least 8 alphanumeric characters. A SHA-256 hash of the password plus a salt is created, encrypted with the Master Key, and stored.
Backup and restore	Server Backup Key	Backups are encrypted using the private key, and are restored using the public key. This key is split in an M-of-N fashion using the "Shamir's Secret Sharing" scheme.

Authorized Service	Cryptographic Key/CSP	Modes of Access
Firmware upgrade	Vormetric Upgrade Verification Key	Upgrade packages are signed by Vormetric in the factory using this key. The module contains the public key, which is used to verify the authenticity of the upgrade package.
Shutdown, reboot, restart Security Server	N/A	N/A
Generate CA certificate	Certificate Authority Key	This key is generated and used to sign other certificates using RSA.
Generate server certificate	Server Key Certificate Authority Key	The Server Key is generated, and a certificate using that key is signed by the Certificate Authority Key.
Configure High Availability	Server Key (of the failover node), Master Key Encrypting Key, Master Key	The Master Key is encrypted with the Server Key of the Failover Node for transport, and the Master Key is stored encrypted with the Master Key Encrypting Key.
Zeroize all data and all key material	All	All data and key material are destroyed.
Create File System Keys	File System Keys, Master Key	Generation of the File System Keys. The File System Keys are encrypted using the Master Key before being stored.
Create Database Backup Keys	Database Backup Keys, Master Key	Generation of the Database Backup Key. The Database Backup Keys are encrypted using the Master Key before being stored.
Create, modify, and delete file system policies	N/A	N/A
Create, modify, and delete database backup policies	N/A	N/A
Import and export keys	Server Backup Key	Keys (File System Keys and Database Backup Keys) are encrypted using the Server Backup key during export. During import they're decrypted using this key.
Apply guard points using policies (and remove them)	N/A	N/A
Submit a CSR and obtain a certificate	Agent Public Key, Certificate Authority Key	The Vormetric Encryption Expert Agent creates a CSR; it is signed by the Certificate Authority Key using RSA.
Obtain host/policy/key info	File System Key Encrypting Key, Agent Public Key, File System Keys	A single-use File System Key Encrypting Key is generated. It is used to encrypt the File System Keys. It is itself encrypted by the Agent Public Key for transport.

Table 8 - Mapping of Cryptographic Keys and CSPs to Services

7.2 Key Destruction/Zeroization

All key material can be zeroized by any administrator with the Network Administrator role. When this action is performed, all key material and CSPs are removed, and the system enters a state that is indistinguishable from the state in which it was shipped to the customer.

7.3 Approved or Allowed Security Functions

The module keys map to the following algorithms certificates:

Approved or Allowed Security Functions	*Certificate*
Symmetric Encryption/Decryption	
AES: (CBC Mode; Encrypt/Decrypt; Key Size = 128, 256)	1838
Triple DES (3-key) (CBC Mode, Encrypt/Decrypt)	1192
Secure Hash Standard (SHS)	
SHA-1, SHA-256	1620
Data Authentication Code	
HMAC-SHA-1, HMAC-SHA-256	1093
Asymmetric Signature Keys	
RSA Key Generation (X9.31, 2048 and 4096 bits)	928
RSA Signature creation and verification (PKCS#1.5 Sig Gen and Sig Verify, 2048 bits)	928
Random Number Generation	
ANSI X9.31	965
Non-Approved Security Function	
SSL v3.0 cipher mode SSL_RSA_WITH_3DES_EDE_CBC_SHA	

Table 9 - FIPS Algorithms

8 SELF-TEST

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

8.1 Power-up Self-Tests

The power-up self tests are performed upon module startup prior to any data or control interface being available. All other processing is inhibited while the tests are in progress. If any test fails, an error status such as “FIPS Integrity Check Failed; Appliance halting” is displayed to the LCD on the front console, and the module will immediately power off. When all tests run to completion, the message “FIPS Integrity Check Completed OK” is displayed to the LCD on the front console, and the module continues normal startup.

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

- AES (CBC mode for Encrypt/Decrypt)
- Triple DES (CBC mode for Encrypt/Decrypt)
- RSA (Sign/Verify)
- SHA-1, SHA-256
- HMAC SHA-1, HMAC-SHA-256
- RNG KAT

Firmware Integrity Tests:
The module checks the integrity of its components using HMAC-SHA-256 during power on.

8.2 Conditional Self-Tests

The module performs the following conditional self-tests:

Firmware Load Test:
This test is run when the firmware is upgraded to verify that the firmware came from a trusted source and hasn't been modified during delivery and installation. It uses RSA signature verification using an RSA 2048-bit key.

Continuous RNG Test:
A continuous RNG test (that is, ensuring that two successive outputs from the RNG are not equal) is performed each time a pseudo-random number is requested.

Pairwise Consistency Test:
Pairwise consistency tests are run automatically when the module generates RSA key pairs. The module performs a sign operation with the private key and verifies it with the public key.

9 Crypto-Officer and User Guidance

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

9.1 Secure Setup and Initialization

The following steps must be taken to securely initialize the module:

- A user in the Network Administrator role must configure networking so that the module has a valid IP address and host name
- A user in the Network Administrator role must generate a CA certificate
- A user in the System Administrator role must log into the UI as the default user "admin"; an immediate password change is required

9.2 Module Security Policy Rules

The module is always operating in FIPS mode. There is a non-approved algorithm that is utilized by the SSL v3.0 cipher mode SSL_RSA_WITH_3DES_EDE_CBC_SHA. This occurs when using the Internet Explorer web browser on Microsoft Windows 2000, 2003, and XP. When using Microsoft Windows Vista, 2008, 7, and the Firefox and Chrome web browsers, ensure that TLS is enabled. All data passing through the SSL_RSA_WITH_3DES_EDE_CBC_SHA cipher mode will be considered plaintext.

10 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 language is used for all firmware components within the module.

11 Mitigation of Other Attacks

The module does not mitigate against any specific attacks.