

Vormetric, Inc
Vormetric Data Security Manager Module

Firmware Version 5.3.0

Hardware Version 3.0

**FIPS 140-2 Non-Proprietary
Security Policy**

Level 2 Validation

May 27, 2016



Table of Contents

1 Introduction	3
1.1 Purpose	3
1.2 References	3
1.3 Document History	3
2 Product Description	4
2.1 Cryptographic Boundary	4
3 Module Ports and Interfaces	5
4 Roles, Services, and Authentication	6
4.1 Identification and Authentication	6
4.2 Strengths of Authentication Mechanisms	7
4.3 Roles and Services	8
5 Physical Security	10
6 Operational Environment	10
7 Cryptographic Key Management	11
7.1 Cryptographic Keys and CSPs	11
7.2 Key Destruction/Zeroization	16
7.3 Approved or Allowed Security Functions	16
8 Self-Tests	17
8.1 Power-Up Self-Tests	17
8.2 Conditional Self-Tests	18
9 Crypto-Officer and User Guidance	18
9.1 Secure Setup and Initialization	18
9.2 Module Security Policy Rules	19
10 Design Assurance	19
11 Mitigation of Other Attacks	19

1 Introduction

1.1 Purpose

This is a non-proprietary FIPS 140-2 Security Policy for the Vormetric Data Security Manager firmware version 5.3.0 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
David Gardner, Ashvin Kamaraju, Steve He, Peter Tsai	3 February 2015	1.0	Firmware version 5.3.0 Hardware version 3.0
Ashvin Kamaraju, Peter Tsai, Steve He	20 th March 2015	1.1	Updated to incorporate feedback from Cygnacom
Peter Tsai	8 June 2015	1.2	Update tamper evident seals
Peter Tsai	30 July 2015	1.3	Update appliance photo, KDF, and KAT.
Peter Tsai, Steve He	20 August 2015	1.4	Update algorithms
Peter Tsai	26 August 2015	1.5	Update service tables, password section, and self-test
Peter Tsai	8 September 2015	1.6	Update security approve function table
Peter Tsai	13 October 2015	1.7	Update CAVP algorithm certificates
Peter Tsai	12 November 2015	1.8	Update ECDHE and non-approved function
Peter Tsai	8 March, 2016	1.9	Change ECDHE to EC DH, revise strength per minute, and update table 9 for TLS.
Peter Tsai	15 April, 2016	1.91	Update table of contents
Peter Tsai	25 April, 2016	1.92	Update table 9 to separate out allowed and non-approved
Peter Tsai	22 May, 2016	1.93	Update table 9 for ECDH key establishment
Peter Tsai	27 May, 2016	1.94	Update table-9

2 Product Description

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

The module implements AES, RSA, ECDSA, NIST SP 800-90A DRBG, SHA-256, SHA-384, HMAC-SHA-256, HMAC-SHA-384, and TLS KDF algorithms in the approved 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 Manager (DSM) is a 1U rack-mount hardware module. The cryptographic boundary is the physical boundary of the hardware module. The power connectors and the power connector wires in the back, two front empty disk bays and the disk-bay backplane, empty memory DIMM slots, heat-sink, empty PCI-e slots, USB connector housing and LAN connector housing near the back of air ventilation, jumper pins, TPM connector, and two SAS cables on the side air ventilation are excluded components. The removable power supplies and removable front bezel are outside the physical cryptographic boundary. The physical design of the module is shown in the following illustration:



Figure 1 – Hardware Module Cryptographic Boundary (front bezel 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 power switch, network interface cards, IPMI port, and serial port are interfaces by which the module can be controlled.

Status output interface: The network interface cards, serial port, the IPMI port, LEDs, and an audible power alarm are status output interfaces. The LEDs are located as follows: two status LEDs on the front panel for each of the two Ethernet ports on the rear panel.

Power Interface: Two removable redundant variable DC external power connector (power supplies are shipped with 100-240V), 2 status LEDs.

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

<i>FIPS 140-2 Interface</i>	<i>Logical Interface</i>	<i>Physical Interface</i>
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	Power Switch, Ethernet, Serial port, IPMI port
Status Output interface	Status output parameters of API function calls that show the status of the module	Ethernet, Serial port, LED, IPMI port, audible power alarm
Power Interface		Variable DC power connector (Power supplies shipped with 100-240V power interface), LEDs

Table 2 – Mapping Physical and Logical Interfaces

4 Roles, Services, and Authentication

The Vormetric Data Security Manager 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. An optional second factor of authentication is available with an RSA token. 2048-bit RSA certificates or ECDSA P-384 certificates are used for the “Network user” account – these correspond to a Vormetric Transparent Encryption Agent instance, which is a separately validated product.

4.1 Identification and Authentication

<i>Role</i>	<i>Group</i>	<i>Type of Authentication</i>	<i>Authentication Data</i>
System Administrator	Crypto-Officer	Identity Based	8-character minimum/32-character maximum alphanumeric password plus optional Two Factor Authentication (TFA) using an RSA token
Network Administrator	Crypto-Officer	Identity Based	8-character minimum/32-character maximum alphanumeric password plus optional TFA using an RSA token
Domain Administrator	Crypto-Officer	Identity Based	8-character minimum/32-character maximum alphanumeric password plus optional TFA using an RSA token
Security Administrator	Crypto-Officer	Identity Based	8-character minimum/32-character maximum alphanumeric password plus optional TFA using an RSA token
Network User	User	Identity Based	2048-bit RSA Certificate or ECDSA P-384 Certificate

Table 3 - Authentication Types

4.2 Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
<p>Username and password</p> <p>(+ optional TFA with RSA token)</p>	<p>The module enforces at minimum 8-character passwords chosen from 76 human readable ASCII characters. The maximum password length is 32 characters.</p> <p>The UI 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. In addition, the Network Administrator enforces an account lockout after 5 attempts for CLI access. The deny time is 5 seconds after each failed attempt. This leads to a theoretical maximum for an attacker to attempt password entry 5 times per minute. After 5th failed attempts, the CLI account is locked up to 15 minutes. CLI lockout time is not configurable and a process wakes up every 15 minutes to clear the lockout account.</p> <p>Taking into account that the password policy requires minimum 1 uppercase, 1 numbers, and 1 special character; thus for 8-character password the probability of a successful random attempt is $1/(26 \times 26 \times 10 \times 14 \times 76 \times 76 \times 76 \times 76)$ or $1/(3,157,396,336,640)$. That is less than 1 in 1 million. The probability of success with multiple consecutive attempts in a one minute period is $10/(3,157,396,336,640)$, which is less than 1 in 100,000.</p> <p>Two Factor Authentication is also optionally available using RSA tokens. This second factor decreases the probability of a successful random attempt significantly further.</p>
<p>RSA Certificate</p>	<p>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.</p> <p>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.</p>
<p>ECDSA Certificate</p>	<p>The module supports Elliptical Curve Cryptography P-384 certificates, which have a minimum equivalent computational resistance to attack of 2^{192}. 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.</p> <p>Thus the probability of a successful random attempt is 2^{192}, which is less than 1 in 1 million. The probability of success with multiple consecutive attempts in a one minute period is $60,000,000/2^{192}$, which is less than 1/100,000.</p>

Table 4 – Strengths of Authentication Mechanisms

4.3 Roles and Services

Roles in the Vormetric Data Security Manager 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 Transparent Encryption Agent.

The Vormetric Data Security Manager 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.

<i>Authorized Services</i>	<i>System Administrator</i>	<i>Network Administrator</i>	<i>Domain Administrator</i>	<i>Security Administrator</i>	<i>Network User</i>
Run Power-On Self-Test		E			
Show basic status on dashboard	R		R	R	
Manage preferences, LDAP, RSA tokens, SNMP, etc	RW		R		
Email and syslog setup	RW		RW	R	
Create and delete administrator accounts; Change and reset passwords	RWE		RWE		
Create and delete domains	RW		R		
Assign administrators to domains	RW		RW		
Create, import, export Wrapper Key	RWE				
Backup and restore	RWE				
Firmware upgrade	RWE	RWE			
Shutdown, reboot, restart Security Server		E			
Generate CA certificate		RWE			
Upload signed web console certificate	RWE				
Generate server certificate		RWE			
Configure High Availability	RWE	RWE			
View, Configure Network Settings		RW			

Authorized Services	System Administrator	Network Administrator	Domain Administrator	Security Administrator	Network User
Set date, time, NTP, etc		RW			
Zeroize all data and all key material		WE			
Create File System Keys (Agent Keys) and Certificates				RWE	
Create Vault Keys and Certificates				RWE	
Create Agent Database Backup Keys				RWE	
Create, modify, and delete file system policies				RW	
Import and Export file system policies				RW	
Create, modify, and delete agent database backup policies				RW	
Import and export keys				RWE	
Create and delete Signatures				RW	
Create and export Reports	RW		RW		
View, delete, and export Log	RW		RW	RW	
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 that include standard passivation techniques. The module is enclosed in an opaque production-grade enclosure with tamper-evident seals placed on the removable parts of the module to indicate attempts at removing the cryptographic module’s cover and the hard drives.

<i>Physical Security Mechanism</i>	<i>Recommended Frequency of Inspection / Test</i>	<i>Inspection / Test Guidance Details</i>
Tamper Evident Seals	3 months	There are 3 tamper-evident seals and these are installed only 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 Manager is a limited operational environment based on Linux. Therefore section 4.6.1 of the standard 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
800-90A CTR_DRBG "V"		Internally gathered	-	DRBG initialization
800-90A CTR_DRBG "Key"		Internally gathered	-	DRBG initialization
HMAC Integrity Key (HMAC-SHA 256-bit with 256-bit key)		At vendor facility	Incorporated into product	Protects the integrity of the module
Certificate Authority Key (for TLS Server)	ECDSA P-384	Generated internally compliant to FIPS 186-4 using a DRBG compliant to NIST SP 800-90A	Keystore	Signs certificates used when the DSM acts as a TLS server
	2048-bit RSA	Generated internally compliant to FIPS 186-4 using a DRBG compliant to NIST SP 800-90A	Keystore	Signs certificates used when the DSM acts as a TLS server
Certificate Authority Key (for TLS Client)	ECDSA P-384	Generated internally compliant to FIPS 186-4 using a DRBG compliant to NIST SP 800-90A	Keystore	Signs certificates used when the DSM acts as a TLS client
	2048-bit RSA	Generated internally compliant to FIPS 186-4 using a DRBG compliant to NIST SP 800-90A	Keystore	Signs certificates used when the DSM acts as a TLS client.
Server Key (for TLS Server)	ECDSA P-384	Generated internally compliant to FIPS 186-4 using a DRBG compliant to NIST SP 800-90A	Keystore	Identifies the DSM in a TLS session when it acts as a TLS server; Key establishment methodology provides 128 or 192 bits of encryption strength.

	2048-bit RSA	Generated internally compliant to FIPS 186-4 using a DRBG compliant to NIST SP 800-90A	Keystore	Identifies the DSM in a TLS session when it acts as a TLS server; Key establishment methodology provides 112 bits of encryption strength.
Server Key (for TLS Client)	ECDSA P-384	Generated internally compliant to FIPS 186-4 using a DRBG compliant to NIST SP 800-90A	Keystore	Identifies the DSM in a TLS session when it acts as a TLS client; Key establishment methodology provides 128 or 192 bits of encryption strength.
	2048-bit RSA	Generated internally using a DRBG compliant to NIST SP 800-90A	Keystore	Identifies the DSM in a TLS session when it acts as a TLS client; Key establishment methodology provides 112 bits of encryption strength.
Web Console Key	ECDSA P-384	Generated internally compliant to FIPS 186-4 using a DRBG compliant to NIST SP 800-90A	Keystore	Identifies the DSM to a web browser: https TLS requests. Key establishment methodology provides 128 or 192 bits of encryption strength.
	2048-bit RSA	Generated internally using a DRBG compliant to NIST SP 800-90A	Keystore	Identifies the DSM to a web browser: https TLS requests. Key establishment methodology provides 112 bits of encryption strength.
Master Key AES 256		Generated internally using a DRBG compliant to NIST SP 800-90A	Keystore	Protects the Protection Key
TLS Session Keys AES 256 (Including pre-master secret and master secret)		Generated internally using a DRBG compliant to NIST SP 800-90A	Not applicable. Session keys only persist for the life of the session.	Negotiated as part of the TLS handshake. Keys are exchanged using EC DH or RSA (depends on cryptography supported by the communicating entities)
TLS HMAC Keys HMAC-SHA-256 / HMAC-SHA-384		Generated internally using a DRBG compliant to NIST SP 800-90A	Not applicable. Session keys only persist for the life of the session	Used as part of TLS cipher suites

TLS Key Exchange EC DH 256-bits EC DH 384-bits	Generated internally using a DRBG compliant to NIST SP 800-90A	Not applicable. Session keys only persist for the life of the session	Negotiated as part of the TLS handshake using elliptical curve.
Protection Key AES 256	Generated internally using a DRBG compliant to NIST SP 800-90A	Database	Protects symmetric file system keys, vault keys, RSA keys for agent database backups, password hashes, backup wrapper keys
Server Wrapper Key AES 256	Generated internally using a DRBG compliant to NIST SP 800-90A	Encrypted and stored in file system	Protects DSM backups
Agent Public Key RSA 2048 bits public key	External Vormetric VTE agent generated using DRBG compliant to NIST SP 800-90A	Database	Protect a single-use File System Key Protection Key for transport.
Vormetric Upgrade Verification Key RSA 2048 bits public key	External generated using a DRBG compliant to NIST SP 800-90A and preloaded.	Obfuscated and Stored in file system	Used to verify the uploaded upgrade package
Symmetric File System Keys AES, Triple-DES, ARIA	Generated internally using a DRBG compliant to NIST SP 800-90A	Database	Encryption keys used by Transparent Encryption agent. The File System Keys are encrypted using the Protection Key before being stored.
Agent Database Backup Keys RSA	Generated internally using a DRBG compliant to NIST SP 800-90A	Database	Encryption keys used by database backup agent. The Agent Database backup Keys are encrypted using the Protection Key before being stored.
Symmetric Vault Keys AES, Triple-DES, ARIA	Manually entered via TLS	Database	Customer keys held by the DSM. The Symmetric Vault Keys are encrypted using the Protection Key before being stored.
Asymmetric Vault Keys RSA	Key entered via TLS	Database	Customer keys held by the DSM. The Asymmetric Vault Keys are encrypted using the Protection Key before being stored.

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. When services are configured to use Trip-DES, ARIA keys, or any non-approved algorithms, the services are in non-FIPS approved mode. The web console key supports both RSA and ECDSA certificates. The web console key is used for authorized services listed in table-5 with system administrator, domain administrator, and security administrator roles.

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 must enter their passwords to perform actions.

Authorized Service	Cryptographic Key/CSP	Modes of Access
Run Power-On Self-Test	N/A	N/A
Show basic status on dashboard	N/A	N/A
Manage preferences, LDAP, RSA tokens, SNMP, etc	N/A	N/A
Setup email and syslog	N/A	N/A
Create and delete administrator accounts; Change and 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 Encryption Key, and stored.
Create and delete domains	N/A	N/A
Assign administrators to domains	N/A	N/A
Create, import, export Wrapper Key	Server Wrapper Key	This is an AES-256 symmetric key used to protect backup. This key is split in an M-of-N fashion using the "Shamir's Secret Sharing" scheme.
Backup and restore	Server Wrapper Key	Backups are encrypted using Server Wrapper Key. This key is split in an M-of-N fashion using the "Shamir's Secret Sharing" scheme.
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 (both keys, as client and as server), Keystore Key, 800-90A CTR_DRBG "V", 800-90A CTR_DRBG "Key"	This key is generated and used to sign other certificates using RSA 2048 or ECDSA P-384.
Upload signed web console certificate	Web Console Key	The admin generates a CSR based on this key, has it signed by an external certificate authority, and uploads the signed certificate to the DSM

Authorized Service	Cryptographic Key/CSP	Modes of Access
Generate server certificate	Server Key Certificate Authority Key (both keys, as client and as server), Keystore Key, 800-90A CTR_DRBG "V", 800-90A CTR_DRBG "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, Protection Key, Keystore Key	The Protection Key is encrypted with the Master Key of the Failover Node for transport, and the Protection Key is stored encrypted with the Master Key.
View, Configure Network Settings	N/A	N/A
Set date, time, NTP	N/A	N/A
Zeroize all data and all key material	All	All data and key material are destroyed.
Create File System Keys (Agent Keys) and Certificates	File System Keys, Protection Key, 800-90A CTR_DRBG "V", 800-90A CTR_DRBG "Key"	Generation of the File System Keys. The File System Keys are encrypted using the Protection Key before being stored.
Create Vault Keys and Certificates	Vault Keys, Protection Key, 800-90A CTR_DRBG "V", 800-90A CTR_DRBG "Key"	Generation of the Vault Keys. The Vault Keys are encrypted using the Protection Key before being stored.
Create Agent Database Backup Keys	Agent Database Backup Keys, Protection Key, 800-90A CTR_DRBG "V", 800-90A CTR_DRBG "Key"	Generation of Agent Database Backup Keys. The Agent Database Backup Keys are encrypted using the Protection Key before being stored.
Create, modify, and delete file system policies	N/A	N/A
Import and Export file system policies	N/A	N/A
Create, modify, and delete agent database backup policies	N/A	N/A
Import and export keys	Server Wrapper Key	Keys (File System Keys) are encrypted using the Server Wrapper key during export. During import they're decrypted using this key.
Create and delete Signatures	N/A	N/A
Create and export Reports	N/A	N/A
View, delete, and export Log	N/A	N/A
Apply guard points using policies (and remove them)	N/A	N/A

Authorized Service	Cryptographic Key/CSP	Modes of Access
Submit a CSR and obtain a certificate	Agent Public Key, Certificate Authority Key (both keys, as client and as server), Keystore Key	The Vormetric Transparent Encryption Agent creates a CSR; it is signed by the Certificate Authority Key using RSA 2048 or ECDSA P-384.
Obtain host/policy/key info	File System Key Protection Key, Agent Public Key, File System Keys, 800-90A CTR_DRBG "V", 800-90A CTR_DRBG "Key"	A single-use File System Key Protection 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 Security Functions	Certificate
Symmetric Encryption/Decryption	
AES: (Java, CBC Mode; Encrypt/Decrypt; Key Size = 128, 256)	3499
AES: (OpenSSL, CBC Mode; Encrypt/Decrypt; Key Size=256) – only used for CTR-DRBG	3536
Secure Hash Standard (SHS)	
SHA-256, SHA-384 (Java)	2887
SHA-1 (Java) – only used for TLS KDF	2915
SHA-256 (OpenSSL) - prerequisite for the OpenSSL HMAC SHA-256 used for the firmware integrity check	2914
Data Authentication Code	
HMAC-SHA-256, HMAC-SHA-384 (Java)	2234
HMAC-SHA-1 (Java) – only used for TLS KDF	2260
HMAC-SHA-256 (OpenSSL) – used for firmware integrity check	2259
Asymmetric Signature Keys	
RSA Key Generation, TLS session key wrapping (NIST SP 800-90A, 2048-bits, 3072 bits)	1796
RSA Signature creation and verification (PKCS#1.5 Sig Gen and Sig Verify, 2048)	1796
ECDSA Key Generation (P-256, P-384)	712

Approved Security Functions	Certificate
ECDSA Signature creation and verification (P-256, P-384)	712
Random Number Generation	
DRBG NIST SP 800-90A (CTR-DRBG)	869
Key Derivation Function (<i>TLS protocol has not been reviewed or tested by the CAVP and CMVP</i>)	
TLS 1.2 KDF	589
TLS 1.0/1.1 KDF	590
Key Transport Scheme	
KTS	AES #3499 and HMAC #2234
Allowed Security Function	
NDRNG – entropy source for SP 800-90A DRBG	
EC DH, key size=256 and 384 bits (key agreement; key establishment methodology provides 128 or 192 bits of encryption strength)	
RSA key wrapper (key establishment methodology provides 112 bits of encryption strength)	
TLS Cipher suites: (<i>TLS protocol has not been reviewed or tested by the CAVP and CMVP</i>) TLS_RSA_WITH_AES_256_CBC_SHA, TLS_RSA_WITH_AES_128_CBC_SHA, TLS_RSA_WITH_3DES_EDE_CBC_SHA, TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256, TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	
Non-Approved Security Functions	
RSA 1024, RSA 4096 (non-compliant)	
ARIA, Key size = 128 and 256 bits (non-compliant)	
Triple-DES (non-compliant)	
SSH KDF (non-compliant) – SSH is not used to provide security for the FIPS module and is considered equivalent to plaintext for this validation	

Table 9 - FIPS Algorithms

This module does not use any mode or key lengths not included in Table 9. RSA 3072-bits is included in the RSA cert #1796 but the key is not being used in the firmware. In addition, AES-128 key is included in the AES cert #3536 for CTR-DRBG but the firmware only uses AES-256 key for CTR-DRBG. The firmware module supports non-deterministic random number generator (NDRNG) that uses internal, unpredictable physical sources of entropy that are outside of human control. Random numbers generated by the NDRNG are used as entropy source for the FIPS approved random number generator (DRBG cert#869).

8 Self-Tests

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 before 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” and “Self Test in progress: failed. Security Server cannot continue” are displayed to the serial console and IPMI console, and the module will

immediately power off. When all tests run to completion, the message “FIPS Integrity Check Completed OK” and “Self Test in progress: passed” are displayed to the serial port console and IPMI console, and the module continues normal startup.

See the serial console or IPMI console for self-test results.

Cryptographic Algorithm KATs:

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

- AES (CBC mode for Encrypt)
- AES (CBC mode for Decrypt)
- RSA (Sign KAT and Verify KAT)
- ECDSA (Sign KAT and Verify KAT)
- SHA-1, SHA-256, SHA-384
- HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384
- DRBG (Instantiate, Reseed, Generate 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. The same test is applied to the source of entropy.

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

Manual Key Entry Test:

Manual key entry is one way to create a File System Key. When manual key entry is used, the key is entered twice and the two entries are verified to be the same.

9 Crypto-Officer and User Guidance

This section describes 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 log into CLI as the default user “cliadmin” and an immediate password change is required
- 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 modules operates in FIPS mode after all the power up self-test have passed and the message described in section 8.1 has been displayed. When operated in FIPS mode, crypto-officer must ensure it is only using approved security functions.

10 Design Assurance

Vormetric uses Concurrent Versioning System (CVS) and Subversion (SVN) for configuration management of product source code. Vormetric also uses 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.