THALES ESECURITY

Vormetric Data Security Manager Virtual Appliance Module

SOFTWARE VERSION 6.0.2

Security Policy FIPS 140-2 Level 1

Copyright

Date	April 11, 2019
Doc. No	TesUSA-DDQ-000057-EN
Version	1

Contents

1 Introduction

1.1 Purpose

This is a non-proprietary FIPS 140-2 Security Policy for the Vormetric Data Security Manager Virtual Appliance software version 6.0.2 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

2 Product Description

The Vormetric Data Security Manager Virtual Appliance is a multi-chip standalone software cryptographic module operating in virtualization environment. 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, SHA-512, HMAC-SHA-256, HMAC-SHA-384 and TLS 1.2 KDF algorithms in the approved mode.

The product meets the overall requirements applicable to Level 1 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	1
Cryptographic Module Ports and Interfaces	1
Roles and Services and Authentication	3
Finite State Machine Model	1
Physical Security	N/A
Operational Environment	1
Cryptographic Key Management	3
EMI/EMC	1
Self-Tests	1
Design Assurance	3
Mitigation of Other Attacks	N/A
Cryptographic Module Security Policy	2
Overall Level of Certification	1

Table 1 - Module Compliance

2.1 Cryptographic Boundary

The Vormetric Data Security Manager Virtual Appliance (DSM) is a software security module designed to execute on a general purpose computer hardware platform running hypervisor. As a software cryptographic module, the virtual appliance has no physical characteristics. The module must rely on physical characteristics of the host system on which it runs. The module supports the physical interfaces of the Supermicro SSG-2028R-E1CR24N. See Figure 1 for a block diagram of the physical system. The module utilizes physical interfaces of the tested platform hosting the virtual environment upon which the module is installed. The hypervisor running on the physical system controls and maps the module's virtual interfaces to that of physical interfaces including processor, memory, network and hard disk.

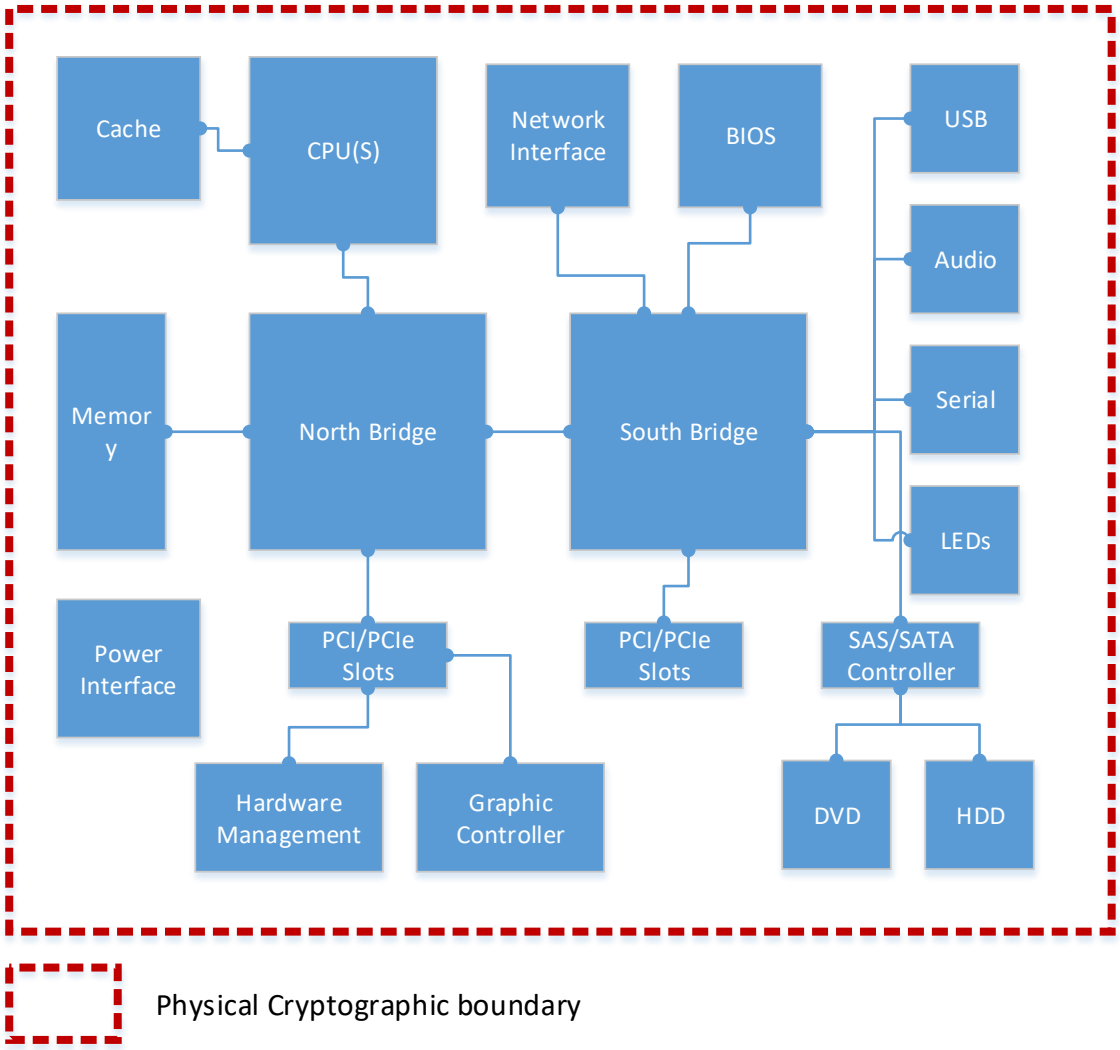

Figure 1 – Physical Module Cryptographic Boundary

The logical cryptographic boundary of the module consists of Vormetric Data Security Manage Virtual Appliance and the operating system running inside the hypervisor as shown in Figure 2. VMWare ESXi is the hypervisor that interacts with DSM virtual appliance.

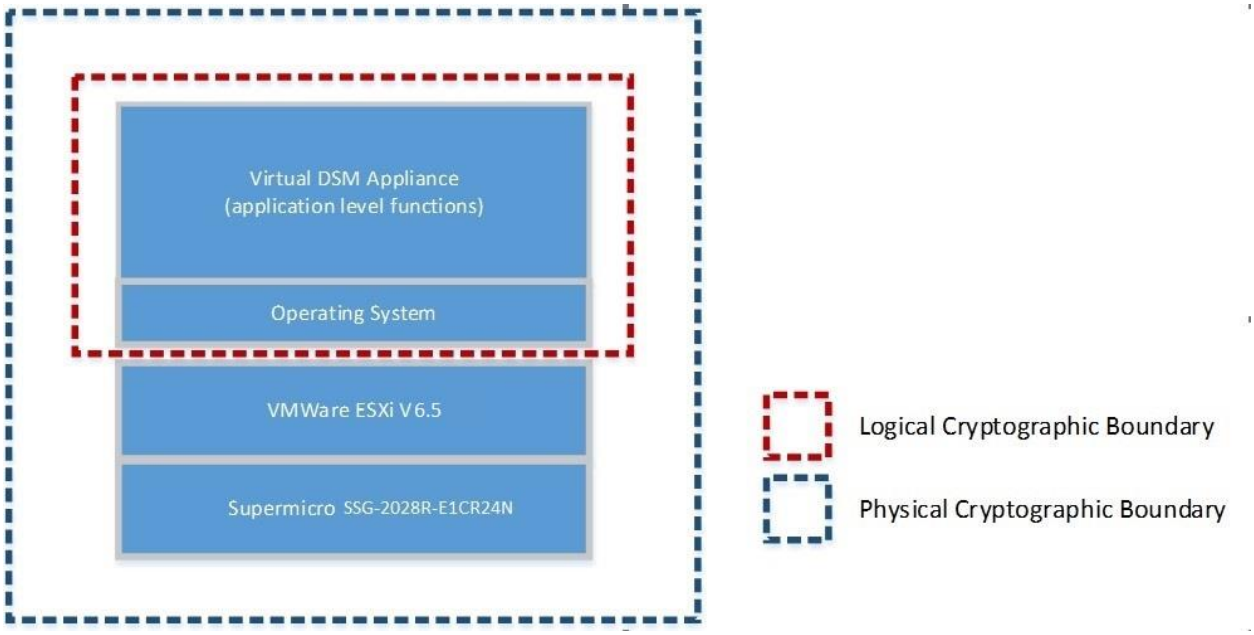

Figure 2. Logical Cryptographic Boundary

3 Module Ports and Interfaces

The module is considered to be a multi-chip standalone module designed to meet FIPS 140-2 Level 1 requirements. The module has the following interfaces

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

The following table 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, Keyboard
Status Output interface	Status output parameters of API function calls that show the status of the module	Ethernet, VGA port
Power Interface	N/A	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 Virtual Appliance 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.
Note: any software loaded into this module that is not shown on the module certificate, is out of the scope of this validation and requires a separate FIPS 140-2 validation

4.1 Identification and Authentication

Role	Group	Type of Authentication	Authentication Data
System Administrator	Crypto-Officer	Identity Based	8-character minimum alphanumeric password plus optional Two Factor Authentication (TFA) using an RSA token or LDAP password.
Network Administrator	Crypto-Officer	Identity Based	8-character minimum alphanumeric password plus optional TFA using an RSA token
Domain Administrator	Crypto-Officer	Identity Based	8-character minimum alphanumeric password plus optional TFA using an RSA token or LDAP password.
Security Administrator	Crypto-Officer	Identity Based	8-character minimum alphanumeric password plus optional TFA using an RSA token or LDAP password.
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
Username and password (+ optional TFA with RSA token)	The module enforces at minimum 8-character passwords chosen from 76 human readable ASCII characters. The maximum password length is 256 characters. 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 for 5 minutes. CLI lockout time is not configurable and a process wakes up every 5 minutes to clear the lockout account. 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 $1/(5.526007 \times 10^{14})$. That is less than 1 in 1 million. The probability of success with multiple consecutive attempts in a one minute period is $10/(5.526007 \times 10^{14})$, which is less than 1 in 100,000.

	Two Factor Authentication is also optionally available using RSA tokens. This second factor decreases the probability of a successful random attempt significantly further.
LDAP username and password	When an LDAP user is imported as a DSM administrator, the LDAP server's rules for password length and complexity are used. It is the Crypto-Officer's responsibility to only use a LDAP server with strong password rules and at least a 8 character password. Strength of authentication and lockout is the same as the "Username and password" authentication mechanism.
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.
ECDSA Certificate	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. 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.

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

The mapping between Authorized Services and Keys can be found in Table 7.

Authorized Services	System Administrator	Network Administrator	Domain Administrator	Security Administrator	Network user
Run Power-On Self-Test		E			
Show basic status on dashboard	R		R	R	
Manage preferences, LDAP, RSA tokens, etc	RW		R		
Email and syslog setup	RW		RW	R	
Create and delete administrator accounts; Change and reset passwords	RWE	RWE			
Create and delte accounts from their own domains		RWE	RWE		
Create and delete domains	RW		R		
Assign administrators to domains	RW		RW		
Create, import, export Wrapper Key	RWE		RWE		
Backup and restore	RWE		RWE		
Software 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 (HA)	RWE	RWE			
View, Configure Network Settings		RW			
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	
Import and export keys				RWE	
Create and delete Signatures				RW	
Create and export Reports	RW			RWE	
View, delete, and export Log	RW		R	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 Vormetric Data Security Manager Virtual Appliance is a multiple-chip standalone cryptographic software module. It does not include physical security mechanisms. Thus, the FIPS 140-2 requirements for physical security are not applicable.

6 Operational Environment

The module was tested and found to be compliant with FIPS 140-2 level 1 requirement on the following operational environment and hardware. All cryptographic keys and CSPs are under the control of the guest operating system.

- Supermicro SSG-2028R-E1CR24N server
    - Intel Xeon CPU (E5-2670V2 @2.5GHz)
    - 131MB of memory
    - 3.26TB of local storage in 8 removable drive bays
    - DVD-ROM
    - 2 RJ45 1Gb network
    - 6 USB
    - 1 VGA
    - 2 removal power supply modules with AC power cords and fault LEDs
    - 6 Status LEDs
    - Power and reset buttons

- VM Environment
    - VMWare ESXi 6.5
    - VM version 11
    - Guest Memory: 4GB
    - Provisioned Storage: 104GB
    - Guest O.S: Centos 7.2 (64-bit)

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 DRBG Seed		Internally gathered	-	DRBG initialization
800-90A DRBG Entropy Input String		Internally gathered	-	DRBG initialization
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 uses EC DH with either 256 or 384 bits keys and 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 uses EC DH with either 256 or 384 bits keys and 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 uses EC DH with either 256 or 384 bits keys and 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 Pre-master and master secret		Agreed upon using EC DH or generated by DRBG and transported using RSA (depends on cryptography supported by the communicating entities)	Not applicable. Session keys only persist for the life of the session.	Negotiated as part of the TLS handshake. Keys are established using EC DH or RSA (depends on cryptography supported by the communicating entities)
TLS Session Keys AES 128, AES 256		Derived using SP 800-135 TLS KDF from TLS Master Secret	Not applicable. Session keys only persist for the life of the session.	Negotiated as part of the TLS handshake. Keys are established using EC DH or RSA (depends on cryptography supported by the communicating entities)
TLS HMAC Keys HMAC-SHA-256 / HMAC-SHA-384		Derived using SP 800-135 TLS KDF from TLS Master Secret	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. The protection key encrypts the domain key.
Domain Key AES 256		Generated internally using a DRBG compliant to NIST SP 800-90A	Database	The domain key is encrypted by the protection key and is used to protect symmetric file system keys, vault keys, RSA keys for agent database backups, password hashes, backup wrapper keys for a defined domain.

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 128 and 256	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	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.
HA Keys (for TLS) ECDH, AES-256	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 for HA.

Table 6 – 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 Triple-DES, ARIA keys, RSA-1024, RSA-4096, SSH KDF 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, etc	N/A	N/A
Setup email and syslog	N/A	N/A

Authorized Service	Cryptographic Key/CSP	Modes of Access
Create and delete administrator accounts; Change and reset passwords	Administrator Passwords Master Key Domain 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	Protection key	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.
Software 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
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, HA Keys (for TLS)	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. TLS session keys are negotiated as part of the TLS handshake and keys are exchanged using EC DH.
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, Domain 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 Domain Key before being stored. (When service is configured to use Triple-DES and ARIA, the service is in non-FIPS approved mode.)

Authorized Service	Cryptographic Key/CSP	Modes of Access
Create Vault Keys and Certificates	Vault Keys, Domain 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. (When service is configured to use Triple-DES and ARIA, the service is in non-FIPS approved mode.)
Create Agent Database Backup Keys	Agent Database Backup Keys, Domain 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	Domain Key	N/A
Import and Export file system policies	Domain Key	N/A
Create, modify, and delete agent database backup policies	Domain Key	N/A
Import and export keys	Server Wrapper Key Domain 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)	Domain Key	N/A
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, Domain 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 7 - 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 the virtual appliance is freshly installed.

7.3 Approved or Allowed Security Functions

7.3.1 Approved security functions

The module keys map to the following algorithms certificates:

CAVP Cert	Algorithm	Standard	Mode/Method	Key Lengths, Curves or Moduli	Use
4846	AES	FIPS 197, SP 800-38A SP 800-38D	CBC, GCM	128, 256	Data Encryption/ Decryption (Java)
5536	AES	FIPS 197, SP 800-38A SP 800-38D	CBC, GCM	128[1], 256	Data Encryption/Decryption (OpenSSL)
3987	SHS	FIPS 180-4	SHA-256, SHA-384, SHA-512	-	Message Digest (Java)
4443	SHS	FIPS 180-4	SHA-256, SHA-384	-	Message Digest (OpenSSL)
3246	HMAC	FIPS 198-1	HMAC-SHA-256, HMAC-SHA-384	256	Message Authentication (Java used for TLS integrity check)
3688	HMAC	FIPS 198-1	HMAC-SHA-256, HMAC-SHA-384[2]	256	Message Authentication (OpenSSL used for software integrity check)
2664	RSA	FIPS 186-4	SHA-256, SHA-384, SHA-512 PKCS1 v1.5	2048	Key pair generation Digital Signature generation and verification PKCS1.5
2970	RSA	FIPS 186-4	SHA-256, SHA-384 PKCS1 v1.5	2048	Key Generation, Digital Signature Generation and Verification used for OpenSSL
1240	ECDSA	FIPS 186-4	SHA-256, SHA-384	P-256, P-384	Key pair generation Digital Signature Generation and verification
1703	DRBG NIST	SP 800-90A	CTR-DRBG	-	Deterministic Random Bit Generation Derivation function used.
N/A	CKG	SP 800-133	-	-	Generate symmetric keys and asymmetric key generation seeds (the result is an unmodified output from DRBG)
N/A	KTS	SP800-38F	AES GCM certificate 4846 and HMAC certificate 3246	128, 256	Key transport through TLS (import and export). Key establishment methodology provides 128 or 256 bits of encryption strength.
			AES GCM certificate 5536	256	Key transport through TLS (import and export) for HA
1482	TLS 1.2 KDF	SP800-135	-	-	TLS KDF used for Java
1979	TLS 1.2 KDF	SP800-135	-	-	TLS KDF used for OpenSSL

Table 8 – Approved security function

[1] AES-128 is CAVP tested but is not used by the module

[2] HMAC SHA-384 is CAVP tested but is not used by the module.

The module uses AES GCM within TLS v1.2 with GCM ciphersuites from SP 800-52 Rev 1, Section 3.3.1. In compliance with RFC 5246. When the IV exhausts the maximum number of possible values for a given session key a new handshake is triggered.
This module does not use any mode or key lengths not included in Table 8. AES-128 key is included in the AES cert #4846 for CTR-DRBG but the software only uses AES-256 key for CTR-DRBG. The software module supports non-deterministic random number generator (NDRNG) that uses internal, unpredictable physical sources of entropy (disk I/O interrupt and Intel RdRand instruction) 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 #1703), NDRNG provides it at least 256 bits of entropy. There is no assurance of the minimum strength of generated keys if porting to an untested platform. When services are configured to use any non-compliant algorithms, the services are in non-FIPS approved mode.

7.3.2 Allowed security functions

Algorithm	Caveat	Use
NDRNG		Entropy source for SP 800-90A DRBG
RSA key wrapping	Provides 112 bits of encryption strength	Key establishment
Elliptic Curve Diffie-Hellman, Supported curves: P-256 and P-384	Provides 128 and 256 bits of encryption strength	Key agreement, Key establishment. Used for TLS and TLS for HA.

Table 9 – Allowed security function

7.3.3 Non-Approved Algorithms

Algorithm	Use
Triple-DES (non-compliant)	Encryption / Decryption
RSA 1024, RSA 4096 (non-compliant)	Key generation
ARIA, Key size = 128 and 256 bits (non-compliant)	Key generation
SSH KDF (non-compliant)	SSH shall not be used in an approved mode of operation.

Table 10 – Non-Approved Algorithms

7.3.4 TLS Cipher Suites

Algorithm	Supported TLS Cipher Suites
TLS Cipher suite	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 TLS_RSA_WITH_AES_256_CBC_SHA256 TLS_ECDHE-RSA-AES256-GCM-SHA384

Table 11 – Supported TLS Cipher Suites

Note that TLS protocol, other than the KDF, has not been reviewed or tested by the CAVP and CMVP.

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 virtual VGA 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 virtual VGA console, and the module continues normal startup.

See the virtual VGA port for self-test results.

Cryptographic Algorithm KATs:

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

- AES for OpenSSL
- AES for Java
- RSA (Sign KAT and Verify KAT) for OpenSSL
- RSA (Sign KAT and Verify KAT) for TLS for HA
- ECDSA (Sign KAT and Verify KAT)
- SHA-256, SHA-384 for OpenSSL
- SHA-256, SHA-384 for Java
- HMAC_SHA256 for Java
- HMAC_SHA256, HMAC_SHA384 for OpenSSL
- DRBG (Instantiate, Reseed, Generate KAT) for OpenSSL

Software 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:

Software Load Test:

This test is run when the software is upgraded to verify that the software 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
- A user in the Network Administrator role shall enable TLS for HA before any High Availability is configured.

9.2 Module Security Policy Rules

The module operates in FIPS mode after all the power up self-test have passed and the message described in section 8.1 has been displayed. Note that to operate in FIPS mode TLS for High Availability must be enabled. When operated in FIPS mode, crypto-officer must ensure it is only using approved security functions.

The module uses AES GCM only within TLS v1.2 and this automatically enforces the IG A.5 IV restoration condition 3 where a new key for the AES GCM encryption/decryption is established in the case where the module’s power is lost and then restored.

Note: network administrator shall not enable TLS1.0/1.1 support

10 Design Assurance

Vormetric uses 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 software components within the module. The secure distribution method of DSM software is via the Vormetric support website. The support website has user and password authentication and files are transferred over HTTPS secure communication.

11 Mitigation of Other Attacks

The module does not mitigate against any specific attacks.