HyTrust KeyControl® Cryptographic Module Security Policy

For FIPS 140-2 Validation

FIPS 140-2 Non-Proprietary Security Policy

Contents

Contents 2
Revision History 3
Introduction 3
References 4
Cryptographic Boundary 4
Ports and Logical Interfaces 5
Security rules 6
Identification and Authentication Policy 8
Services / Critical Security Parameters 8
Physical Security Policy 12
Operational Environment 12
Mitigation of Other Attacks Policy 12
Appendix A 13

Revision History

Author	Date	Version	Description
Steve Pate	November 10th 2015	1.0	Initial public release

Introduction

The HyTrust KeyControl® Cryptographic Module (version 1.0) is a software-only multi-chip standalone cryptographic module designed to provide cryptographic key management for HyTrust KeyControl virtual appliances.

HyTrust KeyControl creates, stores, manages and delivers data encryption keys to Windows and Linux physical and virtual machines where they are used to encrypt files and devices. It implements the following approved algorithms:

- AES (128, 256) CBC (Cert. #3397)
- AES-XTS (user space) (XTS_256) (Cert. #3432)
- AES-XTS (XTS_256) (Cert. #3431)
- HMAC SHA256 (Cert. #2168)
- SHA-1, 256 (Cert #2813)
- DRBG SP800-90A (AES256_CTR with derivation function) (Cert. #813)

The module also uses RSA key encapsulation: non-approved (allowed as per FIPS 140-2 IG D.9). AES-XTS is only used for encryption/decryption of KeyControl disks (storage-level encryption).

The module only supports a FIPS-mode of operation. There is no non-FIPS mode supported.

This Security Policy contains information regarding this implementation, and procedures necessary for the correct handling of the cryptographic module.

The FIPS 140-2 security levels for the module are shown in Table 1:

Security Requirement	Security Level
Cryptographic Module Specification	1
Cryptographic Module Ports and Interfaces	1
Roles, Services, and Authentication	1
Finite State Model	1
Physical Security	N/A
Operational Environment	1
Cryptographic Key Management	1
EMI/EMC	1
Self-Tests	1
Design Assurance	3
Mitigation of Other Attacks	N/A
Overall Level of Certification	1

Table 1 – Security Levels References

References

The HyTrust Cryptographic Module Security Policy complies with the eleven sections of FIPS 140-2. You can view more information about the FIPS 140-2 standard on the NIST website – http://csrc.nist.gov/groups/STM/cmvp/index.html

Visit http://www.hytrust.com for more information about HyTrust.

Cryptographic Boundary

Figure 1 shows the major components of the KeyControl appliance. The components that are in red are inside the KeyControl® Cryptographic Module boundary.

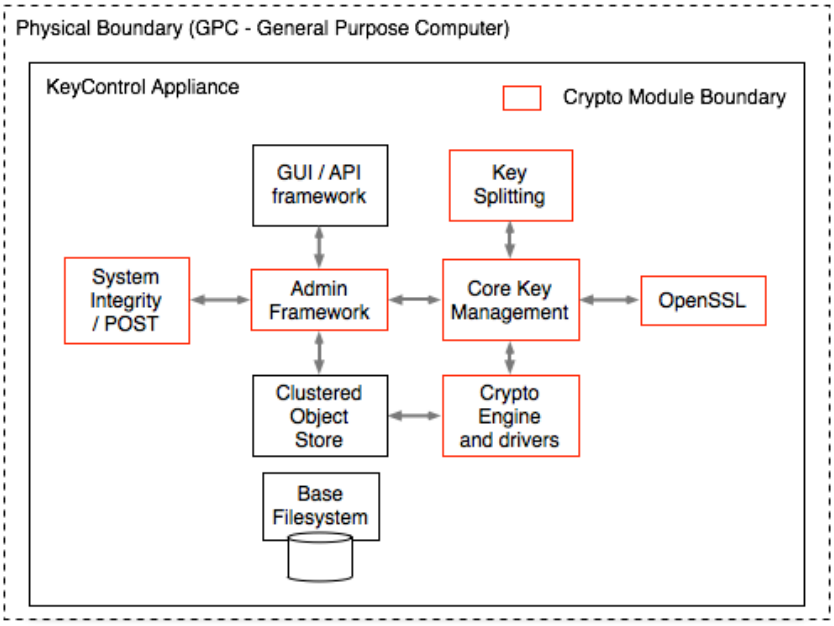

Figure 1 – ***Cryptographic Boundary***

Ports and Logical Interfaces

Table 2 displays the ports and interfaces that the module contains.

Function	Logical Interface
Input API parameters	Data Input
Output API parameters	Data Output
Function API Call	Control Input
Return API Values	Status Output

Table 2 – Specification of Cryptographic Module Ports and Logical Interfaces

Following is the mapping of the physical ports/interfaces to the logical ports/interfaces available to the module:

1. Video connector: Connects a monitor to the general-purpose computing platform: Data Output, Status Output.

2. USB connectors: Connects peripheral general-purpose I/O devices such as mouse, keyboard, and monitor: Data Input, Data Output, Control Input, and Status Output.

3. Ethernet connectors: provides network connectivity: Data Input, Data Output, Control Input, and Status Output.

4. Serial connector: connects peripheral general-purpose I/O devices such as mouse, keyboard, and monitor.

5. Power supply unit: Power input

Security rules

In order to use Approved security functions, the operator is required to properly configure the module to be placed into FIPS Approved mode. Once the FIPS Approved mode has been established, the operator is able to perform various security functions. To place the module into the FIPS Approved mode, the operator is required to perform the following steps:

- Obtain the KeyControl media from HyTrust (ISO or OVA format).
- Power on the physical ESX server, ensure that vCenter is running then log into vCenter using the VMware web-based GUI.
- Install KeyControl as a new virtual machine on top of the appropriate ESX server.
- As the Cryptographic Officer, herein and after referred to as the Security Admin, login through the web-based GUI, accept the EULA, provide email information for alerting and change the Security Admin password.
- At this point the module will now be operating in FIPS-mode. Following a reboot, the module will automatically enter FIPS-mode after executing power-on self-tests.
- Ensure that full and restricted support login capabilities are disabled while operating KeyControl in FIPS mode. There are no specific tasks to be performed here but ensure that the root password for the console menus is kept securely, which will prevent enabling of support login.

The cryptographic module fully implements the SP800-90A Section 11.3 requirements, and therefore meets the requirements of SP800-90A Section 11.3.

This section documents the rules that are enforced by the cryptographic module to satisfy the requirements for a Level 1 software-only module as per FIPS 140-2.

- The module performs the following tests:

  1. Power-up self-tests

     a. HMAC-SHA-256 KAT

     b. AES CBC Encrypt KAT

     c. AES CBC Decrypt KAT

     d. AES XTS Encrypt KAT

     e. AES XTS Decrypt KAT

     f. DRBG KAT

     * Software/firmware integrity test - HMAC-SHA-256

* Critical Functions Test:
  - RSA 2048 bit key size KAT (Encrypt)
  - RSA 2048 bit key size KAT (Decrypt)
  - Split Knowledge KAT

2. Conditional tests
   a. Continuous Random Number Test - performed on NDRNG
   b. Continuous Random Number Generator Test - performed on DRBG
   c. RSA 2048 Pairwise Consistency Test (Encrypt/Decrypt)
   d. Software Load Test: N/A
   e. Bypass Test: N/A
   f. Manual Key Entry Test: N/A

- The module does not provide access to CSPs until the operator is in a valid role.
- Only the security administrator can perform zeroization.
- The operator is capable of commanding the module to perform the power-up self-test by cycling power or resetting the module.
- Power-up self-tests do not require any operator intervention.
- Data output is inhibited during key generation, self-tests, zeroization, and error states.
- Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
- There are no restrictions on which keys or CSPs are zeroized by the zeroization service. The Cryptographic Officer must be in control of the module during zeroization.
- The module does not support a maintenance interface or role.
- The module does not support manual key entry.
- The module does not enter or output plaintext CSPs.
- The module does not output intermediate key values.
- The module enforces logical separation of all data inputs, data outputs, control inputs, and status outputs.
- The general purpose-computing platform includes a power port.
- Roles are implicitly assumed based upon the service requested.
- The following operating system capabilities shall not be used while the module is operating the FIPS Approved mode:
  - Turning on the full and restricted support login capability.
  - Extraction of support data either through the web-based GUI or through restricted support login.

Identification and Authentication Policy

The HyTrust Cryptographic module is designed to meet the requirements specified for a Level 1 software-only module as per FIPS 140-2, and support the following roles in the FIPS Approved mode of operation:

- Cryptographic Officer: This role is responsible for the correct initialization of the cryptographic module. These officers are also responsible for providing their key parts during a restore from backup.
- User: This role has access to a subset of the cryptographic module as described in the User Guidance Manual.

Services / Critical Security Parameters

The module contains the following CSPs:

- Object Store Key (AES-256)
- Master Key (AES-256)
- Admin Private Key (RSA-2048)
- Auth Private Key (RSA-2048)
- Authentication Passphrase (AES-128)
- Agent Data Encrypt Keys (AES-128/256 for CBC/XTS)
- DRBG Seed
- DRBG Value V
- DRBG Key
- DRBG Internal State

The module contains the following Public Keys:

- Auth Public Key (RSA 2048)
- Admin Public Key (RSA 2048)

All objects within KeyControl are encrypted with the Object Store Key. The Object Store Key is encrypted with the Master Key. The Master Key is encrypted with the Admin Public Key. The Admin Private Key is split into “M” key parts using Shamir’s Secret Sharing Algorithm and dispersed to the “M” Security Administrators.

All approved cryptographic functions are shown in Table 3.

Label	Standard	Cryptographic Function
AES	FIPS 197	Advanced Encryption Standard
XTS	SP800-38E	XEX-based Tweaked-cookbook mode with ciphertext Stealing

SHS	FIPS 180-4	Secure Hash Standard
HMAC	FIPS 198	Keyed-Hash Message Authentication Code
DRBG	SP800-90A	Deterministic Random Bit Generator

Table 3 – FIPS Approved Cryptographic Functions

Table 4 lists FIPS non-approved cryptographic functions that are allowed while operating in FIPS approved mode.

Label	Standard	Cryptographic Function
KW	FIPS 140-2 IG D.9	RSA (key wrapping; key establishment methodology provides 112 bits of encryption strength)
NDRNG	N/A	/dev/random

Table 4 – non-FIPS Approved Cryptographic Functions Allowed in FIPS Approved mode

As we describe the services authorized for roles, access rights within services for the CSPs, we will refer to the legend in Table 5.

Item	Type of Access
G	Generate
I	Input
O	Output
U	Use
Z	Zeroize
R	Revoke
N	Unrevoke

Table 5 – Legend for Type(s) of Access

Table 6 lists all the possible methods of access to Cryptographic Keys and CSPs.

Role		Service	Cryptographic Keys & CSPs	Type(s) of Access
Crypto-graphic Officer	User			
☐		Initialization: generates cryptographic key material and prepares the module for use.	Object Store Key Master Key Admin Private Key Auth Private Key Auth Public Key Admin Public Key DRBG Seed DRBG Value V DRBG Key DRBG Internal State	G, U G, U G, O G G, O G, U G G G G
☐		Bootstrap / Object store interactions	Object Store Key Admin Private Key Master Key Auth Private Key Auth Public Key DRBG Seed DRBG Value V DRBG Key DRBG Internal State	U I, U U G G, O G G G G
☐		Add Node to Cluster – KeyControl is an active-active cluster. When nodes are added to the cluster, the object store is replicated to the new node.	Authentication Passphrase Object Store Key Master Key Auth Private Key Auth Public Key Admin Private Key Admin Public Key DRBG Seed DRBG Value V	I I, O G G, U G, O, U G G G G

			DRBG Key DRBG Internal State	G G
☐	☐	Access of the object store during normal runtime – this includes generation of Data Encrypt Keys – an action performed in response to the DataControl Policy Agent in a remote VM requesting the issue of an AES key.	Object Store Key Agent Data Encrypt Keys DRBG Seed DRBG Value V DRBG Key DRBG Internal State	U G, O G G G G
☐		Migration / add node to cluster	Object Store Key Master Key Admin Private Key Auth Private Key Authentication Passphrase Agent Data Encrypt Keys Auth Public Key Admin Public Key	I, O I I, O I, O, U I, O, U I, O I, O, U I, O, U
☐		Key Recovery – in the event that a backup image was restored to a new platform.	Master Key Admin Private Key Object Store Key	U I, U U
	☐	Key Access Control / Revocation – users can revoke / unrevoke access to symmetric keys resulting in data being inaccessible.	Agent Data Encrypt Keys DRBG Seed DRBG Value V DRBG Key DRBG Internal State	R, G, N G G G G
☐		Zeroize – remove all CSPs and key material from the system	Object Store Key Master Key Admin Private Key Auth Private Key Authentication Passphrase	Z Z Z Z Z

			Agent Data Encrypt Keys Auth Public Key Admin Public Key	Z Z Z
☐		Self-Test	N/A	N/A
☐		Show Status	N/A	N/A

Table 6 – Services Authorized for Roles, Access Rights within Services

Physical Security Policy

This module is a software-only module therefore the physical security requirements of FIPS 140-2 are not applicable as shown in Table 7.

Physical Security Mechanisms	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
N/A	N/A	N/A
N/A	N/A	N/A

Table 7 – Physical Security Mechanisms

Operational Environment

As per FIPS 140-2, the HyTrust KeyControl Cryptographic module contains an operational environment that is modifiable, and meets the requirements for a Level 1 software-only module:

- FreeBSD 9.2 on VMware vSphere Hypervisor (ESXi) 5.5.0u2 on Dell Inc. PowerEdge R220, Intel Xeon CPU E3-1241v3 @ 3.50GHz (single user mode)

The operating system can be configured for single-user mode by ensuring that “Full Support” and “Restricted Support” login capabilities remain disabled.

Mitigation of Other Attacks Policy

The HyTrust Cryptographic module is not designed to mitigate against any attacks outside the scope of FIPS 140-2 as shown in Table 8.

Other Attacks	Mitigation Mechanism	Specific Limitations

N/A	N/A	N/A

Table 8 - Mitigation of Other Attacks

Appendix A

Following is a list of the cryptographic module CSPs:

1. Object Store Key:
   Description: AES-256-CBC; used to encrypt all objects within KeyControl
   Generation: via direct output of SP 800-90A DRBG as per SP800-133 Section 7.1
   Storage: stored on disk AES encrypted with Master key; plaintext in RAM
   Entry: AES encrypted with Auth Private key during node join
   Output: AES encrypted with Auth Private key during node join
   Destruction: actively overwritten by the zeroization service

2. Master Key:
   Description: used to wrap the Object Store Key
   Generation: via direct output of SP 800-90A DRBG as per SP800-133 Section 7.1
   Storage: Stored on disk in plaintext; also, an additional copy is stored on disk
   Wrapped with RSA 2048 with Admin public key; plaintext in RAM
   Entry: N/A
   Output: N/A
   Destruction: actively overwritten by the zeroization service

3. Admin Private Key:
   Description: RSA 2048 private key used to decrypt the Master Key
   Generation: via output of SP800-90A DRBG which is acceptable as per FIPS 140-2 IG D.9
   Storage: Split share in plaintext in RAM; full key is also plaintext in RAM
   Entry: Shamir Secret Sharing
   Output: Shamir Secret Sharing
   Destruction: actively overwritten by the zeroization service

4. Auth Private Key:

Description: RSA 2048 private key used for authentication
Generation: via output of SP800-90A DRBG which is acceptable as per FIPS 140-2 IG D.9

Storage: stored on disk AES encrypted with the Object Store Key; plaintext in RAM

Entry: N/A

Output: N/A

Destruction: actively overwritten by the zeroization service

5. Authentication Passphrase:

   Description: 16-byte AES key used to encrypt the Object Store Key

   Generation: N/A

   Storage: plaintext in RAM

   Entry: plaintext

   Output: N/A

   Destruction: actively overwritten by the zeroization service

6. Agent Data Encrypt Keys:

   Description: 128 and 256 bit AES keys

   Generation: via direct output of SP 800-90A DRBG as per SP800-133 Section 7.1

   Storage: plaintext in RAM; stored on disk AES encrypted with Object Store Key

   Entry: AES encrypted with Object Store Key

   Output: AES encrypted with Object Store Key

   Destruction: actively overwritten by the zeroization service

7. DRBG Seed

   Description: Seeding material for the SP800-90A CTR_DRBG

   Generation: internally generated; raw random data from /dev/random

   Storage: Plaintext in RAM

   Entry: N/A

   Output: N/A

   Destruction: actively overwritten by the zeroization service

8. DRBG Value V

   Description: Internal State of SP800-90A CTR_DRBG

   Generation: via SP 800-90A DRBG

Storage: Plaintext in RAM

Entry: N/A

Output: N/A

Destruction: actively overwritten by the zeroization service

9. DRBG Key

   Description: Internal State of SP800-90A CTR_DRBG

   Generation: via SP 800-90A DRBG

   Storage: Plaintext in RAM

   Entry: N/A

   Output: N/A

   Destruction: actively overwritten by the zeroization service

10. DRBG Internal State

    Description: Internal State of SP800-90A CTR_DRBG

    Generation: via SP 800-90A DRBG

    Storage: Plaintext in RAM

    Entry: N/A

    Output: N/A

    Destruction: actively overwritten by the zeroization service

Following is a list of the cryptographic module public keys:

1. Auth Public Key:

   Description: RSA 2048 public key used to wrap the Object Store Key

   Generation: via output of SP800-90A DRBG which is acceptable as per FIPS 140-2 IG D.9

   Storage: stored on disk AES encrypted with the Object Store Key; plaintext in RAM

   Entry: AES encrypted with Object Store Key

   Output: AES encrypted with Object Store Key

   Destruction: actively overwritten by zeroization service

2. Admin Public Key:

   Description: RSA 2048 public key used to encrypt the Master Key

Generation: via output of SP800-90A DRBG which is acceptable as per FIPS 140-2 IG D.9

Storage: plaintext in RAM

Entry: N/A

Output: N/A

Destruction: actively overwritten by zeroization service