HyTrust KeyControl Cryptographic Module

FIPS 140-2 Non-Proprietary Security Policy

© 2021 HyTrust Inc. All rights reserved. www.hytrust.com

This document may be freely reproduced and distributed whole and intact including this copyright notice.

Contents

Revision History

Author	Date	Version	Description
Kannan Sasi	September 10th 2019	1.0	Initial Version
Kannan Sasi	Dec 7th 2021	1.1	NIST Review
Kannan Sasi	Mar 22, 2022	1.2	NIST Review

© 2021 HyTrust Inc.

Introduction

The HyTrust KeyControl Cryptographic Module (version 1.1), also referred to as KeyControl in this document 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-ECB
- AES-GCM
- AES-XTS (kernel)
- AES-ECB (kernel)
- HMAC-SHA256
- SHA-256
- PBKDF2
- SP800-90A DRBG

The module also uses RSA key encapsulation: non-approved (allowed as per FIPS 140-2 IG D.9)

The module only supports 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

© 2021 HyTrust Inc.

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.

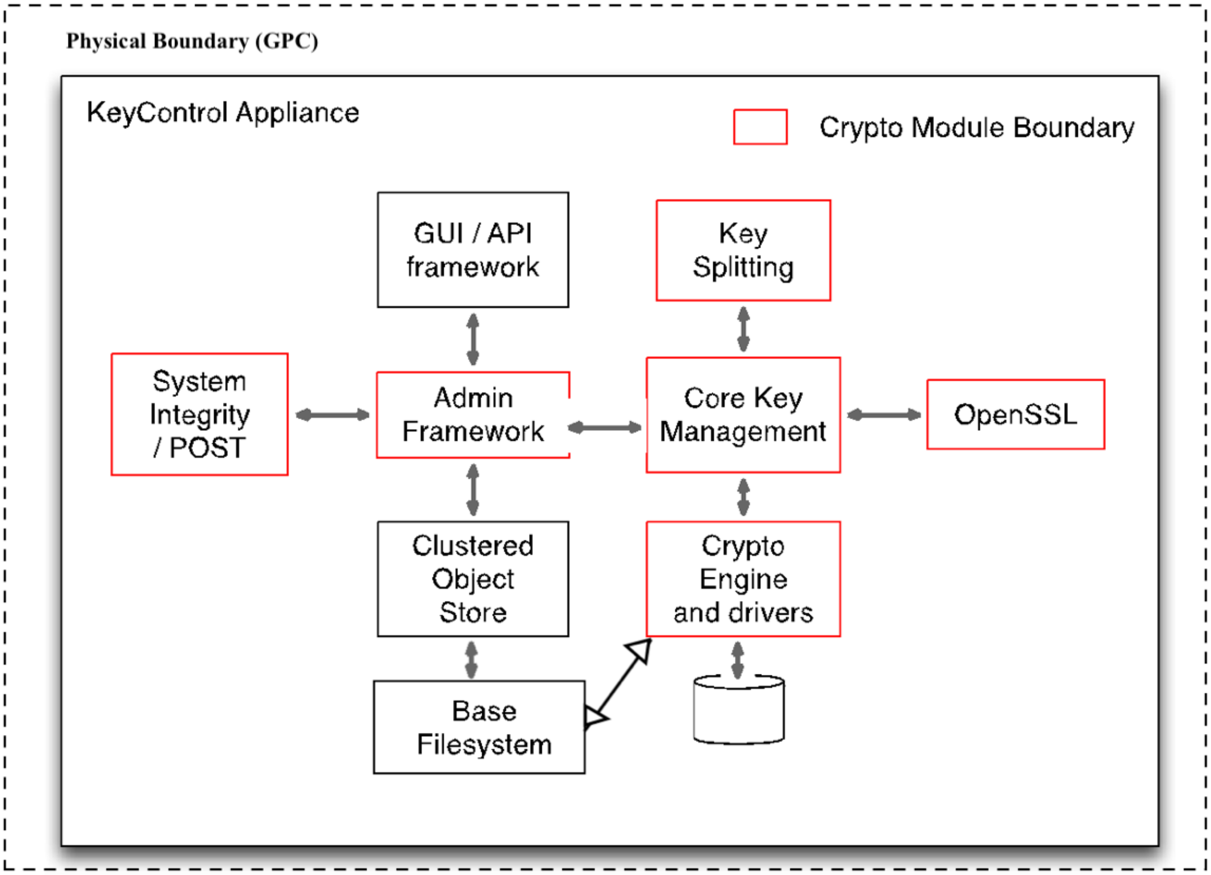

Figure 1 – ***Cryptographic Boundary***

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

© 2021 HyTrust Inc.

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

CAVP Certificates

There are algorithms, modes, and keys that have been CAVs tested but not used by the module. Only the algorithms, modes/methods, and key lengths/curves/moduli shown in this table are used by the module.

Cert Number	Algorithm	Standard	Mode/Method	Key Lengths, Curves or Moduli	Use
C2100 C2101	AES	FIPS 197 SP 800-38A SP 800-38E	ECB, XTS	256	Kernel Encryption and Decryption
A762 ** C2104 C2105	AES	FIPS 197 SP 800-38D	ECB, GCM	256	User mode Encryption and Decryption
C2104 C2105	SHS	FIPS 180-4 SP 800-107	SHA-256	SHA-256	Integrity validation
C2104 C2105	HMAC	FIPS 198-1 SP 800-107	SHA-256	256	Code Integrity validation
A762	DRBG	SP 800-90A	AES-CTR	256	Used for generating Encryption Keys and IV
C2104 C2105	CVL (RSA-DP)	FIPS 186-4 SP 800-56B	PKCS v1.5 padding	*2048	Used for unwrapping the Master Key
A762	RSA	FIPS 186-4 SP 800-56B	PKCS v1.5 padding	2048, 3072, 4096	Used for generation of Admin Key which wraps the Master Key
A762	PBKDF2	SP 800-132	HMAC, SHA256	256	Derive encryption keys from user passwords for wrapping Object Store Key and Master Key

© 2021 HyTrust Inc.

C2102 C2103	SHS	FIPS 180-4 SP 800-107	SHA-256	SHA-256	Code Integrity validation
C2102 C2103	HMAC	FIPS 198-1 SP 800-107	SHA-256	256	Code Integrity validation

Table 3 – Approved Algorithms

*RSA-DP can only be tested with 2048 bit key size in CAVS 21.4.

** AES (Cert. #A762) only supports AES-GCM; AES-ECB prerequisite tested via C2104 and C2105.

Security rules

In order to use Approved security functions, the Cryptographic Officer (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.
- FIPS mode of operation is guaranteed only if the processor on which it runs supports Intel RDRAND instruction. This requirement is in compliance with FIPS 140-2 IG G.5 - Maintaining validation compliance of software or firmware cryptographic modules .
- Modification of any files inside the FIPS boundary will result in a whitelist failure. This causes the message “Whitelist violation detected” to be printed on the console and the module powered off. The module is unrecoverable after this point and needs to be reinstalled.
- The operator must enter a passphrase that is 20 characters at minimum to comply with guidance set forth in SP800-132 for PBKDF2.

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.AES-256-ECB Encrypt KAT

        b.AES-256-ECB Decrypt KAT

        c.SHA-256 KAT

        d.HMAC-SHA-256 KAT

        e.RSA 4096 PKCS1.5 Encrypt KAT

        f.RSA 4096 PKCS1.5 Decrypt KAT

        g.AES-256-XTS (DM_crypt) Encrypt KAT

        h.AES-256-XTS (DM_crypt) Decrypt KAT

        i.AES-256-GCM (OpenSSL) Encrypt KAT

        j.AES-256-GCM (OpenSSL) Decrypt KAT

        k.PBKDF2 SP800-132 KAT

        l. SHA-256 (Gcrypt) KAT

        m. DRBG SP800-90A CTR KAT

    2. Software/firmware tests
        a. HMAC-SHA-256

    3. Critical Functions Tests
        a. Split Knowledge KAT

    4. Conditional tests
        a. Continuous Random Number Test - performed on NDRNG
        b. Continuous Random Number Generator Test - performed on DRBG
        c. RSA 4096 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.

© 2021 HyTrust Inc.

- 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.
- 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.
- The IV used in AES-GCM is generated internally at its entirety *randomly*.
    - The generation **uses** an Approved DRBG that is internal to the module’s boundary
    - The IV length is 96 bits (per **SP 800-38D**)

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

See Annex A for the list of CSPs in the module.

All objects within KeyControl are stored in a block device which is encrypted using dm-crypt with the Object Store Key. The Object Store Key is encrypted with the Master Key. The Master Key

© 2021 HyTrust Inc.

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.

The Master Key can also be encrypted with a key derived from an Admin supplied passphrase using PBKDF2 algorithm.

NOTE: The module has two implementations of HMAC-256, one in openssl module and one in gcrypt module. We only actively use the HMAC-256 implementation in openssl. The one in gcrypt is latent.

All approved cryptographic functions are shown in Table 3.

Label	**Standard**	**Cryptographic Function**
AES	FIPS 197	Advanced Encryption Standard
AES-XTS	SP800-38E	XEX-based Tweaked-cookbook mode with ciphertext Stealing
AES-GCM	SP800-38D	Block Cipher Modes of Operation - Galois/Counter Mode
SHS	FIPS 180-4	Secure Hash Standard
HMAC	FIPS 198	Keyed-Hash Message Authentication Code
DRBG	SP800-90A	Deterministic Random Bit Generator
PBKDF2	SP800-132	Password Based Key Derivation Function

Table 4 – 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**
NDRNG	N/A	Intel RDRAND This provides 256 bits of Security Strength.
RSA (KW)	FIPS 140-2 IG D.9	RSA (key wrapping; key establishment methodology provides 128 bits of encryption strength)
Runtime Key	N/A	IG 1.23 “No Security claimed”

© 2021 HyTrust Inc.

		HyTrust proprietary fixed key used to obfuscate the code in storage using AES-XTS-256 (non-compliant).
Hardware Signature Key	N/A	IG 1.23 “No Security claimed” Hardware Signature Key, derived from the hardware information of the system, is proprietary to HyTrust and is used to obfuscate the master key in storage using AES-CBC-256 (non-compliant). This is considered plain text.

Table 5 – 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
U	Unrevoke

Table 6 – Legend for Type(s) of Access

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

Role		Service	Description	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 Admin Public Key Boot Passphrase Boot Encryption Key Entropy Input Seed Material DRBG Internal State PBKDF2 Internal State	G G G, O G I G U U U U
×		Bootstrap Object store	Bootstrap Object store and subsequent interactions	Object Store Key Admin Private Key Master Key	U U U
×		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.	Node Join Key Object Store Key Master Key Admin Public Key DRBG Internal State Node Join Passphrase PBKDF2 Internal State	G I, O G U U I U
×	×	Access of the object store during normal runtime	This includes generation of Data Encryption 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	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 access to symmetric keys resulting in data being inaccessible.	Object Store Key	U
×		Decommission Service - Zeroize	Remove all CSPs and key material from the system	Object Store Key Master Key Admin Private Key Admin Public Key DRBG Internal State Boot passphrase Boot Encryption Key Node Join Key Node Join Passphrase PBKDF2 Internal State Seed Material	Z Z Z Z Z Z Z Z Z Z Z
×		Self-Test	FIPS Post Test during system initialization	N/A	N/A
×		FIPS Status	FIPS Error Mode indication on the login screen	N/A	N/A

Table 7 – 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.

© 2021 HyTrust Inc.

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

Table 8 – 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:

- Centos 7.7 on VMware vSphere Hypervisor (ESXi) 6.7.0u3 running on Dell PowerEdge R220 with Intel® Xeon® CPU E3-1241v3 @ 3.50GHz (single-user mode)

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

Full and restricted support is not enabled by default and should remain disabled while operating the product in FIPS mode.

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 9 - Mitigation of Other Attacks

Appendix A

Following is a list of the cryptographic module CSPs:

1. Object Store Key:

© 2021 HyTrust Inc.

Description	AES-XTS with 256 bit key; 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	Generated on the first node. And wrapped using AES-GCM with the Node Join Key.
Output	Encrypted with Master Key and Node join key
Destruction	Powercycle enforced by the software module as part of the decommission service- gets rid of RAM
Decommission	zeros out everything

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	Master Key is wrapped with the following keys and the respective wrapped copies are stored on the disk: ● Hardware Signature Key – this is considered plain text. ● RSA 4096 bits Admin public key ● Boot Encryption Key Plaintext in RAM
Entry	N/A
Output	N/A
Destruction	Powercycle enforced by the software module as part of the decommission service- gets rid of RAM
Decommission	zeros out everything

3. Admin Private Key:

Description	RSA 4096 private key used to decrypt the Master Key
Generation	via output of SP800-90A DRBG as per SP 800-133 Section 5. The module supports the PKCS#1-v1.5 padding scheme and is allowed as per IG D.9
Storage	Split share in plaintext in RAM; full key is also plaintext in RAM
Entry	Plain text via Shamir Secret Sharing

Output	Plain text via Shamir Secret Sharing
Destruction	Powercycle enforced by the software module as part of the decommission service- gets rid of RAM
Decommission	zeros out everything

4. Node Join Passphrase:

Description	Used for Node join , Password (Policy will recommend minimum of 20 characters). Currently the module checks for a minimum of 16 characters, and truncates to 16 for interoperability with legacy systems.
Generation	N/A – Generated outside of the module and input into SP800-132 PBKDF2
Storage	plaintext in RAM
Entry	plaintext
Output	N/A
Destruction	Powercycle enforced by the software module as part of the decommission service- gets rid of RAM
Decommission	zeros out everything

5. Node Join Key:

Description	derived from passphrase using PBKDF2 HMAC-SHA256, used to AES-GCM 256 wrap the Object Store Key
Generation	PBKDF2 with HMAC-SHA256, salt 64 bytes from SP800-90A DRBG, 1 million iterations
Storage	plaintext in RAM
Entry	N/A
Output	N/A
Destruction	Actively overwritten with zeros immediately after use.
Decommission	zeros out everything

6. Entropy Input: Intel RDRAND

Description	String of bits obtained from Intel RDRAND, collecting 8 bytes at a time until the module collects 48 bytes. OPENSSL source:: crypto/rand/rand_lib.c -> hytrust_fips_drbg_get_entropy() ->ht_get_random_bytes
Generation	NDRNG (OPENSSL_ia32_rdrand)
Storage	plaintext in RAM
Entry	N/A
Output	N/A
Destruction	Powercycle - gets rid of RAM
Decommission	zeros out everything

7. Seed Material

Description	Constructed during CTR DRBG instantiate and it is the concatenation of entropy input, nonce and personalization string for the combined total of 1024 bits (encrypt=384, nonce=384, personalization string=256).
Generation	SP 800-90A DRBG
Storage	plaintext in RAM
Entry	N/A
Output	N/A
Destruction	Powercycle - gets rid of RAM
Decommission	zeros out everything

8. DRBG Internal State

Description	Internal State of SP800-90A CTR_DRBG (Key=256 bits & V=128 bits) as specified in IG 14.5
Generation	via SP 800-90A DRBG
Storage	plaintext in RAM
Entry	N/A
Output	N/A

© 2021 HyTrust Inc.

Destruction	Powercycle - gets rid of RAM
Decommission	zeros out everything

9. Boot Passphrase

Description	Input into SP800-132 PBKDF-2
Generation	N/A; Provided by Admin
Storage	Temporarily in RAM for generating Boot Encryption Key Size: Password (Policy will recommend minimum of 20 characters). Currently the module checks for a minimum of 12 characters.
Entry	N/A
Output	N/A
Destruction	Powercycle - gets rid of RAM
Decommission	zeros out everything

10. PBKDF2 Internal State

Description	Internal state of the derivation function using HMAC/SHA256 with 64-bytes salt and 1M iterations.
Generation	PBKDF2 with HMAC-SHA256 (SP800-132) Salt: 64 bytes - randomly generated using SP800-90A DRBG, Iteration: 1048576 (1 Million)
Storage	Temporarily in RAM for wrapping / unwrapping Master Key Key Wrapping: AES-GCM (SP800-38D)
Entry	N/A
Output	N/A
Destruction	Powercycle - gets rid of RAM
Decommission	zeros out everything

11. Boot Encryption Key

Description	256-bits key derived from the Boot Passphrase and a random IV of 96-bits.
Generation	PBKDF2 with HMAC-SHA256 (SP800-132) Salt: 64 bytes - randomly generated using SP800-90A DRBG, Iteration: 1048576 (1 Million)
Storage	Temporarily in RAM for wrapping / unwrapping Master Key Key Wrapping: AES-GCM (SP800-38D)
Entry	N/A
Output	N/A
Destruction	Actively overwritten with zeros immediately after use
Decommission	zeros out everything

Following is a list of the cryptographic module public keys:

1. Admin Public Key:

Description	RSA 4096 public key used to encrypt the Master Key
Generation	via output of SP 800-90A DRBG as per SP800-133 Section 5. The module supports the PKCS#1-v1.5 padding scheme and is allowed as per IG D.9.
Storage	plaintext in RAM
Entry	N/A
Output	N/A
Destruction	Power cycle enforced by the software module as part of the decommission service- gets rid of RAM
Decommission	zeros out everything