Fornetix® Key Orchestration™

FIPS 140-2 Level 2 Security Policy for Hardware Part Number KO-2000 Firmware Module Version 2.2-FIPS Non-Proprietary

Publication Date – Jun 11, 2020

NOTICE

Fornetix LLC
5123 Pegasus Ct., Suite X
Frederick, MD 20714
https://www.fornetix.com

The materials provided in this Key Orchestration™ FIPS 140-2 Level 2 Security Policy for KO-2000, which includes electronically distributed materials, (hereinafter referred to as the "Documentation") is for informational purposes only. The information within this document is non-proprietary and freely distributable. Reproduction is only authorized with the inclusion of this copyright notice, and provided that this document is copied in its entirety, without any modification to any of its content.

The use of any software product referenced in the Documentation is governed by the applicable license agreement and such license agreement is not modified in any way by this Notice.

Provided with "Restricted Rights." Use, duplication, or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b)(3), as applicable, or their successors.

Fornetix™ and Key Orchestration™ are trademarks of Fornetix IP LLC. All other trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

Table of Contents

1 Revision History

Table 1: Revision History

Revision/Date		Description Of Change
6/3/2019		Initial Draft for Module Version 2.2-FIPS
9/27/2019		Algorithm Certificate Update
10/3/2019		Review comments
6/11/2020		CMVP comments

2 Introduction

This document sets forth the Security Policy for the Key Orchestration™ Module to conform to FIPS 140-2 Level 2 Security Requirements. This Security Policy details how the Module meets the security requirements of FIPS 140-2 when run in an approved mode of operation.

Additional information on Key Orchestration is available from the Fornetix web site:
http://www.fornetix.com

“Key Orchestration Module”, “Module”, “KO Appliance”, “KO appliance”, and “appliance” are used throughout the document to refer to the Fornetix® Key Orchestration™ module.

3 Overview

Key Orchestration™ provides a means to automate and optimize encryption key management services and aligns encryption key management functions with other components of enterprise management and monitoring to operationalize encryption as a service. It provides a framework, a brokering relationship, between entities that generate keys and entities that require keys, and the business process which requires the transaction in the first place. Focus is placed on interoperability and standards compliance within the encryption management space.

Key Orchestration™ provides a technical bridge in solutions where there are external partners involved and a standards-based mechanism has value in facilitating encryption key distribution across disparate communications platforms and other applications. Key Orchestration™ leverages Key Management Interoperability Protocol (KMIP) as a means of structured data exchange between enabled system components. Using a standards-based approach for key management allows for integrating components of disparate subsystems that leverage KMIP enabled infrastructure.

4 Module Specification

The appliance to be included will be the KO-2000 rackmount server.

- The KO-2000 is the 2U version of the appliance.
- Red Hat Enterprise Linux Server 6.9 is being used.

The Module is considered a multi-chip standalone hardware module, intended to meet FIPS Level 2 compliance. When a KO appliance is installed, it must be placed into FIPS mode in order to meet this compliance. For instructions on placing the KO appliance into FIPS mode, please see the KO Appliance Configuration Guide, Chapter 6.1, FIPS Utilities.

The cryptographic boundary of the appliance is the physical perimeter of the actual box which executes the module. The array of hard drives on the front of the appliance are considered inside the cryptographic boundary and are not field replaceable; Fornetix technical support must be onsite to replace failed drives. Power supplies are field replaceable and are outside the boundary. Also, the empty removable disk drive bays on the rear of the chassis are outside the cryptographic boundary.

The module uses the embedded FIPS 140-2 validated module Red Hat Enterprise Linux 6 OpenSSL Module (Cryptographic Module Validation Program Certificate #2441).

The following table shows the security level for each of the eleven sections of the validation.

Table 2: Module Security Level Specification

Security Requirements Section	FIPS 140-2 Security Level
Cryptographic Module Specification	Level 2
Module Ports and Interfaces	Level 2
Roles, Services, and Authentication	Level 3
Finite State Model	Level 2
Physical Security	Level 2
Operational Environment	N/A
Cryptographic Key Management	Level 2
EMI/EMC	Level 2
Self-Tests	Level 2
Design Assurance	Level 2
Mitigation of Other Attacks	N/A

4.1 Description of the Approved Modes

When a KO appliance is operating in FIPS mode, this status will be displayed in the administrative menu, and can be confirmed by operators in the Server Administrator role. When FIPS mode is operational, the Modules are invoked into FIPS Approved operational mode at initialization time, and the Module automatically utilizes the embedded Red Hat Enterprise Linux 6 OpenSSL Module's FIPS Approved Mode.

The Modules verify the integrity of the runtime executable using a HMAC-SHA-256 digest computed at build time. If the digests matched, the power-up self-test is then performed. If the power-up self-test is successful, the Modules are initialized and are in FIPS Approved mode.

The KO appliance supports the following FIPS 140-2 Approved algorithms in FIPS Approved mode.

Please note that due to running on a new operational environment, the Red Hat Enterprise Linux 6 OpenSSL Module's algorithms were retested for CAVP.

Table 3: Approved Algorithms

CAVP Cert	Algorithm	Standard	Mode/Method	Key Length, Curves or Moduli	Use
C1131[2]	AES	FIPS 197, SP 800-38A, SP 800-38C CCM, SP 800-38D GCM, SP 800-38E XTS	ECB, CBC, OFB, CFB 1, CFB 8, CFB 128, CTR, CCM, GCM, XTS[3]	128, 192 (except XTS), 256	Data Encryption / Decryption
C1131	RSA	FIPS 186-4 Appendix B.3.3		2048, 3072	Key Generation
C1131	RSA	FIPS 186-4	SHA-256, SHA-384, SHA-512	2048, 3072	X9.31 Signature Generation
C1131	RSA	FIPS 186-4	SHA-1, SHA-256, SHA-384, SHA-512	1024, 2048, 3072	X9.31 Signature Verification
C1131	RSA	FIPS 186-4	SHA-224, SHA-256, SHA-384, SHA-512	2048, 3072	PKCS #1 v1.5 and PSS Signature Generation
C1131	RSA	FIPS 186-4	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	1024, 2048, 3072	PKCS #1 v1.5 and PSS Signature Verification
C1131	DRBG	SP 800-90A	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512		HMAC-Based Deterministic Random Bit Generator[1]
C1131	SHS	FIPS 180-4	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512		Hashing
C1131	HMAC	FIPS 198-1	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	At least 112 bits HMAC Key	Message Integrity

[1] Counter DRBG, and Hash DRBG were CAVP tested but are not used by this module.
[2] All C1131 algorithms are implemented within the embedded Red Hat module.
[3] ECB, OFB, CFB 1, CFB 8, CFB 128, CTR, CCM, GMAC, and XTS were tested but not used by this module.

CAVP Cert	Algorithm	Standard	Mode/Method	Key Length, Curves or Moduli	Use
C1131	CVL Partial ECDH	SP 800-56A	ECC	Curve: B-233, B-283, B-409, B-571, K-233, K-283, K-409, K-571, P-224, P-256, P-384, P-521	CAVP tested but not used by this module
C1131	CVL Key Derivation in TLS v1.0, v1.1 and v1.2[1]	SP 800-135rev1			Key Derivation
Vendor Affirmed	CKG	SP 800-133r1			Key Generation
C1150	CVL Key Derivation in SSHv2[1]	SP 800-135rev1			Key Derivation
AES C1131	KTS	SP 800-38F		256 bit	Cluster Communication
AES C1131 & HMAC C1131	KTS	SP 800-38F		AES 256-bit & HMAC 512-bit	Key transport through TLS session
AES C1131 & HMAC C1131	KTS	SP 800-38F		AES 128, 192, 256-bit & HMAC 512-bit	Key transport through SSH session

Note: KO Appliances are compatible with TLS v 1.2 with acceptable GCM cipher suites from SP 800-52 Rev 1, Section 3.3.1. As stated in Sections 7.4.1.1 and 7.4.1.2 of RFC 5246 for the TLS v 1.2 protocol, when the nonce_explicit portion of the IV has exhausted the maximum number of possible values for a given session key, a handshake to establish a new encryption key is triggered. 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. The TLS AES-GCM nonce is derived from the sequence number for initial record transmitted as suggested by the TLS RFCs. The normal packet size has ~1400 bytes of payload per nonce. Every network packet has a new nonce incremented as recommended by TLS RFC for transmission.

1. No parts of this protocol, other than the KDF, have been tested by the CAVP and CMVP

The Modules support the following non-Approved algorithms but allowed in FIPS Approved mode:

Table 4: Non-Approved Algorithms (Allowed)

Algorithm	Caveat	Use
RSA Key Wrapping	Provides between 112 and 150 bits of encryption strength.	Key Establishment
Diffie-Hellman with public key size 2048 bits or larger and private key size 224 bits or 256 bits	Provides 112 bits of encryption strength	Key Establishment

NDRNG		Seeding for the DRBG

The Modules support the following non-FIPS 140-2 Approved algorithms, which are not used in the FIPS Approved mode.

Table 5: Non-Approved Algorithms (Not Allowed)

Algorithm	Usage
RSA (encrypt, decrypt) with key size smaller than 2048 bits	Key wrapping
RSA with key sizes not listed in Table 3	Sign, verify, and key generation
Diffie-Hellman with key sizes not listed in Table 3	Key agreement and establishment
ANSI X9.31 RNG (with AES-128 core)	Random number generation
J-PAKE	Password Authenticated Key Exchange
MD2	Hash function
MD4	Hash function
MD5	Hash function
MDC2	Hash function
RIPEMD	Hash function
Whirlpool	Hash function

5 Module Ports and Interfaces

The following table lists the logical and physical ports and interfaces to the Module.

Table 6: Physical Ports

Port	Description
MGMT Port	Currently unused and reserved for future use.
MGMT Port LEDs	Currently unused and reserved for future use.
RJ-45 Ethernet Ports (6)	Connects to the network and provides services to network attached clients.
RJ-45 Ethernet Ports LEDs (6)	ACT LED indicates network link status. LNK LED indicates network activity.
SATA Drive LEDs	Indicates activity and error state of the SATA drives.
CONSOLE Port	Serial port which connects to a local terminal for initialization of the module and limited local management capabilities.
Video Output	Console video output for external monitor
Front Panel USB 1	Keyboard input
USB 1	Keyboard input
USB 2	Keyboard input
USB 3	Keyboard input
Left Power Interface	PCI Compact Power Adapter for supporting power supply redundancy and high availability.
Left Power Interface LED	Power LED indicates status of removable power supply.
Right Power Interface	PCI Compact Power Adapter for supporting power supply redundancy and high availability.
Right Power Interface LED	Power LED indicates status of removable power supply.

Table 7: Logical Port Mappings

Logical Interface	Physical Interface Mapping
Data Input Interface	RJ-45 Ethernet Ports (6)
Data Output Interface	RJ-45 Ethernet Ports (6)
Control Input Interface	RJ-45 Ethernet Ports (6) CONSOLE Port USB Ports
Status Output Interface	RJ-45 Ethernet Ports (6) RJ-45 Ethernet Ports (6) LEDs CONSOLE Port Video Output Left Power Interface LED Right Power Interface LED

Power Interface	Left Power Connector Right Power Connector

6 Roles, Services, and Authentication

6.1 Roles

The Key Orchestration module supports identity-based authentication for all roles. Associated FIPS roles are Crypto Officer, User, and Factory Control.

Crypto Officer - Responsible for management activities and multi-user key management functions associated with the module.

User - a client program (hereafter referred to as KO Client) that connects to the appliance that may receive or provide key material. Authenticates to the appliance using mutual TLS authentication.

Factory Control - Responsible for performing service on the Key Orchestration module. This is not an operator-accessible role. Fornetix Professional Services must be engaged to perform these services, which are considered outside the purview of FIPS 140-2.

6.1.1 Key Orchestration Roles

- **System Administrator** - This role is concerned with the management of the KO appliance. This includes initial configuration, enabling FIPS compliance mode, and managing various server configuration values.
- **System Recovery Administrator** – This role is concerned with password recovery for the System Administrator role in the event that password is lost.
- **Auditor** - This role audits the creation, usage, and disposal of encryption keys and certificates created by the Key Administrator.
- **Key Administrator** - This role creates and manages new encryption keys and certificates.
- **Policy Administrator** - This role defines policy which will limit which objects can be created, attributes which are required, etc.
- **Server Administrator** - This role creates and manages users and groups within the system.
- **KO Client** - This role is defined as a consumer of the encryption keys and certificates created by the Key Administrator. A client is also able to register its own key for storage within the KO appliance, and can create new key material for itself.

6.1.2 Key Orchestration Roles Mapped to FIPS Roles

Table 8: KO Roles Mapped to FIPS Roles

Fornetix Role	FIPS Mapped Role	Authentication Data
System Administrator	N/A	The role is granted access to the administrative menu interface after providing proper Username and Password.
System Recovery Administrator	N/A	The role is granted access to the password recovery menu interface after providing proper Username and Password.

Fornetix Role	FIPS Mapped Role	Authentication Data
Auditor	N/A	The role is granted access to the Key Orchestration user interface after providing proper Username and Password.
Key Administrator	N/A	The role is granted access to the Key Orchestration user interface after providing proper Username and Password.
Policy Administrator	N/A	The role is granted access to the Key Orchestration user interface after providing proper Username and Password.
Server Administrator	Crypto Officer	The role is granted access to the Key Orchestration user interface after providing proper Username and Password.
KO Client (someone who connects to the appliance)	User	The role authenticates to the Key Orchestration appliance through a signed X.509 Digital Certificate.

6.2 Services

The following tables show the authorized services available for each role (Crypto Officer/User) within the Key Orchestration module. Each service requires authentication to the module. The following flags are used in the 'CSPs and Access Type' column to denote access:

- R – Read: The CSP is read within the cryptographic boundary.
- W – Write: The CSP is written within the cryptographic boundary.
- O – Output: The CSP crosses the cryptographic boundary, from inside to outside.
- I – Input: The CSP crosses the cryptographic boundary, from outside to inside.
- Z – Zeroize: The CSP is zeroized.
- X – Execute: The CSP is used for a cryptographic operation.

6.2.1 System Administrator

Table 9: System Administrator Authorized Services

Service	Description	CSPs and Access Type
Access Appliance (Console)	Authentication via console	Passwords (R/I)

Service	Description	CSPs and Access Type
Access Appliance (SSH)	Authentication via SSH	Passwords (R/I) SSH Krsa public (O) SSH Krsa private (X) SSH DH public param (R/I/W/X) SSH DH private param (W/X) SSH Ks (W/X) SSH Khmac (W/X) DRBG (X)
First boot, initial configuration	System configuration after initial setup or zeroization	CA (W) BEK (W) HTTPS (W) SSH Krsa public (W) SSH Krsa private (W) TLS Krsa public (W) TLS Krsa private (W) DRBG (X)
Change administrator password	Change password for the System Administrator account	Passwords (W/I)
Change network settings	Display/edit network settings	None
Change date/time settings	Update time server configuration	None
Manage syslog configuration[1]	Display/edit remote syslog destinations	None
Manage SNMP configuration[2]	Display/edit SNMP settings (non-FIPS only)	None
FIPS mode operations	Enable FIPS mode, perform self-tests	HMAC-SHA-256 Module Integrity Keys (R) HMAC-SHA-512 Kernel Integrity Keys (R)
FIPS Show Status	Displays current FIPS Status	None

Service	Description	CSPs and Access Type
FIPS Zeroize	Return the system to factory state	BEK (Z) CA (Z) CEK (Z) HTTPS (Z) Passwords (Z) SSH Krsa public (Z) SSH Krsa private (Z) TLS Krsa public (Z) TLS Krsa private (Z) DRBG (Z) UGK (Z) UGC (Z) LDAPUP (Z) LDAPC (Z) BPub (Z) BPriv (Z) BCA (Z) EBSSH (Z)
Chassis Management	Reboot or power down the system	None
Disk Management	Display disk status, enable/disable alarm, identify drive, rebuild a replaced disk	None
KO Policy Engine Control	Display/edit the Policy Engine status	None
Restore Root Policy	Restore Root Policy to factory defaults	None
KO Positional Security	Display/edit the Positional Security status	None
KO Brokering	Display/edit a brokered server configuration	BPub (W/I) BPriv (W/I) BCA (W/I)
KO Clustering	Configure cluster operations	Passwords (R/I) HTTPS (R/O) CEK (R/W/O/I) BEK (R/W/O/I) CA (R/W/O/I) DRBG (X) BPub (R/W/O/I) BPriv (R/W/O/I) BCA (R/W/O/I)
Manage External Authentication (LDAP)[3]	Display/edit/diagnose configuration for external authentication using LDAP	LDAPUP (R/W/X/I) LDAPC (R/W/X/I/O)

Service	Description	CSPs and Access Type
Manage KO services	Display, stop, or start the KO processes	CA (R) CEK (R) HTTPS (R)
Manage Licensing	Display or upload license information	Passwords (R/I) SSH Krsa public (O) SSH Krsa private (X) SSH DH public param (R/I/W/X) SSH DH private param (W/X) SSH Ks (W/X) SSH Khmac (W/X) DRBG (X) UDK (X)
Initialize the Backup system	Prepare the system for performing backups	None
Perform backups	Create a backup of the system. This includes manually initiated backups, and backups initiated by schedules.	BEK (R/X) CA (R) HTTPS (R) Passwords (R) BPub (R) BPriv (R) BCA (R) UGK (R) UGC (R) LDAPUP (R) LDAPC (R)
Restore a backup	Restore the system from a backup	BEK (X/W) CA (W) HTTPS (W) Passwords (W) BPub (W) BPriv (W) BCA (W) UGK (W) UGC (W) LDAPUP (W) LDAPC (W)
Manage Backup Schedules	Display/edit scheduled backups	None
Manage Backup Retention Policies	Display/edit the retention policy for backup files	None

Service	Description	CSPs and Access Type
Configure Export Location	Display/edit connection to an external backup server	EBUP (I/X/Z) EBSSH (I/W/X) SSH Krsa public (O) SSH Krsa private (X) SSH DH public param (R/I/W/X) SSH DH private param (W/X) SSH Ks (W/X) SSH Khmac (W/X) DRBG (X)
Export backup files	Export an existing backup file to the configured Export Location	EBSSH (X) SSH Krsa public (O) SSH Krsa private (X) SSH DH public param (R/I/W/X) SSH DH private param (W/X) SSH Ks (W/X) SSH Khmac (W/X) DRBG (X) BEK (O) CA (O) HTTPS (O) Passwords (O) BPub (O) BPriv (O) BCA (O) UGK (O) UGC (O) LDAPUP (O) LDAPC (O)
Download/Upload backup files	Download or upload existing backup files to locations other than the configured Export Location	Passwords (R/I/O) SSH Krsa public (O) SSH Krsa private (X) SSH DH public param (R/I/W/X) SSH DH private param (W/X) SSH Ks (W/X) SSH Khmac (W/X) DRBG (X) BEK (I/O) CA (I/O) HTTPS (I/O) BPub (I/O) BPriv (I/O) BCA (I/O) UGK (I/O) UGC (I/O) LDAPUP (I/O)

Service	Description	CSPs and Access Type
		LDAPC (I/O)
View audit logs	Review audit logs, only available within SSH session	SSH Ks (W/X) SSH Khmac (W/X) DRBG (X)
Download audit logs (for customer use)	Download a copy of the audit logs for review	Passwords (R/I) SSH Krsa public (O) SSH Krsa private (X) SSH DH public param (R/I/W/X) SSH DH private param (W/X) SSH Ks (W/X) SSH Khmac (W/X) DRBG (X)
Download audit logs (for Fornetix support use)	Download a copy of the audit logs for review by Fornetix Customer Support	FAEK (X) Passwords (R/I) SSH Krsa public (O) SSH Krsa private (X) SSH DH public param (R/I/W/X) SSH DH private param (W/X) SSH Ks (W/X) SSH Khmac (W/X) DRBG (X)

[1] The syslog configuration allows configuration of external syslog servers to receive the filtered CEF (Common Event Format) log messages. These messages contain status only, no sensitive data or key material is output. These connections do not use encrypted communication, so no CSPs are referenced.
[2] SNMP is a non-FIPS service and is disabled when operating in FIPS mode.
[3] External authentication via LDAP occurs over default TLS connections configured on the module using the provided credentials.

6.2.2 System Recovery Administrator

Table 10: System Recovery Administrator Authorized Services

Service	Description	CSPs and Access Type
Access Appliance (Console)	Authentication via console	Passwords (R/I)
Reset the ko_admin password	Change password for the System Administrator account	Passwords (W/I)
Reset the ko_recovery password	Change password for the System Recovery Administrator account	Passwords (W/I)

6.2.3 Auditor

Table 11: Auditor Authorized Services

Service	Description	CSPs and Access Type
Access REST API (Local Authentication)	Authentication to the REST API	Passwords (R/I) HTTPS (R/O) DRBG (X)
Access REST API (External LDAP Authentication)	Authentication to the REST API	Passwords (I/O) LDAPUP (X) LDAPC (R/X) HTTPS (R/O) TLS Pre-MS (W/O) TLS MS (W) TLS Krsa public (R/O) TLS Krsa private (X) TLS Ks (X) TLS Khmac (X) DRBG (X)
Access Web UI (Local Authentication)	Authentication to the Web UI	Passwords (R/I) HTTPS (R/O) DRBG (X)
Access Web UI (External LDAP Authentication)	Authentication to the Web UI	Passwords (I/O) LDAPUP (X) LDAPC (R/X) HTTPS (R/O) TLS Pre-MS (W/O) TLS MS (W) TLS Krsa public (R/O) TLS Krsa private (X) TLS Ks (X) TLS Khmac (X) DRBG (X)
View Clients	View list of clients	UGC (R/O)
View Groups	View list of groups	None
View Jobs	View list of scheduled jobs	None
View Users	View user information for all users	None
Change password (self)	Change own password	Passwords (R/W/I)
View Managed Objects	View list of managed objects	None
View Nodes	View list of nodes	None

Node - View Associated Managed Objects	View managed objects associated with a specified node	None
Node - View Associated Policies	View policy associated with a specified node	None
View Reports - Managed Objects Expiration	Review reports of object expirations	None
View Reports - Transactions	Review reports for all transactions, failed transactions, and user transactions	None

6.2.4 Key Administrator

Table 12: Key Administrator Authorized Services

Service	Description	CSPs and Access Type
Access REST API (Local Authentication)	Authentication to the REST API	Passwords (R/I) HTTPS (R/O) DRBG (X)
Access REST API (External LDAP Authentication)	Authentication to the REST API	Passwords (I/O) LDAPUP (X) LDAPC (R/X) HTTPS (R/O) TLS Pre-MS (W/O) TLS MS (W) TLS Krsa public (R/O) TLS Krsa private (X) TLS Ks (X) TLS Khmac (X) DRBG (X)
Access Web UI (Local Authentication)	Authentication to the Web UI	Passwords (R/I) HTTPS (R/O) DRBG (X)
Access Web UI (External LDAP Authentication)	Authentication to the Web UI	Passwords (I/O) LDAPUP (X) LDAPC (R/X) HTTPS (R/O) TLS Pre-MS (W/O) TLS MS (W) TLS Krsa public (R/O) TLS Krsa private (X) TLS Ks (X) TLS Khmac (X) DRBG (X)

Service	Description	CSPs and Access Type
View Clients	View list of clients	UGK (R/O) UGC (R/O)
Clients - Associate Managed Objects	Associate managed objects with a specified client	None
View Groups	View list of groups	None
Groups - Associate Managed Objects	Associate managed objects with a specified group	None
View Jobs	View list of scheduled jobs	None
Execute Jobs	Execution of scheduled jobs, or run a job on demand	UGK (R/W/X/O/I/Z) UGC (R/W/X/O/I/Z) BPub (R/O) BPriv (X) BCA (R)
View Users	View user information for all users	None
Change password (self)	Change own password	Passwords (R/W/I)
View Managed Objects	View list of managed objects	None
View Managed Object Details	View attributes of a specified managed object	UGK (R/O) UGC (R/O)
Manage Managed Objects	Create, update, and delete managed objects	UGK (R/W/O/I/Z) UGC (R/W/O/I/Z) CA (R) DRBG (X) BPub (R/O) BPriv (X) BCA (R)
View Nodes	View list of nodes	None
Node - View Associated Managed Objects	View managed objects associated with a specified node	None
Node - Associate Managed Objects	Associate managed objects with a specified node	None
Node - View Associated Policies	View policy associated with a specified node	None
View Reports - Managed Objects Expiration	Review reports of object expirations	None
View Reports - Transactions	Review reports for all transactions, failed transactions, and user transactions	None

6.2.5 Policy Administrator

Table 13: Policy Administrator Authorized Services

Service	Description	CSPs and Access Type
Access REST API (Local Authentication)	Authentication to the REST API	Passwords (R/I)

Service	Description	CSPs and Access Type
		HTTPS (R/O) DRBG (X)
Access REST API (External LDAP Authentication)	Authentication to the REST API	Passwords (I/O) LDAPUP (X) LDAPC (R/X) HTTPS (R/O) TLS Pre-MS (W/O) TLS MS (W) TLS Krsa public (R/O) TLS Krsa private (X) TLS Ks (X) TLS Khmac (X) DRBG (X)
Access Web UI (Local Authentication)	Authentication to the Web UI	Passwords (R/I) HTTPS (R/O) DRBG (X)
Access Web UI (External LDAP Authentication)	Authentication to the Web UI	Passwords (I/O) LDAPUP (X) LDAPC (R/X) HTTPS (R/O) TLS Pre-MS (W/O) TLS MS (W) TLS Krsa public (R/O) TLS Krsa private (X) TLS Ks (X) TLS Khmac (X) DRBG (X)
View Clients	View list of clients	UGC (R/O)
View Groups	View list of groups	None
Groups - Create Policy	Create policy for a specified group	None
View Jobs	View list of scheduled jobs	None
View Users	View user information for all users	None
Change password (self)	Change own password	Passwords (R/W/I)
View Managed Objects	View list of managed objects	None
View Nodes	View list of nodes	None
Manage Nodes	Create, update, and delete nodes	None
Node - Create Clients	Create clients for specified nodes	None
Node - Associate Nodes	Associate other nodes as children to specified nodes	None
Node - View Associated Policies	View policy associated with a specified node	None

Service	Description	CSPs and Access Type
Node - Create Policies	Create policy for a specified node	None
View Reports - Transactions	Review reports for all transactions, failed transactions, and user transactions	None

6.2.6 Server Administrator

Table 14: Server Administrator Authorized Services

Service	Description	CSPs and Access Type
Access REST API (Local Authentication)	Authentication to the REST API	Passwords (R/I) HTTPS (R/O) DRBG (X)
Access REST API (External LDAP Authentication)	Authentication to the REST API	Passwords (I/O) LDAPUP (X) LDAPC (R/X) HTTPS (R/O) TLS Pre-MS (W/O) TLS MS (W) TLS Krsa public (R/O) TLS Krsa private (X) TLS Ks (X) TLS Khmac (X) DRBG (X)
Access Web UI (Local Authentication)	Authentication to the Web UI	Passwords (R/I) HTTPS (R/O) DRBG (X)
Access Web UI (External LDAP Authentication)	Authentication to the Web UI	Passwords (I/O) LDAPUP (X) LDAPC (R/X) HTTPS (R/O) TLS Pre-MS (W/O) TLS MS (W) TLS Krsa public (R/O) TLS Krsa private (X) TLS Ks (X) TLS Khmac (X) DRBG (X)
View Clients	View list of clients	UGK (R/O) UGC (R/O)
Manage Clients	Create, update, and delete clients	CA (R) UGK (R/W/O/I/Z) UGC (R/W/O/I/Z)

Service	Description	CSPs and Access Type
		DRBG (X)
Manage Compositions	Create, update, and delete stored compositions	None
View Groups	View list of groups	None
Manage Groups	Create, update, and delete groups	None
Groups - Associate Managed Objects	Associate managed objects with a specified group	None
Groups - Create Policy	Create policy for a specified group	None
View Jobs	View list of scheduled jobs	None
Create Jobs	Create scheduled jobs	None
Execute Jobs	Execution of scheduled jobs, or run a job on demand	UGK (R/W/X/O/I/Z) UGC (R/W/X/O/I/Z) BPub (R/O) BPriv (X) BCA (R)
Modify Jobs	Modify scheduled jobs	None
Delete Jobs	Deleted scheduled jobs	None
View Users	View user information for all users	None
Manage Users	Create, update and delete users	Passwords (W/I/Z) UGK (W/Z) UGC (W/Z) DRBG (X)
Change password (self)	Change own password	Passwords (R/W/I)
Reset User Password	Change another user's password	Passwords (W/I)
View Managed Objects	View list of managed objects	None
View Managed Object Details	View attributes of a specified managed object	UGK (R/O) UGC (R/O)
View Nodes	View list of nodes	None
Manage Nodes	Create, update, and delete nodes	None
Node - Associate Clients	Associate clients with specified nodes	None
Node - Associate Nodes	Associate other nodes as children to specified nodes	None
Node - View Associated Managed Objects	View managed objects associated with a specified node	None
Node - View Associated Policies	View policy associated with a specified node	None
Node - Create Policies	Create policy for a specified node	None
View Reports - Transactions	Review reports for all transactions, failed transactions, and user transactions	None

6.2.7 KO Client

Table 15: KO Client Authorized Services

Service	Description	CSPs and Access Type
Establish KMIP Connection	Establishes a mutual TLS connection on port 5696 for KMIP communication	CA (R) TLS Pre-MS (W/I/O) TLS MS (W) TLS Krsa public (R/O) TLS Krsa private (X) TLS Ks (X) TLS Khmac (X) DRBG (X)
Clients - Associate Managed Objects	Associate managed objects with a specified client[1]	None
View Managed Objects	View list of managed objects	None
View Managed Object Details	View attributes of a specified managed object	UGK (R/O) UGC (R/O)
Manage Managed Objects	Create, update, and delete managed objects	UGK (R/W/O/I/Z) UGC (R/W/O/I/Z) CA (R) DRBG (X) BPub (R/O) BPriv (X) BCA (R)
Node - View Associated Managed Objects	View managed objects associated with a specified node	None
Perform Cryptographic Operations with Managed Objects	Perform KMIP encrypt/decrypt operations using a specified managed object	UGK (X) BPub (R/O) BPriv (X) BCA (R)

[1] While Positional Security is enabled (recommended), a KO Client has visibility only to managed objects associated with itself or its ancestors in the hierarchy. This includes the ability to associate a managed object with one if its ancestors.

6.3 Authentication

Authentication for the **KO Client** role is completed using certificates. Authentication for all other KO Roles (including **System Administrator**, **System Recovery Administrator**, **Auditor**, **Key Administrator**, **Policy Administrator**, and **Server Administrator)** is completed using username and password combinations.

Passwords
Passwords must be at least 10 characters in length and must contain:

- At least one uppercase letter: A-Z
- At least one lowercase letter: a-z
- At least one number: 0-9
- At least one special symbol: !@#$%^&*()?~

An account lockout feature is also implemented where the user account will be locked out after three (3) failed attempts at authentication via the HTTPS connection. Once locked, these accounts must be unlocked by a member of the Server Administrator role.

For the administrative menu interface used by the System Administrator role, the lockout is for 30 minutes after three (3) failed attempts at authentication. After the lockout has expired, this account will automatically unlock.

The System Recovery Administrator role does not have a lockout feature enforced.

There is no feedback of authentication data to the User that might serve to weaken the authentication mechanism.

Certificates
Certificates used for authentication are a minimum of RSA 3072, which provides an encryption strength of 128 bits.

By default, the KO appliance will allow 32 simultaneous incoming connections. This number is configurable via the administrative menu. Once a port has been opened by a client, it cannot be recycled for another connection for 60 seconds. Thus, only 32 attempts could be made within a 60 second timeframe.

There is no feedback of authentication data to the User that might serve to weaken the authentication mechanism.

Table 16: Authentication Permutations

Method	Specification	Attempts per Minute	Permutations	Probability of Random Success
Password – System Administrator Role	Minimum Length: 10 Maximum Length: Unlimited At least one uppercase letter: A-Z At least one lowercase letter: a-z At least one number: 0-9 At least one special symbol: !@#$%^&*()?~	Three attempts before user lockout for 30 minutes	Assumed a minimum password length of 10 characters, with the minimum requirements of one uppercase letter, one lowercase letter, one number, and one special character from the 12 allowed, and the remainder randomly chosen from the 74-character allowed set. Take the total amount of permutations available (74^{10}) and subtract combinations which only meet one, two, or three of the required character sets: 74^{10} - 26^{10} - 26^{10} - 10^{10} - 12^{10} - 52^{10} - 36^{10} - 38^{10} - 36^{10} - 38^{10} - 22^{10} - 62^{10} - 64^{10} - 48^{10} - 48^{10}, yields approximately 2.63e18 permutations.	2.63e18 permutations = one in 2400 quadrillion odds of guessing a password randomly. This is significantly lower probability than the one in 1,000,000 required by FIPS 140-2 for single attempts. And divided by the 3 possible attempts per minute = 1 in 800 quadrillion odd of guessing a password randomly in a minute. This is significantly lower probability than the one in 100,000 required by FIPS 140-2 per minute.
Password – System Recovery Administrator Role	Minimum Length: 10 Maximum Length: Unlimited At least one uppercase letter: A-Z At least one lowercase letter: a-z At least one number: 0-9 At least one special symbol: !@#$%^&*()?~	There is no lockout for this role. With only console login rights, the user is limited to how many characters they can enter via the console, which operates at 38400 baud. Translating to approximately 4800 bytes/sec, and assuming minimum password length, this would yield a conservative maximum of 480 attempts per second, or 28,800 per minute.	Assumed a minimum password length of 10 characters, with the minimum requirements of one uppercase letter, one lowercase letter, one number, and one special character from the 12 allowed, and the remainder randomly chosen from the 74-character allowed set. Take the total amount of permutations available (74^{10}) and subtract combinations which only meet one, two, or three of the required character sets: 74^{10} - 26^{10} - 26^{10} - 10^{10} - 12^{10} - 52^{10} - 36^{10} - 38^{10} - 36^{10} - 38^{10} - 22^{10} - 62^{10} - 64^{10} - 48^{10} - 48^{10}, yields approximately 2.63e18 permutations.	2.63e18 permutations = one in 2400 quadrillion odds of guessing a password randomly. This is significantly lower probability than the one in 1,000,000 required by FIPS 140-2 for single attempts. And divided by the 28,800 possible attempts per minute = 1 in 83 trillion odd of guessing a password randomly in a minute. This is significantly lower probability than the one in 100,000 required by FIPS 140-2 per minute.

Method	Specification	Attempts per Minute	Permutations	Probability of Random Success
Password - HTTPS and REST	Minimum Length: 10 Maximum Length: Unlimited At least one uppercase letter: A-Z At least one lowercase letter: a-z At least one number: 0-9 At least one special symbol: !@#$%^&*()?~	Three attempts before user lockout for 30 minutes	Assumed a minimum password length of 10 characters, with the minimum requirements of one uppercase letter, one lowercase letter, one number, and one special character from the 12 allowed, and the remainder randomly chosen from the 74-character allowed set. Take the total amount of permutations available (74^{10}) and subtract combinations which only meet one, two, or three of the required character sets: 74^{10} - 26^{10} - 26^{10} - 10^{10} - 12^{10} - 52^{10} - 36^{10} - 38^{10} - 36^{10} - 38^{10} - 22^{10} - 62^{10} - 64^{10} - 48^{10} - 48^{10}, yields approximately 2.63e18 permutations.	2.63e18 permutations = one in 2400 quadrillion odds of guessing a password randomly. This is significantly lower probability than the one in 1,000,000 required by FIPS 140-2 for single attempts. And divided by the 3 possible attempts per minute = 1 in 800 quadrillion odd of guessing a password randomly in a minute. This is significantly lower probability than the one in 100,000 required by FIPS 140-2 per minute.
Certificate	RSA 3072	32 attempts on available connections, which will then require one minute to recycle	Encryption strength of 128 bits, yielding 2^{128} permutations	2^{128} permutations = one in 3.40282E38 odd of using a matching certificate. This is significantly lower probability than the one in 1,000,000 required by FIPS 140-2 for single attempts. 2^{128} permutations / 32 attempts on available connections = one in 1.06338E37 odds of using a matching certificate randomly in a minute. This is significantly lower probability than the one in 100,000 required by FIPS 140-2 per minute.

6.4 Procedures to Initialize a Module to Comply with FIPS 140-2 Level 2

Log into the web UI as the default Server Administrator (admin) and assign a new password which meets password complexity requirements.

Log into the Appliance at the console as the System Recovery Administrator (ko_recovery) and assign a new password which meets password complexity requirements.

Place the KO Appliance into FIPS Mode:

1. Log into the Appliance as a System Administrator.
2. Enter "4" to manage the Key Orchestration Appliance Chassis and press **ENTER**.
3. Enter "2" to access FIPS Utilities and press **ENTER**.
4. Enter "2" to turn on FIPS Mode and press **ENTER**.
5. Confirm whether you wish to continue by entering **Yes/No**. ***Answer is case-sensitive.***
6. Enter first confirmation code **1-1A** and press **ENTER**.
7. Enter second confirmation code **1-1A-2B** and press **ENTER**.
8. Enter third confirmation code **1-1B-2B-3** and press **ENTER**.
9. Enter final confirmation code **000-FIPS-INIT-0** and press **ENTER**. ***Once final confirmation code is entered and process is initiated by pressing ENTER, initialization of FIPS mode begins and cannot be reversed.***

Note: Warning screen confirmation requires that a positive answer (Yes) be case-sensitive. All other entries will fail.

6.5 Verify the Module is in Level 2 FIPS Mode

To display the configuration mode for the server (Standard Mode, FIPS Mode):

1. Log into the Appliance as a System Administrator.
2. Enter "4" to manage the Key Orchestration Appliance Chassis and press **ENTER**.
3. Enter "2" to access FIPS Utilities and press **ENTER**.
4. Enter "1" to display the configuration mode of the server and press **ENTER**.

To verify that startup tests completed, and cryptographic services are online:

1. Log into the Appliance as a System Administrator.
2. Enter "6" to manage the Key Orchestration Processes and press **ENTER**.
3. Enter "1" to display the status of the cryptographic services and press **ENTER**.

To review log information for power up self-tests performed at system start:

1. Log into the Appliance as a System Administrator.
2. Enter "7" to access the Support section and press **ENTER**.
3. Enter "4" to access Logs and press **ENTER**.
4. Enter a selection to View, Tail, or Download a log and press **ENTER**.
5. Choose the System-Messages log and press **ENTER**.
6. Follow the on-screen instructions to view or download the log information.

6.6 Operating in level 2 FIPS mode

When operating in FIPS Mode, the KO Appliance will run using only crypto algorithms that are FIPS 140-2 compliant. Once FIPS Mode is activated, there is only a limited number of utilities available in the menu system, and only System Administrators have access to these utilities. In addition to showing FIPS status and turning on FIPS Mode, the following options are also available in FIPS Mode:

- Place Server in Self-Test Mode
- Zeroize FIPS Mode

6.6.1 Place Server in Self-Test Mode

To place the server into Self-Test Mode:

1. Log into the Appliance as a System Administrator.
2. Enter "4" to manage the Key Orchestration Appliance Chassis and press **ENTER**.
3. Enter "2" to access FIPS Utilities and press **ENTER**.

4. Enter "4" at the prompt and press **ENTER**.
5. The KO services are stopped. Press **ENTER** and FIPS self-tests are performed.
6. Press **ENTER** to restart the KO services.

6.6.2 Zeroize FIPS Mode

To Zeroize FIPS Mode:

1. Log into the Appliance as a System Administrator.
2. Enter "4" to manage the Key Orchestration Appliance Chassis and press **ENTER**.
3. Enter "2" to access FIPS Utilities and press **ENTER**.
4. Enter "6" at the prompt and press **ENTER**.
5. Enter first confirmation code 1-1A and press **ENTER**.
6. Enter second confirmation code 1-1A-2B and press **ENTER**.
7. Enter third confirmation code 1-1B-2B-3 and press **ENTER**.
8. Enter final confirmation code 000-DESTRUCT-0 and press **ENTER**.

7 Physical Security Mechanisms

As a Level 2 multi-chip standalone hardware module, the Key Orchestration Server has an opaque enclosure that is tamper evident. All of the module within the FIPS boundary are obscured with the use of a foam mesh to prevent visual inspection. Unused network interfaces are disabled.

USB ports are active but can only be used for keyboard input by customers for data entry to the administrative menu. Any USB storage devices attached to these ports are not accessible from the appliance and attempting to boot from USB has been explicitly disabled in the BIOS.

Factory applied, serial numbered, tamper evident seals are used to ensure that only authorized Fornetix customer support staff can access the module within the crypto boundary. Once the module has been configured to meet FIPS 140-2 Level 2 requirements, the module cannot be accessed without signs of tampering.

A locking front bezel is included with each Key Orchestration Server. The bezel is required to remain in place during normal operations to protect the front drive interfaces from unauthorized access and to block visibility of the drive backplane.

Tamper evident seals are applied between the front bezel and the chassis, on both the top and bottom of the appliance. In the event of a hard drive failure, a replacement hard drive must be authorized and obtained from Fornetix and must be installed by Fornetix customer support staff in order to maintain FIPS compliance and replacement of the tamper evident seals.

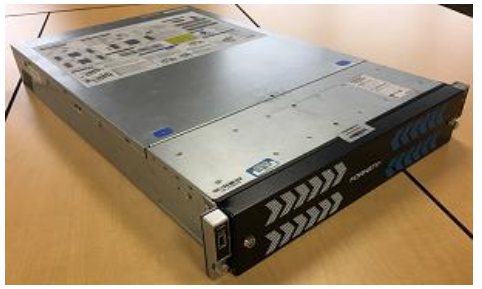

Image 1: KO-2000

Image 2: KO-2000 Locking Front Bezel

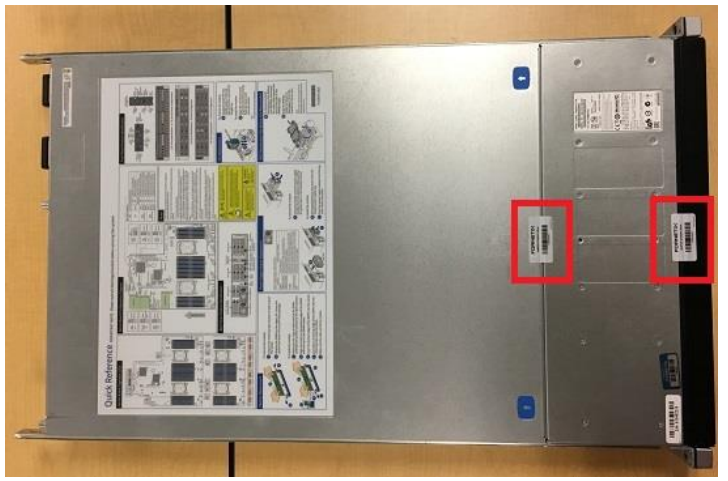

Image 3: KO-2000 with Tamper Evident Seals (Top)

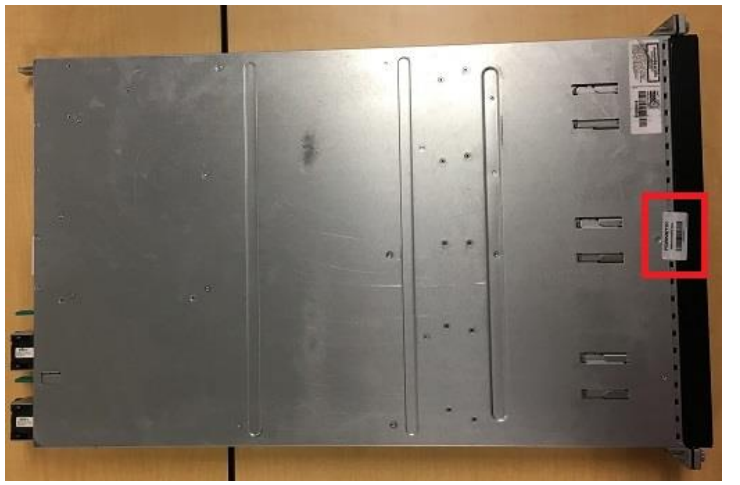

Image 4: KO-2000 with Tamper Evident Seal (Bottom)

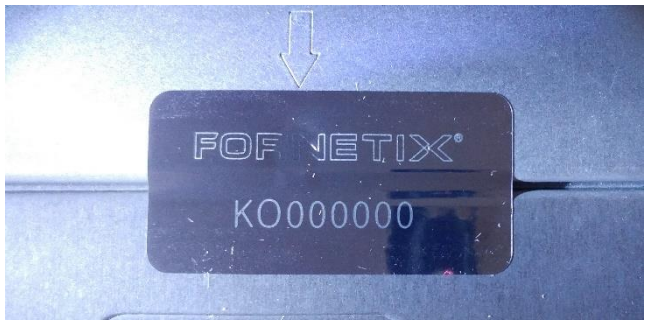

Image 5: Tamper Evident Seal

8 Operational Environment

The KO appliance uses Red Hat Enterprise Linux Server 6.9 as the operating system, with required operational modules pre-loaded. A custom shell is used as the administration menu and prevents users from performing operations outside of those defined in the administration menu. The menu is accessible only by a single named user. There is no capability for customers to perform manual adjustments, or to install unapproved software, scripts, etc.

Using the administration menu, System Administrators may apply authorized upgrade packages supplied by Fornetix Customer Support in order to load security updates, functionality corrections and improvements, and additional features (non-modifiable environment with firmware loading support). These upgrade packages are signed at the time of creation by Fornetix. Upon upload to the KO appliance, the signature is validated against the Upload Verification Keys (UVK) to ensure a valid signature. This information is presented to the user for review, and the operator may choose to apply the upgrade or cancel. If the operator chooses to apply the signed upgrade, the Upload Decryption Key (UDK) is then used to decrypt the upgrade package. Only after successful decryption will the upgrade package begin processing. If a non-validated firmware version is applied to the Appliance, the Appliance is no longer FIPS 140-2 validated.

Cryptographic services are disabled when the system begins processing an upgrade package. Once the upgrade package has been applied successfully, the appliance will be rebooted in order to allow the power-up self-tests to run.

9 Cryptographic Key Management

9.1 Cryptographic Keys and CSPs

Table 17: Keys and CSPs

Key/CSP	Description	Key/CSP Type & Size	Generation/Input	Output	Storage	Zeroization
Backup Encryption Key (BEK)	Used to encrypt backups	RSA 2048 wrapping key AES 256 ephemeral key	RSA - FIPS 186-4 AES - SP 800-133 Encrypted by SSH session when uploading for restoration	Encrypted by SSH session when downloading	Plaintext	Appliance Zeroization
Certificate Authority certificate (CA)	Used to sign certificates generated by the appliance	RSA 4096	FIPS 186-4 Backup restoration: encrypted	Plaintext (public key) Never (private key) Backed up: encrypted	Plaintext	Appliance Zeroization
Cluster Communication Encryption Key (CEK)	Used to encrypt communications between cluster nodes. Utilizes PostgreSQL support for TLS connectivity, with no custom elements.	RSA 3072 certificate for validation AES-GCM 256 ephemeral key	RSA - FIPS 186-4 during generation on primary cluster node AES-GCM - SP 800-133 Encrypted by HTTPS session during cluster configuration when input to joining node	Encrypted by HTTPS session during cluster configuration	Plaintext	Appliance Zeroization
Fornetix Customer Support Audit Log Encryption Key (FAEK)	Used to encrypt Audit Logs when the user specifies they will be transmitted to Fornetix Customer Support	RSA 4096 wrapping key AES 256 ephemeral key	RSA - Public key pre-loaded AES – SP 800-133	RSA – Never AES – Output wrapped by the RSA	Plaintext	Not zeroized
HTTPS and REST certificate (HTTPS)	Used for encryption of REST API calls and HTTPS web connections	RSA 2048 wrapping key Ephemeral key will be negotiated from these allowed algorithms: AES 128, 256 AES-GCM 128, 256	RSA - FIPS 186-4 AES/AES-GCM - SP 800-133 Backup restoration: encrypted	Plaintext (public key) Never (private key) Backed up: encrypted	Plaintext	Appliance Zeroization

Key/CSP	Description	Key/CSP Type & Size	Generation/Input	Output	Storage	Zeroization
Passwords	Username/password combinations used to login to the administrative menu or the REST/HTTPS interfaces	Minimum of 10-character passwords that meet complexity requirements	User input Backup restoration: encrypted	Never Backed up: encrypted	Hashed	Appliance Zeroization
Upload Decryption Key (UDK)	Used to decrypt uploads of licenses and upgrades provided by Fornetix	RSA 2048 wrapping key AES 256 ephemeral key	RSA – Private static key-agreement key preloaded AES – external/wrapped by RSA public key	Never	Plaintext	RSA Private static key-agreement key Not zeroized[4] AES zeroized
Upload Verification Keys (UVK)	GPG public keys used to verify signature of upgrades provided by Fornetix	3072-bit RSA public key	Public keys pre-loaded	Never	Plaintext	Appliance Zeroization
HMAC-SHA-256 Module Integrity Keys	Used to ensure cryptographic library files have not been changed	256-bit hash 128-bit key	preloaded	Never	Plaintext	Not zeroized
HMAC-SHA-512 Kernel Integrity Keys	Used to ensure kernel files have not been changed	512-bit hash 128-bit key	preloaded	Never	Plaintext	Not zeroized
SP800-90A DRBG: Entropy input string, V, C and Key (DRBG)	Entropy input seed data obtained from NDRNG	entropy input 4096-bit, HMAC key	internal from NDRBG	Never	In volatile memory	Zeroized by a module's API function call when the cipher handler is released
SSH DH public param	Negotiate SSH Ks and SSH Khmac	2048-bit Diffie-Hellman public parameters	DRBG	Plaintext	In volatile memory	Upon session termination
SSH DH private param	Negotiate SSH Ks and SSH Khmac	224-, 256-bit Diffie-Hellman private parameters	DRBG	Never	In volatile memory	Upon session termination
SSH Krsa public	Verify the signature of the server’s message	2048-bit RSA public key	FIPS 186-4	Plaintext	Plaintext	Appliance Zeroization
SSH Krsa private	Sign the server’s message	2048-bit RSA private key	FIPS 186-4	Never	Plaintext	Appliance Zeroization
SSH Ks	Encrypt and decrypt data	SSH session 128-, 192-, 256-bit AES key	Diffie-Hellman key agreement	Never	In volatile memory	Upon session termination or when a new Ks is generated (after

Key/CSP	Description	Key/CSP Type & Size	Generation/Input	Output	Storage	Zeroization
						a certain timeout)
SSH Khmac	Authenticate data	SSH session 512-bit HMAC key	Diffie-Hellman key agreement	Never	In volatile memory	Upon session termination or when a new Khmac is generated (after a certain timeout)
TLS Pre-MS	Derive MS	TLS pre-master secret	Input in encrypted form from client	Never	In volatile memory	Upon session termination
TLS MS	Derive TLS Ks and TLS Khmac	TLS master secret	Derived from Pre-MS using FIPS Approved key derivation function	Never	In volatile memory	Upon session termination
TLS Krsa public	Client encrypts Pre-MS. Client verifies server signatures	2048-, 3072-bit Server RSA public key	FIPS 186-4	Plaintext X509 certificate	Plaintext	At operator delete or zeroize request
TLS Krsa private	Server decrypts Pre-MS. Server generates signatures	2048-, 3072-bit Server RSA private key[1]	FIPS 186-4	Never	Plaintext	At operator delete or zeroize request
TLS Ks	Encrypt and decrypt data	TLS session 256-bit AES key	Derived from MS	Never	In volatile memory	Upon session termination
TLS Khmac	Authenticate data	TLS session 512-bit HMAC key	Derived from MS	Never	In volatile memory	Upon session termination
LDAP Binding Username and Password (LDAPUP)	Username/password combination used for binding to optional external LDAP authentication server	User-entered password which meets length and complexity requirements of their external LDAP server	User input Backup restoration: encrypted	Never Backed up: encrypted	Plaintext	At operator delete or zeroize request
LDAP CA Certificate (LDAPC)	CA Certificate of the optional external LDAP authentication server	User-uploaded CA certificate which meets key type and size requirements of their external LDAP server	User input Backup restoration: encrypted	Plaintext X509 certificate Backed up: encrypted	Plaintext	At operator delete or zeroize request
External Backups Username and Password (EBUP)	Username/password combination used for initial	User-entered password which meets length and	User input	Never	In volatile memory	After configuring the SSH Public Key of the

Key/CSP	Description	Key/CSP Type & Size	Generation/Input	Output	Storage	Zeroization
	setup of external backup server	complexity requirements of their external backup server				external backup server
External Backups SSH Public Key (EBSSH)	SSH public key of the external backup server, used for ongoing connectivity	2048-, 3072-bit RSA public key[1]	User input[2]	Plaintext	Plaintext	At operator delete or zeroize request
User-Generated Key Material (UGK)	Public/Private key pairs and symmetric keys generated by user actions.	Varies	Generation: Varies Backup restoration: encrypted; Encrypted in transit by HTTPS or TLS session	Encrypted in transit by HTTPS or TLS session Backed up: encrypted	Plaintext	At operator delete or zeroize request
User-Generated Certificates (UGC)	Certificates generated by user actions. Excludes the private key, which is treated as a UGK.	Varies	Generation: Varies Backup restoration: encrypted; User input plaintext	Plaintext Backed up: encrypted	Plaintext	At operator delete or zeroize request
Brokering Public Key (BPub)	Public Key of optional external Brokering server(s)	2048-, 3072-bit RSA public key[3]	User input Backup restoration: encrypted	Plaintext X509 certificate Backed up: encrypted	Plaintext	At operator delete or zeroize request
Brokering Private Key (BPriv)	Private Key of optional external Brokering server(s)	2048-, 3072-bit Server RSA private key[3]	User input Encrypted by SSH session when uploading Backup restoration: encrypted	Never Backed up: encrypted	Plaintext	At operator delete or zeroize request
Brokering CA Certificate (BCA)	CA Certificate of optional external Brokering server(s)	User-uploaded CA certificate which meets key type and size requirements of their optional external Brokering server(s)	User input Backup restoration: encrypted	Never Backed up: encrypted	Plaintext	At operator delete or zeroize request

[1] The public key used for SSH authentication to the external backups server can be 2048- or 3072-bit. Configuration of an external backup server to use any other key length is considered outside of FIPS guidance.

[2] During the configuration of an external backup server, username and password are used to establish the first connection. Using this connection, the SSH keys are exchanged to use for further communication.

[3] Public/private key pairs used for TLS authentication by clients or brokered servers can be 2048- or 3072-bit. Configuration of a client or brokered server to use any other key length is considered outside of FIPS guidance.

[4] This RSA and AES encryption is not considered a security service, and so per IG 1.23 the upload is considered to be in the equivalent of plaintext for 140-2 validation purposes.

9.2 Random Number Generation

The KO Appliance uses unmodified output from a SP800-90A-compliant Deterministic Random Bit Generator (DRBG) for creation of HMAC keys, key components of asymmetric keys, symmetric keys, and random number generation. As defined in SP800-90A, the DRBG obtains the seed and nonce from the kernel non-deterministic random number generator (NDRNG) during appliance startup. The DRBG is also reseeded after every 2^{48} requests for random numbers. During shutdown, 4096 bits of entropy are saved to ensure a new seed during the next restart.

The entropy available from /dev/random has been supplemented with additional hardware and a HAVEGE algorithm daemon as sources of entropy to reduce scenarios of entropy pool draining.

Continuous self-tests are performed on the output of NDRNG and SP800-90A DRBG to ensure that consecutive random numbers do not repeat.

The DRBG seed length is 4096 bits. With a minimum entropy of 6.36 bits per byte, this means the DRBG is seeded with (4096 bits / 8) * 6.36 bits/byte = 3256.32 bits of entropy.

9.3 Storage of Generated Key Material

Keys generated by authorized users of the KO Appliance are physically stored on the hard drive array on the front of the appliance.

Keys are stored in plaintext.

9.4 Protection of Stored Key Material

All communications with the KO Appliance to obtain key material requires an encrypted connection, using either mutual TLS, HTTPS, or SSH. Key material is never available in plaintext.

Access to obtain key material is controlled by user and role membership permissions, administered by the Crypto Officer.

9.5 System Initialization

When a KO appliance is booted for the first time out of the box, or after a zeroization, a System Administrator must access the console and implement the ‘first boot’ process. This process is triggered immediately on login using the factory default username and password and cannot be circumvented.

At the end of this process, all required system keys, certificates, and key-encrypting keys are generated.

For more information on this process, please see the User Guide.

9.6 Zeroization

Zeroization is performed using the system administration menu system. These functions are only accessible by System Administrators, via SSH connection or direct console access to the appliance. A four-value series of challenge/response prompts ensures that zeroization is only performed as an intentional operation.

- The process returns the KO appliance to factory defaults, except it leaves the system in FIPS mode.
- All system-generated keys and certificates, including the key encryption key, are deleted.
- All user credentials in all roles are deleted.
- All user-generated data is deleted.
- All backups are deleted.
- All of the deleted files are overwritten using Linux shred operations.
- The system is rebooted to ensure all in-memory data is purged.
- The system administrator will be able to confirm the zeroization after the system reboots, as it will force the same reconfiguration (including forced password change) as occurs when the appliance is first booted out of the box.

10 Self-Tests

FIPS self-tests are executed each time the KO Appliance is booted. This is an automatic process which does not require operator intervention and cannot be circumvented or disabled.

System Administrators may also manually execute the FIPS self-tests via the administrative menu: (4 - Manage Key Orchestration Appliance Chassis, 2 - FIPS Utilities, 4 - Place server in Self-Test mode)

In the event that self-tests are unsuccessful, the cryptographic services remain disabled, and no data inputs or outputs are permitted. A System Administrator can use the administrative menu to place the appliance into FIPS Self-Test mode in order to display the error message. Since there are no user-serviceable methods to correct FIPS failure status, detailed error messages are not displayed to the user, only the message “Your system has failed its FIPS tests.”

Customers are advised to reboot the KO Appliance in order to run the FIPS tests again on startup in an attempt to clear the FIPS failure state. If the FIPS error state persists, customers are instructed to contact Fornetix Customer Support for assistance when a FIPS error state occurs.

10.1 Power-Up Tests

Table 18: Power-Up Tests

Algorithm	Test
HMAC-SHA-512	Integrity Test
AES	KAT, encryption, and decryption are tested separately
RSA	KAT, signature generation and verification are tested separately
EC Diffie-Hellman	Primitive "Z" Computation KAT

HMAC-SHA-1, -224, -256, -384, -512 KAT	KAT
SHA-1, -224, -256, -384, -512 KAT	KAT
Module Integrity	HMAC-SHA-256
SP 800-90A HMAC DRBG	SP 800-90A section 11.3 health tests KAT

10.2 Conditional Tests

Table 19: Conditional Tests

Algorithm	Test
RSA	Pairwise consistency test: signature generation and verification, encryption, and decryption
SP 800-90A DRBG	Continuous Random Number Generator Test
NDRNG	Continuous Random Number Generator Test
RSA signature verification	Firmware Load Test

11 Guidance

11.1 Setup and Configuration

Fornetix KO appliances will be delivered with a tamper evident seal covering the screw which secures the top panel of the appliance and the gap between panels. There are additional tamper evident seals between the chassis and the front bezel on the top and bottom of the appliance. If these have been altered, do not use the appliance, and contact Fornetix Customer Support immediately for guidance.

The packaging in which the KO appliance is shipped also has factory seals. If these have been altered, do not use the appliance, and contact Fornetix Customer Support immediately for guidance.

When first powered on, an administrator must have console access (via serial terminal, or via KVM switch) to walk through a first boot configuration process. This process uses a factory default username and password which are noted in the KO setup and user guide.

11.2 FIPS Mode

After the initial configuration, FIPS mode must be enabled to ensure operation in a FIPS-approved state. This will be performed via the Administrative Menu, available immediately after the initial setup and configuration.