FIPS 140-2 Non-Proprietary Security Policy

DataLocker Inc.

Sentry - Encrypted USB Flash Drive

Document Version 1.1

May 23, 2018

Abstract

This document provides a non-proprietary FIPS 140-2 Security Policy for the Sentry - Encrypted USB Flash Drive.

Table of Contents

List of Tables

List of Figures

1 Introduction

1.1 About FIPS 140-2

Federal Information Processing Standards Publication 140-2 — Security Requirements for Cryptographic Modules specifies requirements for cryptographic products to be deployed by Federal Agencies in both the United States and Canada for the protection of sensitive but unclassified information. The Cryptographic Module Validation Program (CMVP) is a joint effort between the National Institute of Standards and Technology (NIST) and the Communications Security Establishment Canada (CSEC) that validates cryptographic modules to the FIPS 140-2 standard. The CMVP accredits independent Cryptographic and Security Testing (CST) laboratories to perform FIPS 140-2 testing. The CST labs use the Derived Test Requirements (DTR), Implementation Guidance (IG), and applicable CMVP programmatic guidance to test the cryptographic modules against the applicable standards. NIST's Computer Security Division (CSD) and CSEC jointly serve as the Validation Authorities for the CMVP, validating CST test reports and issuing certificates for products pursuing FIPS 140-2 validation. *Validation* is the term given to a product that is documented and tested against the FIPS 140-2 criteria.

More information is available on the CMVP website at
http://csrc.nist.gov/groups/STM/cmvp/index.html.

1.2 About this Document

This non-proprietary Cryptographic Module Security Policy for the Sentry - Encrypted USB Flash Drive from DataLocker Inc. (DataLocker) provides an overview of the product and a high-level description of how it meets the security requirements of FIPS 140-2. This document contains details on the module's cryptographic keys and critical security parameters. This Security Policy concludes with instructions and guidance on running the module in a FIPS 140-2 mode of operation.

The DataLocker Sentry - Encrypted USB Flash Drive may also be referred to as the "module" in this document.

1.3 External Resources

The DataLocker website (https://datalocker.com) contains information on the full line of products from DataLocker, including a detailed overview of the Sentry - Encrypted USB Flash Drive solution. The validated modules listing on the CMVP website (http://csrc.nist.gov/groups/STM/cmvp/validation.html) contains links to the FIPS 140-2 certificate and DataLocker contact information.

1.4 Notices

This document may be freely reproduced and distributed in its entirety without modification.

1.5 Acronyms

The following table defines acronyms found in this document:

Acronym	Term
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
CSEC	Communications Security Establishment of Canada
CSP	Critical Security Parameter
DRBG	Deterministic Random Bit Generator
DTR	Derived Test Requirements
ECB	Electronic Codebook
FIPS	Federal Information Processing Standard
GPC	General Purpose Computer
GUI	Graphical User Interface
HMAC	Hashed Message Authentication Code
KAT	Known Answer Test
NIST	National Institute of Standards and Technology
NVRAM	Non-Volatile Random Access Memory
PBKDF	Password-Based Key Derivation Function
RNG	Random Number Generator
RSA	Rivest Shamir Adelman
SHA	Secure Hash Algorithm
USB	Universal Serial Bus

Table 1 – Acronyms and Terms

2 DataLocker Sentry - Encrypted USB Flash Drive

2.1 Product Overview

DataLocker's Sentry - Encrypted USB Flash Drive is assembled in the U.S. for organizations that require a secure way to store and transfer portable data. The stored data is secured by hardware-based 256-bit AES encryption to guard sensitive information in case the drive is lost or stolen. Its durable, metal casing provides added protection.

The Sentry - Encrypted USB Flash Drive is an enterprise-grade USB Flash drive with 256-bit on-the-fly encryption. Its strong password rules and lock-down control protect against brute force attacks. Such advanced security features make the Sentry - Encrypted USB Flash Drive ideal for corporations and service organizations that require employees to transport large digital files consisting of confidential documents.

2.2 Validation Level Detail

The following table lists the level of validation for each area in FIPS 140-2:

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

Table 2 – Validation Level by DTR Section

The "Mitigation of Other Attacks" section is not relevant as the module does not implement any countermeasures towards special attacks.

2.3 Cryptographic Algorithms

2.3.1 Approved Algorithms

In FIPS mode of operation, only the following FIPS approved algorithms are to be used:

- AES ECB/CBC/XTS mode with 256-bit keys encryption/decryption
- SHA-256 hashing
- HMAC-SHA-256 for HMAC functions
- DRBG: HMAC-SHA-256 DRBG
- RSA: Signature verification using 2048-bit keys with SHA-256 (Used for firmware update verification)
- SP 800-132 PBKDF (option 2a) (vendor-affirmed)
    - Password/passphrase length used in key derivation: 8 bytes ~ 136 bytes
    - The upper bound of the probability of having the password guessed at random is: 1 / (26 * 2 + 10 + 32)^8. Please see Section 2.6.3 for a detailed description of the authentication mechanism.
    - The "iteration" count of SP 800-132 PBKDF2 (HMAC-SHA-256) module is 1024. There is a 256-byte salt used in the module and the salt is generated by SP 800-90A HMAC-SHA-256 DRBG and is stored to eMMC.

2.3.2 Algorithm Implementation Certificates

The module's cryptographic algorithm implementations have received the following certificate numbers from the Cryptographic Algorithm Validation Program:

Algorithm Type	Algorithm	Standard	CAVP Certificate	Use
Random Number Generation	DRBG: HMAC-SHA-256 DRBG	SP 800-90A	# 494	Random Number Generation
Hashing	SHS (SHA-256)	FIPS 180-4	# 2379	Message digest
Symmetric Key	AES ECB/CBC/XTS mode with 256-bit keys	FIPS 197 SP 800-38E	# 2838	Encryption / decryption for entire partition
Hashed message authentication code	HMAC-SHA-256	FIPS 198-1	# 1779	HMAC functions
Asymmetric Key	RSA	FIPS 186-4	# 1480	Firmware update verification

Table 3 – Algorithm Certificates

2.3.3 Other Algorithms

The module implements the following other algorithms:

- Hardware-based random number generator (HWRNG)
    - This HWRNG is used only as a seeding mechanism to the FIPS-approved DRBG.
- RSA 2048 for key wrapping (allowed for use in FIPS mode)
    - Key establishment methodology provides 112 bits of encryption strength

2.4 Cryptographic Module Specification

The module is the DataLocker Sentry - Encrypted USB Flash Drive running Firmware Version 3.05. The following Part Numbers are included and differ only by the bundled host application, which is excluded from the validation.

Description	Part Numbers
Sentry EMS - Using EMS Client UI and only compatible with EMS management services	SEMS04, SEMS08, SEMS16, SEMS32, SEMS64
Sentry SC Managed - Using SafeConsole's Client UI and only compatible with SafeConsole management services	SSC004M, SSC008M, SSC016M, SSC032M, SSC064M
Sentry One - Using a new unified SafeConsole/EMS Client UI and compatible with both EMS and SafeConsole management services	SONE004, SONE008, SONE016, SONE032, SONE064, SONE128, SONE256
Sentry One Managed - Using a new unified SafeConsole/EMS Client UI and compatible with both EMS and SafeConsole management services	SONE004M, SONE008M, SONE016M, SONE032M, SONE064M, SONE128M, SONE256M

Table 4 – Part Numbers

The module is classified as a multi-chip standalone cryptographic module, and the physical cryptographic boundary is drawn at the module's printed circuit board with USB connector and LED interface and includes all significant components within that boundary. The module's memory is logically partitioned; memory not executable by the module (Host-application on CD-ROM partition) is considered excluded. The physical boundary is pictured in the image below:

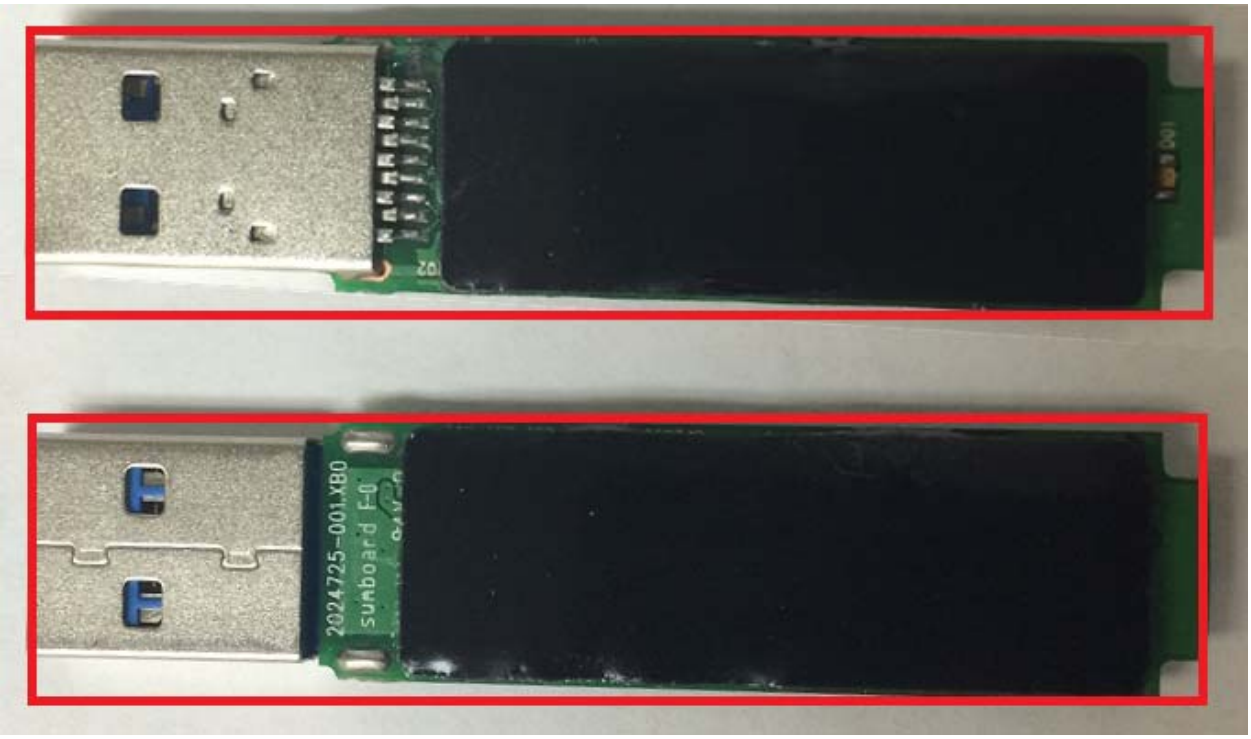

Figure 1 – Physical Boundary

The cryptographic boundary does not include the polymer case and USB cap of the Sentry – Encrypted USB Flash Drive. The host application (version 4.8, 5.5, 6.0) is inside of the crypto boundary but is excluded from validation. The potting provides sufficient physical security; compromising the exterior metallic casing does not compromise the security of the device. No excluded components process CSPs, plaintext data, or other information that if misused could lead to a compromise.

2.5 Module Interfaces

The interfaces for the cryptographic boundary include physical and logical interfaces. The physical interfaces provided by the module are mapped to four FIPS 140-2 defined logical interfaces: Data Input, Data Output, Control Input, and Status Output. The mapping of logical interfaces to module physical interfaces is provided in the following table:

FIPS 140-2 Logical Interface	Module Physical Interface
Data Input	Data pins within the USB Port
Data Output	Data pins within the USB Port
Control Input	Data pins within the USB Port
Status Output	Data pins within the USB Port LED
Power	Power pin within the USB Port

Table 5 – Logical Interface / Physical Interface Mapping

The USB 3.0 protocol ensures these logical interfaces are distinct. The module does not support the input or output of plaintext cryptographic key components, authentication data, and CSPs.

2.6 Roles, Services, and Authentication

The following table lists the roles in the module that operators may assume. The respective services for each role are described in the following sections.

Role	Authentication Type & Mechanism
Crypto Officer (CO)	Identity-based authentication via username and password (see Section 2.6.2)
User	Identity-based authentication via username and password (see Section 2.6.2)
Firmware Update Officer	Identity-based authentication via username and RSA 2048 digital signature verification during the Firmware Load Test. (This role has a hardcoded password, but no security is claimed for the password method of authentication.)
Vendor	N/A: This role is unauthenticated. (This role has a hardcoded password, but no security is claimed for the password method of authentication.)
CD Update Officer	N/A: This role is unauthenticated. (This role has a hardcoded password, but no security is claimed for the password method of authentication.)

Table 6 – Supported Roles

2.6.1 Operator Services and Descriptions

The services available to the roles in the module are as follows:

Service	Description	Service Input	Service Output	Roles
Zeroization	Zeroize all keys and CSPs	Password Authentication	Keys/CSPs zeroized	Crypto Officer
Firmware Update	Load/Update firmware	Signed Firmware	Status output via LED and alert to host machine GUI	Firmware Update Officer
Set Vendor INFO	Set information on Vendor INFO Block	Vendor INFO values	Vendor INFO value stored	Vendor
CD Update	Load/Update CD Image to the CD-ROM partition	CD Image	CD Image stored	CD Update Officer
Initialize	Create password and generate keys to place the	Enter password	Password stored, self tests run, and	User

Service	Description	Service Input	Service Output	Roles
	module in FIPS 140 mode of operation		keys generated	
Show Status	Verify self-test success/failure	Password Authentication	Status output via LED and alert to host machine GUI	User
Encrypt	Encrypt partition with AES	Password Authentication	Partition encrypted	User
Decrypt	Decrypt AES-encrypted partition when reading from the device	Password Authentication	Partition decrypted and files are readable	User
Format Drive	Erase all files stored on the module and zeroizes keys and CSPs	User initiates "Forgot Password" procedure or initiates the format drive function once authenticated	Partition formatted and keys/CSPs overwritten with new values	User
Run Self Tests	Performs power on self tests; invoked by inserting module into the host machine	N/A	Status output of results / module disabled in tests fail, allows authentication if tests pass	User

Table 7 – Operator Services and Descriptions

2.6.2 Operator Authentication

Username & Password

The user authenticates as part of the setup process. The module needs to validate two values before the operator gets access to the private encrypted area:

1. The default user name of 12345678
2. The secret disk password entered by the user.

The module validates these values. The User roles authenticate via host machine over the USB port. Other than status functions available by viewing LEDs, the services described in Table 7 – Operator Services and Descriptions are available only to identified and authenticated operators.

When a User first inserts the module, they are prompted by the host application to create a username and password. Once created, the module will generate a Data Encryption Key to encrypt the partition associated with that password. Access to the host application and thus any available module services requires a valid password, which is entered via a login prompt that is displayed when the module is connected to the host machine. To authenticate to the module, an operator must connect to the module via management application and provide a username and password. A valid login (i.e., valid

username and valid associated password) is required for all services accessed through the application. Once authenticated, further use of the module on the host machine will not require the user to authenticate since it will already be associated with the software on the host machine. If the module is removed from the host PC and then reinserted, the operator will be required to authenticate before the module can be used.

The module ensures there is no visible display of Crypto Officer or User authentication data during data entry.

RSA Digital Signature

The Firmware Update Officer role is identified using an 8-digit username and authenticated using the RSA 2048 signature embedded within the firmware image.

2.6.3 Authentication Strength

Username & Password

The User and Crypto Officer are authenticated via a username and password. The Crypto Officer password is 8-characters in length; the User password must be at least 8-characters in length. Passwords may include the following character types: uppercase letters, lowercase letters, numbers, and special characters (all US-keyboard printable special characters). Therefore, the character space is 94. The probability that a random attempt will succeed or a false acceptance will occur is approximately $1/94^8$, which is less than 1/1,000,000.

The module will lock an account after 10 consecutive failed authentication attempts; thus, the maximum number of attempts in one minute is 10. Therefore, the probability of a success with multiple consecutive attempts in a one minute period is $10/94^8$ which is less than 1/100,000.

RSA Digital Signature

RSA 2048 with SHA-256 provides 112 bits of security, therefore the probability of a successful random attempt is $1/(2^{112})$, which is less than 1/1,000,000.

An attacker may be able to perform 0.83 attempts per second via a scripted or automatic attack, therefore the probability of a success with multiple attempts in a one minute period is $50/(2^{112})$, which is less than 1/100,000.

2.7 Physical Security

The module is a multiple-chip standalone module and conforms to Level 3 requirements for physical security. The module is composed of production-grade components and is completely covered with a hard, opaque potting material. Any attempts to remove the potting will result in permanent damage to the module.

Note: Module hardness testing was only performed at ambient temperature; no assurance is provided for Level 3 hardness conformance at any other temperature.

The operator of the module should inspect the outer casing of the module every time before connecting the module to a computer. If tamper evidence is observed on the outer casing, please discontinue use of the module immediately.

2.8 Operational Environment

The module operates in a limited operational environment and does not implement a General Purpose Operating System.

2.9 EMI/EMC

The module meets the requirements of 47 CFR PART 15 regulation & ANSI C63.4 and ICES-003 for the evaluation of Class B of electromagnetic compatibility. This device complies with Part 15 of FCC Class B rules for home or office use.

2.10 Cryptographic Key Management

The table below provides a complete list of Critical Security Parameters used within the module:

R = Read W = Write D = Delete

Key/CSP Name	Description / Use	Generation	Storage	Establishment / Export	Destruction	Privileges
AES Session Key (secure channel)	AES-256 key used to encrypt secure channel data between host application and module	Internal generation by SP 800-90A DRBG.	**Storage:** RAM plaintext **Association:** Associated with unique secure channel session between host application and module.	**Agreement**: RSA keywrap **Entry**: NA **Output**: RSA keywrapped	Overwrite with zeros immediately after secure session is terminated	User: R CO: R (Generated before authentication from users is initiated)
MAC Key (secure channel)	HMAC-SHA-256 key used to authenticate messages sent via secure channel between host application and module.	Internal generation by SP 800-90A DRBG.	**Storage:** RAM plaintext **Association:** Associated with unique secure channel session between host application	**Agreement**: RSA keywrap **Entry**: NA **Output**: RSA keywrapped	Overwrite with zeros immediately after secure session is terminated	User: R CO: R (Generated before authentication from users is initiated)

Key/CSP Name	Description / Use	Generation	Storage	Establishment / Export	Destruction	Privileges
			and module.			
Data Encryption Key	XTS-AES 256-bit key for encryption / decryption of all files on the drive	Internal generation by SP 800-90A DRBG.	**Storage**: NVRAM (obfuscated with DEK Encryption Key). **Association**: The system is the one and only owner. Relationship is maintained by the controller via protected memory. Only a single AES-256 data key to encrypt a whole partition content.	**Agreement**: NA **Entry**: NA **Output**: None	The operator initiates the "Forgot Password" procedure The CO decommissions the drive to securely wipe the contents	CO: D User: R W D
DEK Encryption Key	256-bit AES key for obfuscating the Data Encryption Key	Derived from User Password using PKCS#5 PBKDF2 and HMAC-SHA-256	**Storage**: RAM plaintext	**Agreement**: NA **Entry**: NA **Output**: None	Overwrite with zeros immediately	None
DRBG Entropy Input	HWRNG providing 512-bit entropy to seed the SP 800-90A DRBG	Internal generation by HWRNG	**Storage**: RAM plaintext **Association**: The system is the one and only owner.	**Agreement**: NA **Entry**: NA **Output**: NA	Reset / reboot the module Generate a new value The operator initiates the "Forgot Password" procedure The CO decommissions the drive to securely wipe the contents	CO: D User: None
DRBG Nonce	HWRNG providing 512-bit Nonce to seed the SP 800-90A DRBG	Internal generation by HWRNG	**Storage**: RAM plaintext **Association**: The system is the one and	**Agreement**: NA **Entry**: NA **Output**: NA	Reset / reboot the module Generate a new value The operator	CO: D User: None

Key/CSP Name	Description / Use	Generation	Storage	Establishment / Export	Destruction	Privileges
			only owner.		initiates the "Forgot Password" procedure The CO decommissions the drive to securely wipe the contents	
DRBG V Value	Secret value of the internal state	Internally generated by SP 800-90A DRBG	**Storage**: RAM plaintext **Association**: The system is the one and only owner.	**Agreement**: NA **Entry**: NA **Output**: NA	Reset / reboot the module Generate a new value The operator initiates the "Forgot Password" procedure The CO decommissions the drive to securely wipe the contents	CO: D User: None
DRBG Key Value	Secret value of the internal state	Internally generated by SP 800-90A DRBG	**Storage**: RAM plaintext **Association**: The system is the one and only owner.	**Agreement**: NA **Entry**: NA **Output**: NA	Reset / reboot the module Generate a new value The operator initiates the "Forgot Password" procedure The CO decommissions the drive to securely wipe the contents	CO: D User: None
Crypto Officer Password	Alphanumeric passwords for authentication to the module.	Not generated by the module;	**Storage**: NVRAM hashed with SHA-256 **Association**: controlled by the controller	**Agreement**: NA **Entry**: AES encrypted entry via host machine management application. Passwords are $\geq$ 8 characters	The CO decommissions the drive to securely wipe the contents	CO: R W D

Key/CSP Name	Description / Use	Generation	Storage	Establishment / Export	Destruction	Privileges
				in length. **Output**: NA		
User Password	Alphanumeric passwords externally generated by a human user for authentication to the module.	Not generated by the module;	**Storage**: NVRAM hashed with SHA-256 **Association**: controlled by the controller	**Agreement**: NA **Entry**: AES encrypted entry via host machine management application. Passwords are ≥ 8 characters in length. **Output**: NA	The operator initiates the "Forgot Password" procedure to overwrite the passwords with a new one The CO decommissions the drive to securely wipe the contents	CO: D User: R W D

Table 8 – CSP Management Details

The table below provides a complete list of public keys used within the module:

R = Read W = Write D = Delete

Key Name	Description / Use	Generation	Storage	Establishment / Export	Destruction	Privileges
RSA Public Key (keywrap)	2048-bit key used in the establishment of the secure channel between the host application and module.	Generated externally by host application and imported to the module during establishment of secure session.	**Storage:** RAM plaintext **Association:** The host application is the one and only owner. Relationship is maintained by the host application, which owns the corresponding private key.	**Agreement**: NA **Entry**: Plaintext **Output**: None	Overwrite with zeros immediately after secure session is terminated	User: W CO: W
RSA public key	2048-bit key used in the Firmware integrity check and firmware load test.	N/A - programmed during manufacturing	**Storage:** Stored in the Firmware Area (NVRAM) along with Firmware Code and RSA-2048/SHA-256 signature where the Firmware Area	**Agreement:** NA **Entry:** Plaintext with new firmware upload **Output:** NA	NA	User: R CO: R Firmware Update Officer: R W

Key Name	Description / Use	Generation	Storage	Establishment / Export	Destruction	Privileges
			is logically allocated in the eMMC during manufacturing			

Table 9 – Public Key Management Details

The module does not support key entry. The module supports entry of passwords for authentication, and these parameters are not distributed outside the cryptographic boundary.

When the user initiates the "Forgot Password" procedure from the application, the module will overwrite all keys and CSPs with new values. Data encrypted with the overwritten Data Encryption Key cannot be decrypted. When the Crypto Officer authenticates and issues a command to zeroize the device, all keys and CSPs will be zeroized, and the module will be decommissioned.

2.11 Self-Tests

The module includes an array of self-tests that are run during startup and periodically during operations to prevent any secure data from being released and to ensure all components are functioning correctly. In the event of any self-test failure, the module will output an error dialog and will shutdown. No keys or CSPs will be output when the module is in an error state.

The module does not support a bypass function.

The following sections discuss the module's self-tests in more detail.

2.11.1 Power-On Self-Tests

Power-on self-tests are run upon every initialization of the module and if any of the tests fail, the module will not initialize. The module will enter an error state and no services can be accessed by the users. The module implements the following power-on self-tests:

- SHA-256 KAT
- HMAC-SHA-256 KAT
- RSA-2048/SHA-256 Signature Verification KAT
- AES-256 ECB Encrypt and Decrypt KATs
- AES-256 CBC Encrypt and Decrypt KATs
- AES-256 XTS Encrypt and Decrypt KATs
- HMAC-SHA-256 DRBG KAT

- RSA-2048/SHA-256 Signature Verification for Firmware Integrity Check

The SP 800-132 PBKDF KAT is currently not required per IG D.6.

The module performs all power-on self-tests automatically when the module is initialized. All power-on self-tests must be passed before a User/Crypto Officer can perform services. The Power-on self-tests can be run on demand by rebooting the module.

An operator can discern that all power-on self-tests have passed and FIPS-mode is enabled via normal operation of the module, presentation of the GUI interface, and observing the LED blinking slowly at 3.125 hertz during initialization and read/write activity to the module.

If the module fails a POST, the module will not be connected to the host system and the USB D+/D- pins will be isolated. In this case, the module will not be initialized and no critical security parameters will be available. The LED will blink rapidly at 16 hertz.

2.11.2 Conditional Self-Tests

Conditional self-tests are test that run continuously during operation of the module. If any of these tests fail, the module will enter an error state. The module can be re-initialized to clear the error and resume FIPS mode of operation. No services can be accessed by the operators. The module performs the following conditional self-tests:

- Continuous RNG test run on output of DRBG
    - Because there is 16-byte random number output after calling RNG each time, there are two calls to generate the AES 256 key. The test is run with each call.
- Continuous test on output of DRBG seed mechanism (HW RNG)
- Firmware Load Test (RSA-2048 Signature Verification)

If the module fails a conditional self-test, the module will not be connected to the host system and the USB D+/D- pins will be isolated.

2.12 Mitigation of Other Attacks

The module does not mitigate other attacks.

3 Guidance and Secure Operation

This section describes how to configure the module for FIPS-approved mode of operation. Operating the module without maintaining the following settings will remove the module from the FIPS-approved mode of operation.

3.1 Crypto Officer Guidance

3.1.1 General Guidance

The Crypto Officer must not disclose passwords and must store passwords in a safe location and according to his/her organization's systems security policies for password storage.

3.2 User Guidance

3.2.1 Module Initialization and Configuration

The User must configure and enforce the following initialization procedures:

1. Verify that the firmware version is 3.05. Initialize the device following the instruction on the user-interface and log into the device. Click on the "Help" tab on the UI window and select "About" option. Then, the following screen will show the firmware and application versions.
2. When the module is initializing in FIPS mode, the LED will blink slowly at 3.125 hertz. After module initialization occurs, and the partition is mounted, the LED will blink at 3.125 hertz while read/write activity is occurring.
3. Do not disclose passwords and store passwords in a safe location and according to the organization's systems security policies for password storage.

Note that when the module is plugged into to a host machine for the first time, the User will create a password, and the module will be formatted.