FIPS 140-2 Non-Proprietary Security Policy
Apricorn FIPS Module 140-2

Author: Robert Davidson
Date: Tuesday, February 14, 2017
Document Issue: REV C February 14, 2017

Table of Contents

Revision History	
Version 1.0	Initial Public Release
Version 1.1	Change to add firmware version 7.6

Table 1 - Revision History

1. References

Author	Title
NIST	FIPS PUB 140-2: Security Requirements For Cryptographic Modules, December, 2002
NIST	Derived Test Requirements for FIPS PUB 140-2, March, 2004
NIST	Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program, May, 2006
NIST	FIPS 197
NIST	FIPS 180-4
NIST	FIPS 186-4
NIST	SP 800-90A Revision 1
NIST	SP 800-38A
NIST	SP 800-38E
NIST	SP 800-56A Revision 2

Table 2 - References

2. Target Audience

- NIST, CSE, Accredited Laboratory and the FIPS 140-2 Validation Group
- Developers Working on the Release
- Product Verification
- Documentation
- Product and Development Managers
- Security Assurance
- Administrator and General User

3. Introduction

This Security Policy document contains a description of the Apricorn FIPS Module 140-2 Cryptographic Module (also referred to herein as the **cryptographic module**, or simply the **module**). This document contains a specification of the security rules under which the module must operate as derived from the requirements of FIPS 140-2.

3.1 Purpose of the Security Policy

There are three major reasons that this security policy is defined for, and must be followed by, the cryptographic module:

- This document is required for FIPS 140-2 validation.
- This document allows individuals and organizations to determine whether the cryptographic module, as implemented, satisfies the stated security policy.
- This document describes the capabilities, protection, and access rights provided by the cryptographic module, allowing individuals and organizations to determine whether it will meet their security requirements.

3.2 Cryptographic Module Description

The cryptographic module is a multi-chip embedded cryptographic module. Specifically, the module is a USB 3.0 to SATA II which implements hardware encryption dependent on operator authentication.

The module provides secure encrypted (AES-XTS 256) storage, ensuring that only authorized operators have access to the protected data.

Access is granted by use of a keypad whereby the authorized operator inputs a personal identification number (PIN) to access and unlock the secured data.

Apricorn FIPS Module 140-2	
Firmware Version	7.0 [A], 7.6 [B]
Hardware Version	REV. D with CAN 1A [A, B]

Table 3 - Cryptographic Module Hardware and Firmware Versions

List of all Approved Security Functions:

The cryptographic module offers FIPS Approved cryptographic security functions including the following:

CAVP Cert.	Algorithm	Standard	Mode / Method	Key Lengths, Curves or Moduli	Use
2235	AES	SP 800-38E	XTS	256-bit	Data Encryption / Decryption Note: This mode is only approved for storage applications, and AES-XTS-128 is NOT supported by the cryptographic module.
4032	AES	SP 800-38A	CBC	256-bit	Data Decryption
260	DRBG	SP 800-90A Revision 1	HASH_Based DRBG		Deterministic Random Bit Generation
919	ECDSA	FIPS 186-4	PKG, PKV	P-256	Prerequisite to KAS ECC CDH
86	KAS EC-DH	SP 800-56A Revision 2	ECC	P-256	Key Agreement
1911	SHS	FIPS 180-4	SHA-256		Message Digest

Table 4 – List of All Approved Security Functions

NOTICE: Users should reference the transition tables that will be available at the CMVP Web site (http://csrc.nist.gov/groups/STM/cmvp/). The data in the tables will inform Users of the risks associated with using a particular algorithm and a given key length.

List of all non-Approved but Allowed Security Functions:

Algorithm	Caveat	Use
Hardware NDRNG	None; not applicable	Seeding for the HASH DRBG

Table 5 – List of all non-Approved but Allowed Security Functions

Figures 1-6 – Pictures of FIPS Module 140-2 REV. D with CAN 1A

NOTICE: In accordance with Apricorn's implemented configuration management system different aspects of the hardware are subject to unique identification and version/revision. To avoid any confusion about part numbers shown in the images below, please be mindful of the following:

1) The cryptographic module described herein is hardware version/revision: "Rev. D with CAN 1A".

2) The "REV A" as shown in Figure 6 is the version/revision of the silk screen of the cryptographic module

Figure 1 Cryptographic Boundary (Front Picture)

Figure 2 Cryptographic Boundary (Left Picture)

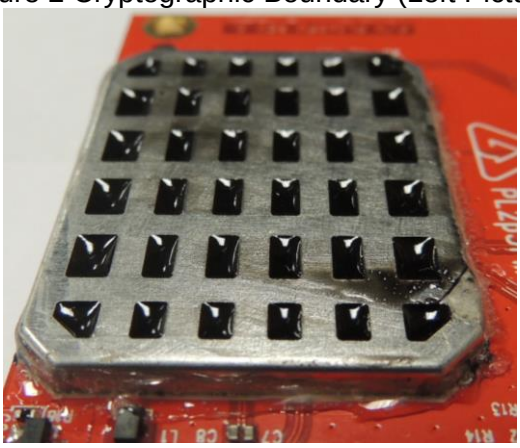


Figure 3 Cryptographic Boundary (Right Picture)

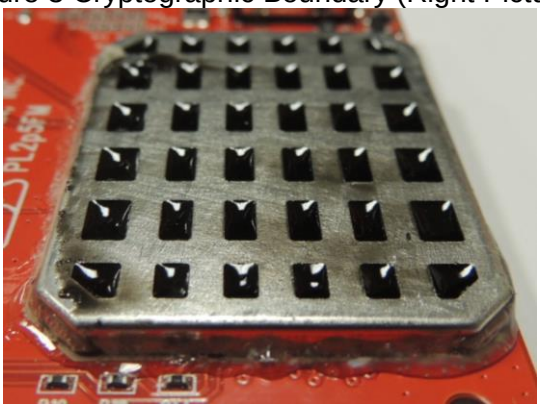


Figure 4 Cryptographic Boundary (Back Picture)

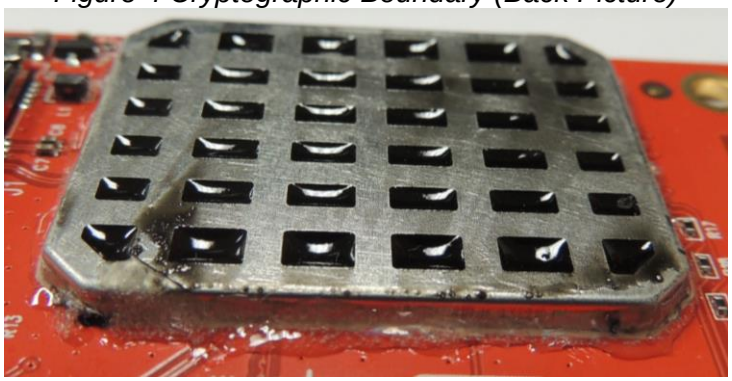


Figure 5 Cryptographic boundary (Top Picture)

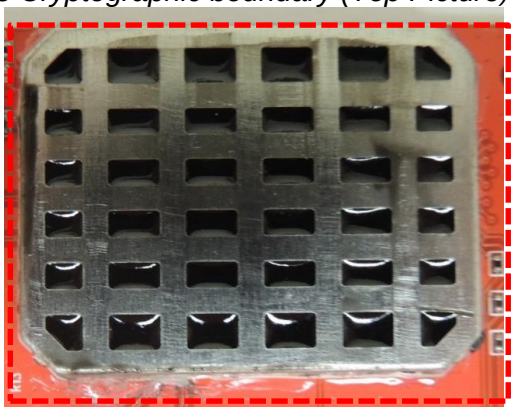
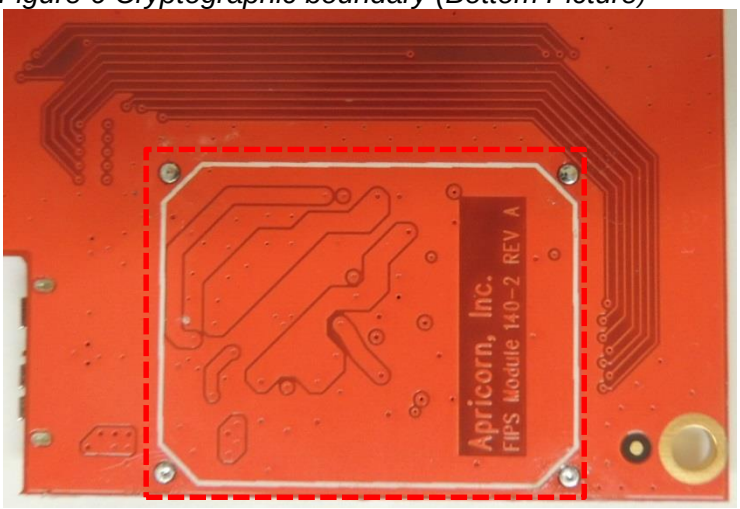


Figure 6 Cryptographic boundary (Bottom Picture)



Note: The "REV A" in Figure 6 does NOT represent the Hardware Version of the cryptographic module.

The cryptographic module is designed to meet FIPS 140-2 Level 2 cryptographic module requirements for the storage of user credentials and file systems. The module will only operate in the "FIPS Approved" mode of operation (i.e. non-FIPS mode is not supported).

The diagram below, marked Apricorn FIPS Module 140-2, represents the physical boundary of the device and the cryptographic boundary as outlined by the red marking.

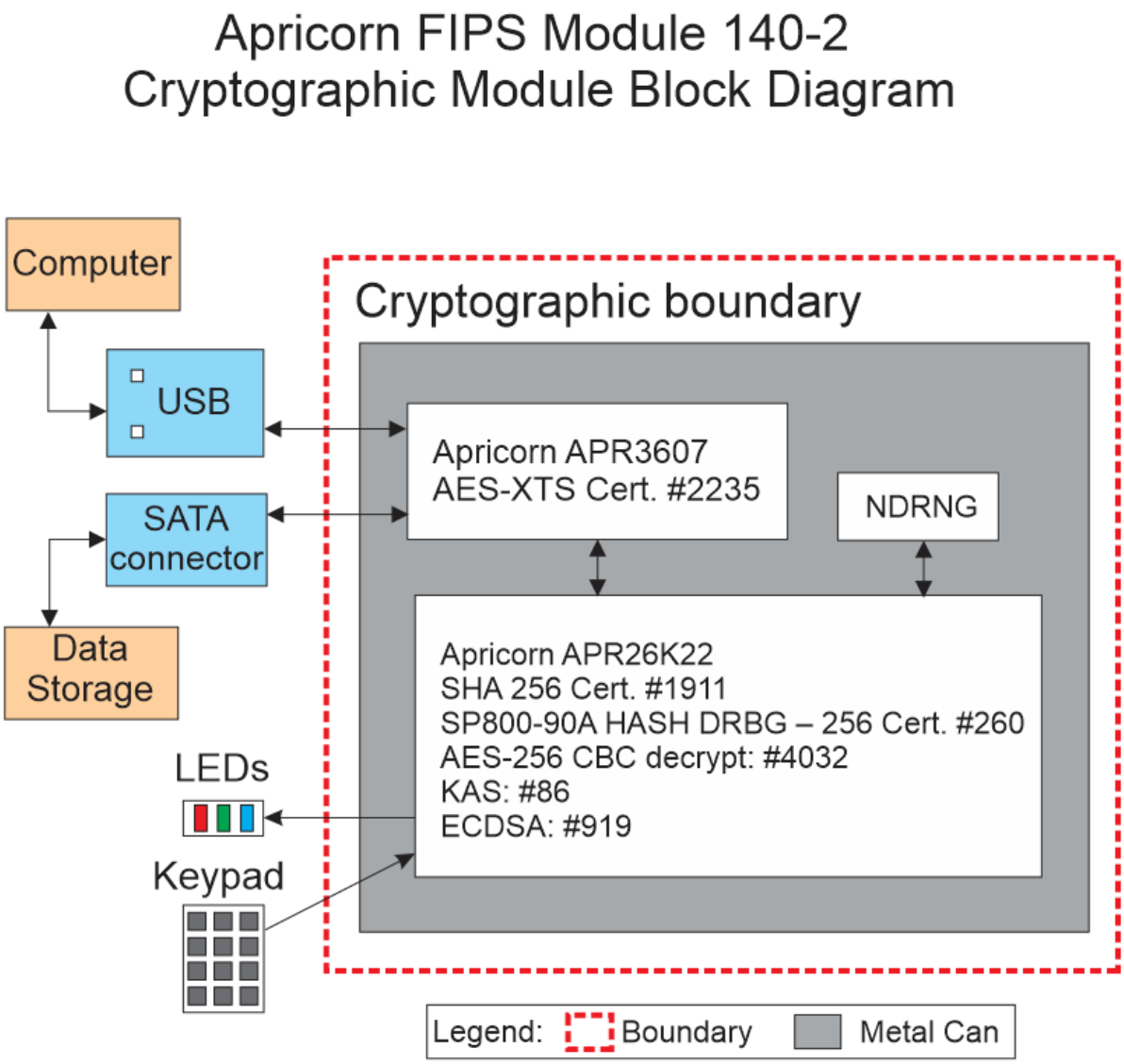


Figure 7 – Apricorn FIPS Module 140-2 Block Diagram

Note: The Computer, USB, SATA connector, Data Storage, Keypad, and LEDs are NOT a part of the cryptographic boundary.

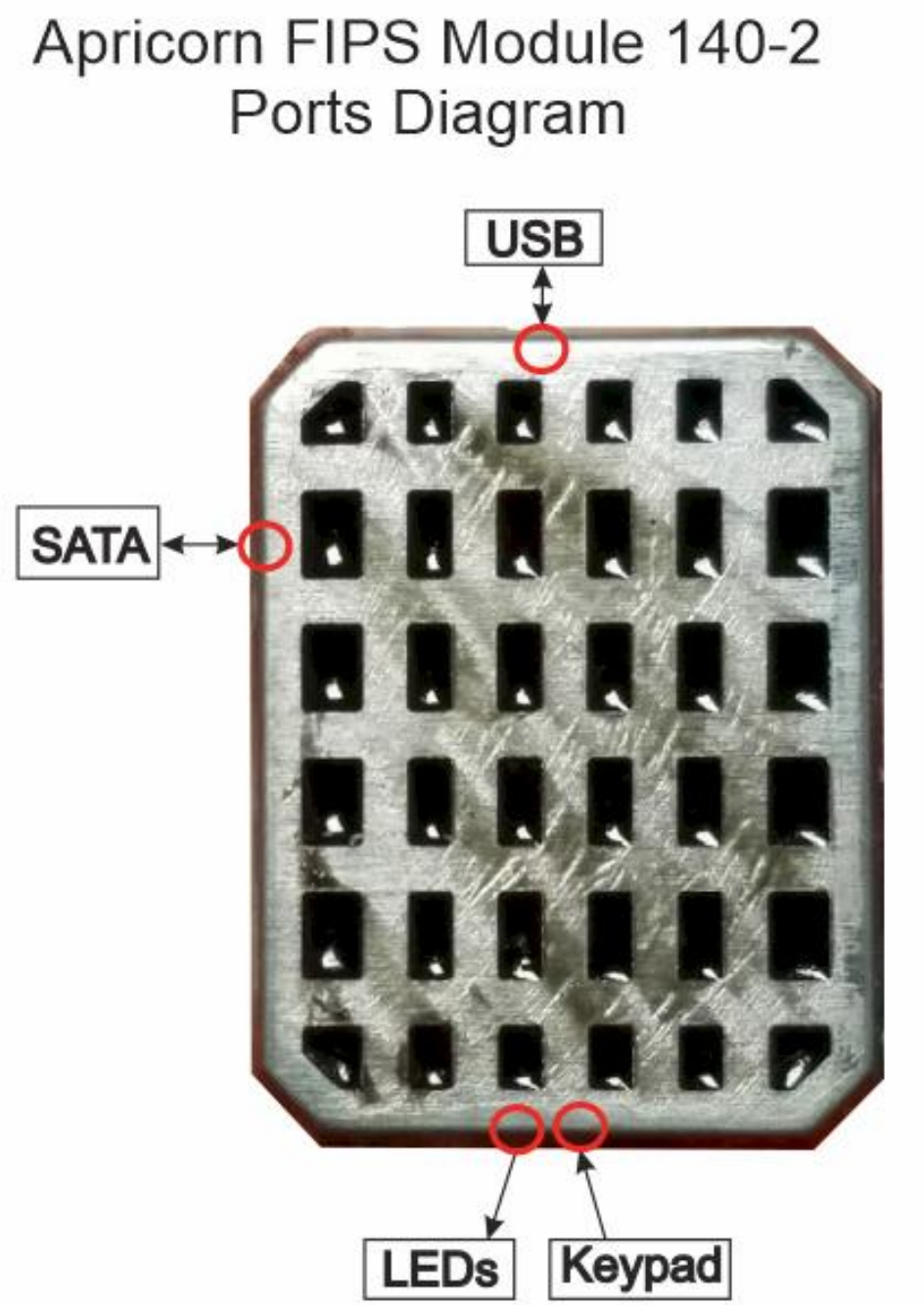


Figure 8 – Apricorn FIPS Module 140-2 Ports Diagram

4. Security Levels

The cryptographic module meets an overall security FIPS 140-2 Level 2. The FIPS 140-2 specification defines security requirements that are grouped into Security Requirement Areas. These areas are tested individually for a specific level of achievement. The table below defines the targeted level in each section for the module.

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

Table 6 - Security Levels

5. Interfaces and Ports

There are four physical ports on the cryptographic module: a Super Speed Universal Serial Bus (USB 3.0), a Keypad, a SATA connector for the external storage device, and signals to drive three external status LEDs.

Physical Port	Description	Logical Interface
Super Speed Universal Serial Bus (USB 3.0)	Super Speed Universal Serial Bus Signals (USB 3.0)	Data Input/ Data Output/Power
Keypad	External Keypad Control Input Signals	Control Input (manual controls)
SATA	SATA Signals	Data Input/ Data Output/Power
LEDs output (Red, Blue, Green)	Signals output to External LEDs (Red, Blue, Green)	Status Output

Table 7 - Physical Ports and Interfaces

6. Cryptographic Key and CSP Management

6.1 AES Master Key

The cryptographic module uses an AES Master Key (an AES-XTS 256-bit key) to encrypt/decrypt protected data. The AES 256-bit key is generated using the FIPS Approved deterministic random bit generator (SP 800-90A HASH DRBG Cert #260).

6.2 PIN Access Codes

On the cryptographic module, each personal identification number (PIN) has a minimum of seven digits and maximum of sixteen digits. The module supports one Admin PIN, four User PINs, and four Recovery PINs.

The Admin PIN is used by the cryptographic officer to administer the device or access the storage area.

The User PIN is used to access the storage area.

The Recovery PIN is used to create a new User PIN.

6.3 Random Number Generation

The cryptographic module contains a non-deterministic hardware random number generator (NDRNG) that uses an internal, unpredictable physical source of entropy that is outside of human control. Random numbers generated by the NDRNG are used as seeding values for the FIPS Approved Deterministic Random Bit Generator (SP 800-90A HASH DRBG Cert #260). Continuous RNG tests are performed on the outputs of the NDRNG and on the outputs of the Approved SP 800-90A DRBG.

The HASH DRBG Internal State is used to generate keys.

The HASH DRBG Seed is used to generate keys.

6.4 ECC CDH Key Establishment

AES-CBC Decryption Key is used to decrypt the data sent from the host.

Client ECC CDH Public Key is used to create secure communication with the host.

Client ECC CDH Private Key is used to create a public key and shared secret.

Client ECC CDH Shared Secret "Z" is used to generate a key derivation function.

Client ECC CDH Secret Keying Material is used for generating in the creation of the key derivation function.

Host ECC CDH Public Key is used to create secure communication with the Client.

Client ECC CDH KDF Internal State is used to generate the Client ECC CDH Secret Keying Material.

6.5 Zeroization

The module supports active zeroization of all critical security parameters. When zeroization occurs, all critical security parameters are permanently destroyed.

7. Identification and Authentication Policy

7.1 Roles

The cryptographic module performs role based authentication via verification of the PIN code for the Administrator role and General User role.

The Administrator role is the Cryptographic Officer role as defined in the FIPS 140-2 standard. The Administrator role is responsible for the overall security of the module.

The Administrator can change his/her own personal identification number (PIN) and can access all of the data stored within the device, as well as add and erase a General User.

The General User role is the User role as defined in the FIPS 140-2 standard. The General User role has limited privileges and access to limited services of the module. The General User can change his/her own personal identification number (PIN) and access all of the data stored within the storage device.

The cryptographic module supports up to 9 authenticated operators; at least one authenticated operator will be an Administrator.

7.2 Authentication

The cryptographic module requires a minimum of seven digits and maximum of sixteen digits for a personal identification number (PIN). When the module is powered on it will allow a maximum of 10 attempts to correctly enter the PIN code. The human that takes physical possession of the module and initializes the PIN for the first time is the Administrator.

Upon a total of ten failed authentication attempts (as described above), the module will lock the keypad and require a pre-defined command sequence to be entered to allow the Administrator or General User another ten attempts at entering the correct PIN code depending on the settings controlled by the Administrator when the device is setup.

If the module does not receive the correct PIN code within the maximum of 20 attempts (described above), all critical security parameters will be actively zeroized. In such case any encrypted data remaining on the external storage device(s) will be useless (unrecoverable).

Role	Type of Authentication	Authentication Data
Administrator (Cryptographic Officer)	Role-based	Personal Identification Number (PIN)
General User (User)	Role-based	Personal Identification Number (PIN)

Table 8 - Roles and Authentication Data

Authentication Mechanism	Strength of Mechanism
PIN code verification	A minimum seven digit PIN is used, with each digit selected from twenty possible characters. The twenty possible characters include the digits 0 to 9, and the additional SHIFT 0 to SHIFT 9 (e.g. SHIFT 0, SHIFT 1, SHIFT 2, etc.) Therefore the probability of a random attempt to authenticate to the module is 1/1,280,000,000 which is much less than 1/1,000,000. The probability of multiple consecutive attempts to authenticate to the module during a one minute period is 10/1,280,000,000 which is much less than 1/100,000.

Table 9 - Authentication Mechanisms and Strengths

8. Access Control Policy

The cryptographic module supports two roles: Administrator and General User. The type of services corresponding to each of the supported roles is described below.

Types of Access:

- Read: R
- Write: W
- Zeroize: Z
- N/A: Not applicable

Role			***Service***	***Cryptographic Keys and CSPs***	***Type of Access***
Administrator (Cryptographic Officer)	General User (User)	No Role Required (Unauthenticated services that are not security relevant and do not require an authorized/authenticated operator)			
X	X		Login/Unlock: authenticate operator to the module.	Admin PIN (or) User PIN	R
				AES Master Key	R
X	X		Logout/Lock: de-authenticate the operator and lockup the module.	N/A	N/A
X	X		Write Data: receive plaintext data from host, AES encrypt data to external storage, outside of the cryptographic boundary.	AES Master Key	R
X	X		Read Data: AES decrypt data from external storage, output plaintext to host outside of the cryptographic boundary.	AES Master Key	R
X	X		Change PIN: update the PIN.	Admin PIN	W
				User PIN	W
X			Set self-destruct: prepare the module for duress event.	Admin PIN	W
X			Self-destruct: reinitialize the module.	AES Master Key HASH DRBG Internal State HASH DRBG Seed Admin PIN User PIN Recovery PIN	Z
X			Delete all User PINs: overwrite and supersede all PINs.	User PIN Admin PIN Recovery PIN	W

X			Set unattended Auto lock: set idle timeout value in minutes.	N/A	N/A
X	X		Set read only: When set does not allow writing of data to the storage.	N/A	N/A
X			Set Lock override: Sets the device to ignore re-enumeration over the USB bus.	N/A	N/A
X			Create Recovery PINs: Admin set a PIN used create a user PIN.	User PIN	W
X	X		Use Recovery PIN: create a new User PIN.	User PIN	W
X			Setup Forced enrollment: Admin set the drive to require a PIN setup on next use.	N/A	N/A
X			Set Minimum PIN length: Admin setting for minimum digit length of PINs.	N/A	N/A
X			Set LED flicker: LED to flash when buttons are pressed.	N/A	N/A
X			Configurator: Setup the device over USB using Software.	Admin PIN User PIN Recovery PIN AES-CBC Decryption Key Client ECC CDH Public Key Client ECC CDH Private Key Client ECC CDH Shared Secret "Z" Client ECC CDH Secret Keying Material Host ECC CDH Public Key Client ECC CDH KDF Internal State HASH DRBG Internal State HASH DRBG Seed	R and W
X	X	X	Run Diagnostic mode: Verify proper keypad function and check firmware version.	N/A	N/A
X			Set Brute force attempts: Sets the number of tries before the drive will lock.	N/A	N/A
X	X	X	Self-Test: perform required power-up self-tests.	N/A	N/A
X	X	X	Get Status: status outputs.	N/A	N/A
X	X	X	Zeroize: destroy all CSPs.	AES Master Key	Z

				HASH DRBG Internal State HASH DRBG Seed Admin PIN User PIN Recovery PIN AES-CBC Decryption Key Client ECC CDH Public Key Client ECC CDH Private Key Client ECC CDH Shared Secret "Z" Client ECC CDH Secret Keying Material Host ECC CDH Public Key Client ECC CDH KDF Internal State	
X	X	X	User reset: reset the module and zeroize all CSPs.	AES Master Key HASH DRBG Internal State HASH DRBG Seed Admin PIN User PIN Recovery PIN AES-CBC Decryption Key Client ECC CDH Public Key Client ECC CDH Private Key Client ECC CDH Shared Secret "Z" Client ECC CDH Secret Keying Material Host ECC CDH Public Key Client ECC CDH KDF Internal State	Z

Table 10 – Roles, Services, CSPs, Types of Access

9. Physical Security Policy

Epoxy coating
The module is encapsulated with a hard, opaque, tamper-evident epoxy coating and an epoxy can.

Physical Security Mechanisms	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Hard, opaque, tamper-evident epoxy coating and epoxy can	In accordance with Administrator role organizational security policy.	Inspect the cryptographic boundary for scratches, gouges, scrapes, deformations, and any other suspicious signs of malice and tampering. If any evidence of tampering exists, the Administrator role is required to cease use of the cryptographic immediately.

Table 11 - Physical Security Mechanisms

10. Regulatory Compliance

The cryptographic module has been tested for and passes the following:

- EMI/EMC requirements specified by 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class B (i.e., for home use).

11. Security Rules

11.1 Initialization Period of the Cryptographic Module

The Administrator role is responsible for the overall security of the module and initializing the cryptographic module into the FIPS Approved mode of operation.

The Administrator shall perform one (1) of the following two (2) procedures to initialize the module into FIPS mode:

1. Power up the module by plugging into a powered USB port. The module will perform all power-up self-tests and flash the GREEN LED 3 times upon successful completion.
   a. The Blue and Green LEDs will glow solidly. Press UNLOCK + 9 at the same time. The BLUE LED will glow solidly and the GREEN LED will be blinking.
   b. Enter the series of numbers that you will use for the Admin PIN and press the UNLOCK button.
   c. Re-enter that same PIN and press the UNLOCK button again. The GREEN LED will illuminate for one second followed by the BLUE LED glowing solidly by itself.
   d. The module can be administered or press the lock key will revert to a standby state with the RED LED on solid.

2. Execute the “Configurator” service to perform the initialization of the module with the following settings:
   a. Amount of brute-force attempts of incorrect authentication data before the module locks: maximum of 10 attempts
   b. Minimum PIN length: 7 digits

Upon completion of the initialization period, the module’s LED status will indicate a solid RED LED.

The cryptographic module only supports a FIPS Approved mode of operation, therefore a non-compliant configuration is out of scope for this validation.

11.2 FIPS Approved Mode

- The cryptographic module shall always run in a FIPS Approved mode of operation (i.e. non-FIPS mode shall not be supported). It shall be possible to determine that the module is in FIPS mode by powering up the module (automatically invoking the self-tests) and observing LED status as follows: RED LED is solid on to indicate self-tests completed successfully; RED LED is flashing to indicate an error state, including failure of a power-up self-test as well as failure of a conditional self-test.
- The firmware revision can be determined by the following procedure:
    1. Power up the module by plugging in to a powered USB port.
    2. Push the Lock + 1 keys at the same time and release
    3. Push and hold the 0 key, the LED's will flash Red and Blue for 5 seconds then all the LEDs will come on for 1 second. Release the 0 key
    4. The LED's will flash the firmware revision:
        Example:
        a. 7 Blue LED blinks = 7
        b. Then 1 Red blinks = .
        c. 6 Blue Blinks = 6
        d. Then Red LED on solid = end of sequence
        This firmware revision shows 7.6
- The cryptographic module shall enforce separation of all data inputs, data outputs, control inputs, status outputs via defined ports and interfaces.
- The cryptographic module shall receive power via its defined power interface.
- The cryptographic module shall not support a maintenance interface or bypass capability.
- The cryptographic module shall not support the output of any cryptographic keys or CSPs in any form.
- During error states, the cryptographic module shall: enforce the inhibition of all data outputs, cease to provide any cryptographic or otherwise security relevant services, and provide non-security relevant error status.
- The cryptographic module shall support Role-based authentication.
- The cryptographic module shall provide a hard, opaque, tamper evident enclosure.
- The cryptographic module shall enforce a non-modifiable operational environment.
- The cryptographic module shall protect all critical security parameters from unauthorized disclosure, modification, and substitution.
- The cryptographic module shall provide a non-Approved non-deterministic hardware random number generator strictly for the purposes of seeding the Approved deterministic random bit generator.
- The cryptographic module shall not support manual key entry.
- The cryptographic module shall support zeroization to destroy all critical security parameters.
- The cryptographic module shall conform to applicable EMI/EMC requirements.
- The cryptographic module generates cryptographic keys whose strengths are a minimum 256 bits of entropy. As per IG A.9, the AES-XTS implementation verifies that Key_1 ≠ Key_2, before the keys are to be used.

- The cryptographic module shall perform all required self-tests:
    - Power-up Self-tests
        1. SHA-256 KAT
        2. SP 800-90A HASH DRBG KAT
        3. AES-XTS Encrypt KAT
        4. AES-XTS Decrypt KAT
        5. AES-CBC Decrypt KAT
        6. ECC CDH KAT
        7. Firmware integrity test (16-bit EDC)
    - Conditional Self-tests
        1. Continuous RNG test on Approved SP 800-90A HASH DRBG
        2. Continuous RNG test on non-Approved NDRNG for seeding the Approved SP 800-90A HASH DRBG
        3. ECC CDH Pairwise Consistency Test
        4. Firmware load test: N/A
        5. Manual key entry test: N/A
        6. Bypass test: N/A

12. Mitigation of Other Attacks Policy

The module is not designed to mitigate any specific attacks outside the scope of FIPS 140-2.

Other Attacks	Mitigation Mechanism	Specific Limitations
Not applicable	Not applicable	Not applicable

Table 12 - Mitigation of Other Attacks

13. Acronyms

- AES: Advanced Encryption Standard
- CBC: Cipher Block Chaining
- CMVP: Cryptographic Module Validation Program
- CSE: Communications Security Establishment
- CSP: Critical Security Parameters
- DRBG: Deterministic Random Bit Generator
- ECC CDH: Elliptic Curve Cryptography Cofactor Diffie-Hellman
- EDC: Error Detection Code
- EMI/EMC: Electromagnetic Interference/Electromagnetic Compatibility
- FIPS: Federal Information Processing Standards
- KAT: Known Answer Test
- LED: Light Emitting Diode
- NIST: National Institute of Standards and Technology
- NDRNG: Non-Deterministic Random Number Generator
- N/A: Not Applicable
- PIN: Personal Identification Numbers
- RNG: Random Number Generator
- SATA: Serial Advanced Technology Attachment
- SHA: Secure Hashing Algorithm
- USB: Universal Serial Bus
- XTS: XEX Tweakable Block Cipher with Ciphertext Stealing

Appendix A. Critical Security Parameters

The public keys, cryptographic keys, cryptographic key components, and CSPs used by the module are as follows:

1) AES Master Key
Description: 256-bit AES-XTS key used to encrypt/decrypt protected data
Generation: Internally using the SP 800-90A HASH DRBG
Establishment: N/A
Entry: N/A
Output: N/A
Storage: EEPROM
Zeroization: Actively overwritten via "Self-destruct", "User reset" and "Zeroize" services

2) User PIN
Description: 7 to 16 digit PIN; authentication data for the General User
Generation: Externally generated by the operator during module initialization
Establishment: N/A
Entry: Direct entry via keypad or AES-CBC encryption with AES-CBC Decryption Key via the "Configurator" service
Output: N/A
Storage: SHA-256 hash value stored in EEPROM
Zeroization: Actively overwritten via "Self-destruct", "Delete all User PINs", "User reset", "Change PIN" and "Zeroize" services

3) Admin PIN
Description: 7 to 16 digit PIN; authentication data for the Administrator
Generation: Externally generated by the operator during module initialization
Establishment: N/A
Entry: Direct entry via keypad or AES-CBC encryption with AES-CBC Decryption Key via the "Configurator" service
Output: N/A
Storage: SHA-256 hash value stored in EEPROM
Zeroization: Actively overwritten via "Self-destruct", "Delete all User PINs", "User reset", "Change PIN" and "Zeroize" services

4) Recovery PIN
Description: 7 to 16 digit PIN; authentication data for the General User/ Administrator
Generation: Externally generated by the operator during module initialization
Establishment: N/A
Entry: Direct entry via keypad or AES-CBC encryption with AES-CBC Decryption Key via the "Configurator" service
Output: N/A
Storage: SHA-256 hash value stored in EEPROM
Zeroization: Actively overwritten via “Self-destruct”, "Delete all User PINs", "User reset", "Change PIN" and "Zeroize" services

5) HASH DRBG Internal State
Description: 880-bit; Values of V and C of HASH DRBG mechanism

Generation: Internally using the SP 800-90A HASH DRBG
Establishment: N/A
Entry: N/A
Output: N/A
Storage: Plaintext in RAM
Zeroization: Actively overwritten via "Self-destruct", "User reset" and "Zeroize" services

6) HASH DRBG Seed
Description: 440-bit; Used only in generating the initial state of the SP 800-90A HASH DRBG
Generation: Internally using the SP 800-90A HASH DRBG
Establishment: N/A
Entry: N/A
Output: N/A
Storage: Plaintext in RAM
Zeroization: Actively overwritten via "Self-destruct", "User reset" and "Zeroize" services

7) AES-CBC Decryption Key
Description: 256-bit AES-CBC key used to decrypt protected data
Generation: Internally using Client's ECC CDH Key Derivation Function
Establishment: N/A
Entry: N/A
Output: N/A
Storage: Plaintext in RAM
Zeroization: Actively overwritten via "User reset", and "Zeroize" services

8) Client ECC CDH Public Key
Description: Client's P-256 SP 800-56A ECC CDH public key
Generation: calculated from ECC CDH Private Key
Establishment: N/A
Entry: N/A
Output: Plaintext
Storage: Plaintext in RAM
Zeroization: Actively overwritten via "User reset" and "Zeroize" services

9) Client ECC CDH Private Key
Description: Client's P-256 SP 800-56A ECC CDH private key
Generation: Internally using the SP 800-90A HASH DRBG
Establishment: N/A
Entry: N/A
Output: N/A
Storage: Plaintext in EEPROM
Zeroization: Actively overwritten via "User reset", and "Zeroize" services

10) Client ECC CDH Shared Secret "Z"
Description: Client's 256-bit SP 800-56A ECC CDH Shared Secret "Z" used in ECC CDH key agreement; Used as input to the Client ECC CDH Key Derivation Function
Generation: N/A
Establishment: ECC CDH Key Agreement as per SP 800-56A
Entry: N/A
Output: N/A
Storage: Plaintext in RAM

Zeroization: Actively overwritten via “User reset”, and “Zeroize” services

11) Client ECC CDH Secret Keying Material
Description: Client’s 256-bit secret keying material from the SP 800-56A KDF
Generation: N/A
Establishment: ECC CDH Key Agreement
Entry: N/A
Output: N/A
Storage: Plaintext in RAM
Zeroization: Actively overwritten via “User reset”, and “Zeroize” services

12) Host ECC CDH Public Key
Description: Host’s P-256 SP 800-56A ECC CDH Public Key
Generation: N/A
Establishment: N/A
Entry: Plaintext
Output: N/A
Storage: Plaintext in RAM
Zeroization: N/A

13) Client ECC CDH KDF Internal State
Description: Client's Internal state of the ECC CDH key derivation function (SHA-256)
Generation: N/A
Establishment: ECC CDH Key Agreement
Entry: N/A
Output: N/A
Storage: Plaintext in RAM
Zeroization: Actively overwritten via "User reset", and "Zeroize" services