FIPS 140-2 Non-Proprietary Security Policy
Aegis Secure Key 3Z Cryptographic Module
Author: Robert Davidson
Date: Tuesday, February 14, 2017
Document Issue: REV C, February 14, 2017

This document may be copied without the author’s permission, provided that it is copied in its entirety without any modification.

Apricorn is a trademark or a registered trademark of Apricorn in certain countries. All Apricorn product names and logos are trademarks or registered trademarks of Apricorn in certain countries. All other company and product names and logos are trademarks or registered trademarks of their respective owners in certain countries.
# Table of Contents

1. References .................................................................................................................. 3
2. Target Audience ......................................................................................................... 3
3. Introduction .................................................................................................................. 4
   3.1 Purpose of the Security Policy ................................................................................. 4
   3.2 Cryptographic Module Description ...................................................................... 4
4. Security Levels ............................................................................................................. 8
5. Interfaces and Ports .................................................................................................... 9
6. Cryptographic Key and CSP Management ................................................................. 9
   6.1 AES Master Key .................................................................................................... 9
   6.2 PIN Access Codes ................................................................................................. 9
   6.3 Random Number Generation .............................................................................. 9
   6.4 ECC CDH Key Establishment .............................................................................. 10
   6.5 Zeroization .......................................................................................................... 10
7. Identification and Authentication Policy ................................................................. 10
   7.1 Roles ...................................................................................................................... 10
   7.2 Authentication ...................................................................................................... 11
8. Access Control Policy ................................................................................................. 12
9. Physical Security Policy ............................................................................................. 15
10. Regulatory Compliance ............................................................................................. 15
11. Security Rules ............................................................................................................. 16
   11.1 Initialization Period of the Cryptographic Module ............................................. 16
   11.2 FIPS Approved Mode ......................................................................................... 17
12. Mitigation of Other Attacks Policy .......................................................................... 18
13. Acronyms ................................................................................................................... 19
Appendix A. Critical Security Parameters ....................................................................... 20
Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>Initial Public Release</td>
</tr>
<tr>
<td>1.1</td>
<td>Add firmware version 7.5</td>
</tr>
<tr>
<td>1.2</td>
<td>Add firmware version 7.7</td>
</tr>
</tbody>
</table>

1. References

<table>
<thead>
<tr>
<th>Author</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>NIST</td>
<td>FIPS PUB 140-2: Security Requirements For Cryptographic Modules, December, 2002</td>
</tr>
<tr>
<td>NIST</td>
<td>Derived Test Requirements for FIPS PUB 140-2, March, 2004</td>
</tr>
<tr>
<td>NIST</td>
<td>Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program, May, 2006</td>
</tr>
<tr>
<td>NIST</td>
<td>FIPS 197</td>
</tr>
<tr>
<td>NIST</td>
<td>FIPS 180-4</td>
</tr>
<tr>
<td>NIST</td>
<td>SP800-90A Revision 1</td>
</tr>
<tr>
<td>NIST</td>
<td>SP800-38E</td>
</tr>
</tbody>
</table>

Table 1 - 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 Aegis Secure Key 3Z 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 standalone cryptographic module. Specifically, the module is a USB 3.0 to Solid State Memory Module 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.

<table>
<thead>
<tr>
<th>Aegis Secure Key 3Z Cryptographic Module</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Firmware Version</strong></td>
</tr>
<tr>
<td><strong>Hardware Version</strong></td>
</tr>
<tr>
<td><strong>Part Numbers</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

Table 2 – Cryptographic Module Version
List of all Approved Security Functions:

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

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

Table 3 – 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:

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Caveat</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware NDRNG</td>
<td>N/A</td>
<td>Seeding for the HASH DRBG</td>
</tr>
</tbody>
</table>

Table 4 – List of all non-Approved but Allowed Security Functions
Figure 1 - Pictures of Aegis Secure Key 3Z Cryptographic Module
The cryptographic module is designed to meet FIPS 140-2 Level 3 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 Aegis Secure Key 3Z Cryptographic Module, represents the physical boundary of the device and the cryptographic boundary as outlined by the red marking.

**Aegis Secure Key 3Z Cryptographic Module Block Diagram**

Figure 2 – Aegis Secure Key 3Z Cryptographic Module Block Diagram
4. Security Levels

The cryptographic module meets an overall security of FIPS 140-2 Level 3. 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.

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

Table 5 – Security Levels
5. Interfaces and Ports

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

<table>
<thead>
<tr>
<th>Physical Port</th>
<th>Description</th>
<th>Logical Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>Super Speed Universal Serial Bus (USB 3.0)</td>
<td>Super Speed Universal Serial Bus Signals (USB 3.0)</td>
<td>Data Input/ Data Output/ Power</td>
</tr>
<tr>
<td>Keypad</td>
<td>External Keypad Control Input Signals</td>
<td>Control Input (manual controls)</td>
</tr>
<tr>
<td>LEDs output (Red, Blue, Green)</td>
<td>Signals output to External LEDs (Red, Blue, Green)</td>
<td>Status Output</td>
</tr>
</tbody>
</table>

Table 6 – Interfaces and Ports

6. Cryptographic Key and CSP Management

6.1 AES Master Key

The cryptographic module uses an AES Master Key (an AES 256-bit key) to encrypt/decrypt protected data. The AES 256-bit key is generated using the FIPS Approved deterministic random bit generator (SP800-90A 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, one User PIN, 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 that will overwrite the current 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 (SP800-90A HASH DRBG Cert #260). Continuous RNG tests are performed on the outputs of the NDRNG and on the outputs of the Approved SP800-90A 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 identity based authentication via verification of the PIN code for the Administrator role and General User role.

The human that takes physical possession of the module and initializes the PIN for the first time is the Administrator. 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 2 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).

<table>
<thead>
<tr>
<th>Role</th>
<th>Type of Authentication</th>
<th>Authentication Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator (Cryptographic Officer)</td>
<td>Identity-based</td>
<td>Personal Identification Number (PIN)</td>
</tr>
<tr>
<td>General User (User)</td>
<td>Identity-based</td>
<td>Personal Identification Number (PIN)</td>
</tr>
</tbody>
</table>

Table 7 - Roles and required authentication

<table>
<thead>
<tr>
<th>Authentication Mechanism</th>
<th>Strength of Mechanism</th>
</tr>
</thead>
<tbody>
<tr>
<td>PIN code verification</td>
<td>A minimum seven digit PIN is used, with each digit selected from 10 possible characters.</td>
</tr>
<tr>
<td></td>
<td>Therefore the probability of a random attempt to authenticate to the module is 1/10,000,000 which is much less than 1/1,000,000.</td>
</tr>
<tr>
<td></td>
<td>The probability of multiple consecutive attempts to authenticate to the module during a one minute period is 10/10,000,000 which is much less than 1/100,000.</td>
</tr>
</tbody>
</table>

Table 8 – Strengths of authentication mechanisms
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

<table>
<thead>
<tr>
<th>Role</th>
<th>Service</th>
<th>Cryptographic Keys and CSPs</th>
<th>Type of Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator (Cryptographic Officer)</td>
<td>Login/Unlock: authenticate operator to the module.</td>
<td>Admin PIN (or) User PIN</td>
<td>R</td>
</tr>
<tr>
<td>General User (User)</td>
<td>Logout/Lock: de-authenticate the operator and lockup the module.</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Administrator (Cryptographic Officer)</td>
<td>Write Data: receive plaintext data from host, AES encrypt data to external storage, outside of the cryptographic boundary.</td>
<td>AES Master Key</td>
<td>R</td>
</tr>
<tr>
<td>General User (User)</td>
<td>Read Data: AES decrypt data from external storage, output plaintext to host outside of the cryptographic boundary.</td>
<td>AES Master Key</td>
<td>R</td>
</tr>
<tr>
<td>General User (User)</td>
<td>Change PIN: update the PIN.</td>
<td>Admin PIN</td>
<td>W</td>
</tr>
<tr>
<td>General User (User)</td>
<td>Set self-destruct: prepare the module for duress event.</td>
<td>Admin PIN</td>
<td>W</td>
</tr>
<tr>
<td>General User (User)</td>
<td>Self-destruct: reinitialize the module.</td>
<td>AES Master Key</td>
<td>Z</td>
</tr>
</tbody>
</table>

© Apricorn, Inc.  February 14, 2017  Page 12 of 22
<table>
<thead>
<tr>
<th></th>
<th></th>
<th>Delete all User PINs: overwrite and supersede all PINs.</th>
<th>User PIN Admin PIN Recovery PIN</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td></td>
<td>Set unattended Auto lock: set idle timeout value in minutes.</td>
<td>N/A N/A</td>
</tr>
<tr>
<td>X</td>
<td>X</td>
<td>Set read only: When set does not allow writing of data to the storage.</td>
<td>N/A N/A</td>
</tr>
<tr>
<td>X</td>
<td></td>
<td>Set Lock override: Sets the device to ignore re-enumeration over the USB bus.</td>
<td>N/A N/A</td>
</tr>
<tr>
<td>X</td>
<td></td>
<td>Create Recovery PINs: Admin set a PIN used create a user PIN.</td>
<td>User PIN W</td>
</tr>
<tr>
<td>X</td>
<td>X</td>
<td>Use Recovery PIN: create a new User PIN.</td>
<td>User PIN W</td>
</tr>
<tr>
<td>X</td>
<td></td>
<td>Setup Forced enrollment: Admin set the drive to require a PIN setup on next use.</td>
<td>N/A N/A</td>
</tr>
<tr>
<td>X</td>
<td></td>
<td>Set Minimum PIN length: Admin setting for minimum digit length of PINs.</td>
<td>N/A N/A</td>
</tr>
<tr>
<td>X</td>
<td></td>
<td>Set LED flicker: LED to flash when buttons are pressed.</td>
<td>N/A N/A</td>
</tr>
<tr>
<td>X</td>
<td></td>
<td>Configurator: Setup the device over USB using Software.</td>
<td>Admin PIN User PIN Recovery PIN HASH DRBG Internal State HASH DRBG Seed 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 R and W</td>
</tr>
<tr>
<td>X</td>
<td>X</td>
<td>Run Diagnostic mode: Verify proper keypad function and check firmware version.</td>
<td>N/A N/A</td>
</tr>
<tr>
<td>X</td>
<td></td>
<td>Set Brute force attempts: Sets the number of tries before the drive will lock.</td>
<td>N/A N/A</td>
</tr>
<tr>
<td>X</td>
<td>X</td>
<td>X</td>
<td>Self-Test: perform required power-up self-tests.</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>------------------------------------------</td>
</tr>
<tr>
<td>X</td>
<td>X</td>
<td>X</td>
<td>Get Status: status outputs.</td>
</tr>
<tr>
<td>X</td>
<td>X</td>
<td>X</td>
<td>Zerize: destroy all CSPs.</td>
</tr>
<tr>
<td>X</td>
<td>X</td>
<td>X</td>
<td>User reset: reset the module and zeroize all CSPs.</td>
</tr>
</tbody>
</table>

Table 9 – Roles, Services, CSPs, Types of Access
9. Physical Security Policy

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

Note: The module hardness testing was only performed at an ambient, single temperature (i.e. 73.4°F) and no assurance is provided for Level 3 hardness conformance at any other temperature.

<table>
<thead>
<tr>
<th>Physical Security Mechanisms</th>
<th>Recommended Frequency of Inspection/Test</th>
<th>Inspection/Test Guidance Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hard, opaque, tamper-evident epoxy coating</td>
<td>In accordance with Administrator role organizational security policy.</td>
<td>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 module immediately.</td>
</tr>
</tbody>
</table>

Table 10 – Physical Security

10. Regulatory Compliance

The cryptographic module has been tested for and passes the following:
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. Wake up the module by pressing the Unlock button, the BLUE and GREEN LEDs will glow solidly.
   a. 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. Push the Lock button.

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. Push the Unlock button to bring the module out of a sleep state or plug into 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 blink = .
     c. Then 7 Blue blink = 7
     d. Then Red LED on solid = end of sequence
     This firmware revision shows 7.7

- 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 Identity-based authentication.
- The Administrator and General User roles are explicitly prohibited from sharing PINs with any other operator. In the event that the Administrator role share’s his or her PIN, the cryptographic module is deemed non-compliant and unfit for service to protect sensitive but unclassified data.
- 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:
  o Power-up Self-tests
    1. SHA-256 KAT
    2. SP800-90A 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)
  o Conditional Self-tests
    1. Continuous RNG test on Approved SP800-90A HASH DRBG
    2. Continuous RNG test on non-Approved NDRNG for Approved SP800-90A 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.

<table>
<thead>
<tr>
<th>Other Attacks</th>
<th>Mitigation Mechanism</th>
<th>Specific Limitations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not applicable</td>
<td>Not applicable</td>
<td>Not applicable</td>
</tr>
</tbody>
</table>

Table 10 – Mitigation of Other Attacks
13. Acronyms

- AES: Advanced Encryption Standard
- CBC: Cipher Block Chaining
- CMVP: Cryptographic Module Validation Program
- CSEC: Communications Security Establishment Canada
- 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  
Enter: 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  
Enter: 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  
Enter: 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  
Enter: 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  
Enter: 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