FIPS 140-2 Non-Proprietary Security Policy
Aegis Secure Key 3.0 Cryptographic Module

Author: Robert Davidson
Date: Friday, May 13, 2016
Document Issue: REV C May 13, 2016

Table of Contents

Revision History	
Version 1.0	Initial Public Release
Version 1.1	Addition of Firmware Version 6.5.1
Version 1.2	Addition of Appendix A

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	SP800-90A Revision 1
NIST	SP800-38E

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 3.0 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.

Aegis Secure Key 3.0	
Firmware Version	6.5 and 6.5.1
Hardware Part Number	RevD

Table 2 – Cryptographic Module Version

List of all Approved Security Functions:

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

- Random number generation (SP800-90A HASH DRBG – 256 Cert. #260)
- Symmetric encryption/decryption (AES-XTS Cert. #2235)
- Secure hash (SHA 256 Cert. #1911)

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 Security Functions:

- Non-deterministic hardware random number generation (for seeding Approved DRBG)
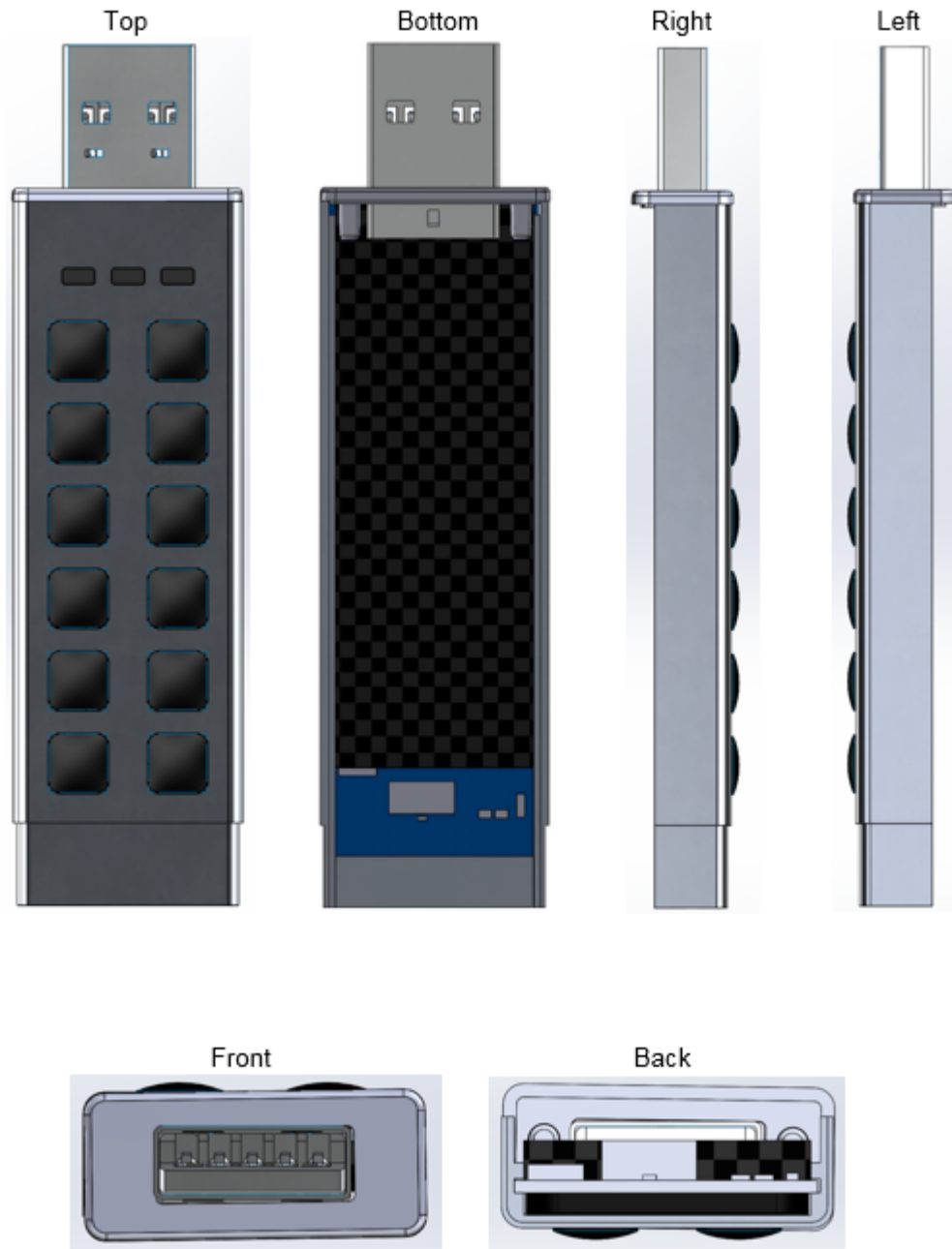
Figure 1 - Pictures of Aegis Secure Key 3.0 Cryptographic module

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 Apricorn Encryption Module, represents the physical boundary of the device and the cryptographic boundary as outlined by the red marking.

Figure 2 – Apricorn Secure Key 3.0 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.

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

Table 3 – 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	Logical Interface
Super Speed Universal Serial Bus (USB 3.0)	Data Input/ Data Output/ Power
Keypad	Control Input (manual controls)
SATA	Data Input/ Data Output/ Power
LEDs output (Red, Blue, Green)	Status Output

Table 4 – Interfaces and Ports

6. Cryptographic Key and CSP Management

6.1 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 Administrator PIN and one General User PIN code.

6.2 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.

Note: the minimum number of bits of entropy generated by the module for use in key generation is 256512.

6.3 AES Master Key

The cryptographic module uses 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).

6.4 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 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.

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)	Identity-based	Personal Identification Number (PIN)
General User (User)	Identity-based	Personal Identification Number (PIN)

Table 5 - Roles and required authentication

Authentication Mechanism	Strength of Mechanism
PIN code verification	A minimum seven digit PIN is used, with each digit selected from 10 possible characters. 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. 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.

Table 6 – 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

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.	Admin PIN User PIN AES Master Key DRBG Internal State	Z
X			Delete all User PINs: overwrite and supersede all PINs	User PIN Admin PIN	W
X			Set unattended: set idle timeout value in minutes.	N/A	N/A
X	X	X	Set read only: Sets the device to only all reading of the data	N/A	N/A
X			Set Lock override: Sets the device to ignore re-	N/A	N/A

			enumeration over the USB bus		
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 DRBG Internal State Admin PIN User PIN	Z
X	X	X	User reset: reset the module and zeroize all CSPs	AES Master Key DRBG Internal State Admin PIN User PIN	Z

Table 7 – 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 a single temperature and no assurance is provided for Level 3 hardness conformance at any other temperature.

Physical Security Mechanisms	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Hard, opaque, tamper-evident epoxy coating	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 module immediately.

Table 8 – Physical Security

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

- 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 permanently to indicate an error state.

- While the key is attached to a computer and unlocked, the firmware version can be determined by the "Get Status" service via the following procedures:

  o **Windows Operating Systems**
    1. Open *Devices and Printers* from *Control Panel*
    2. Right Click on the "Secure Key 3.0" and select *properties*
    3. Open the *Hardware* tab and click the *properties* button
    4. Open the *Details* tab and select the *Hardware Ids* category from the dropdown menu
    5. The firmware version can be identified as the topmost *value* as follows:
        A. **For firmware version 6.5:**
           "USBSTOR\DiskApricornSecure_Key_3.0__**0306**"

        B. **For firmware version 6.5.1:**
           "USBSTOR\DiskApricornSecure_Key_3.0__**0308**"

  o **OSX Operating Systems**
    1. Go to the Apple Menu in the top-left corner and select *About This Mac*
    2. Click the *System Report* button
    3. Under the "Hardware" column, select *USB* and then select *Secure Key 3.0* from the "USB Device Tree" pane on the right
    4. The firmware version can be determined as follows:
        A. **For firmware version 6.5**:
           "**3.06**" will be shown in the "Version" field

        B. **For firmware version 6.5.1:**
           "**3.08**" will be shown in the "Version" field

  o **Linux Operating Systems**
    1. Open the *Gnome Disk* Utility
    2. Select the "Apricorn Secure Key 3.0" disk drive from the list of "Devices"
    3. The firmware version can be determined as follows:
        A. **For firmware version 6.5:**
           "Apricorn Secure Key 3.0 (**0306**)" will be shown in the "Model" field

        B. **For firmware version 6.5.1:**
           "Apricorn Secure Key 3.0 (**0308**)" will be shown in the "Model" field

- 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 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 or any other type of key entry/output.
- 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 shall perform all required self-tests:
  - Power-up Self-tests
    1. SHA-256 KAT
  - SP800-90A HASH DRBG KAT
    1. AES-XTS Encrypt KAT
    2. AES-XTS Decrypt KAT
    3. Firmware integrity test (16-bit EDC)
  - Conditional Self-tests
    1. Continuous RNG test on Approved SP800-90A HASH DRBG
    2. Continuous RNG test on non-Approved NDRNG
    - Firmware load test: N/A
    - Manual key entry test: N/A
    - Pairwise consistency test: N/A
    - 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 8 – Mitigation of Other Attacks

13. Acronyms

- AES: Advanced Encryption Standard
- CMVP: Cryptographic Module Validation Program
- CSEC: Communications Security Establishment Canada
- CSP: Critical Security Parameters
- DRBG: Deterministic Random Bit Generator
- 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

1). AES Master Key
Description: AES XTS 256-bit used to encrypt/decrypt protected data
Generation: Internally using the SP800-90 HASH DRBG
Entry: N/A
Output: N/A
Zeroization: Actively overwritten via "Self-destruct", "User reset" and "Zeroize" services

2). User and Admin PIN
Description: 7 to 16 digit PIN; authentication data for the General User/ Administrator
Generation: Externally generated by the operator during module initialization
Entry: Direct entry via keypad
Output: N/A
Zeroization: Actively overwritten via "Self-destruct", "Delete all User PINs", "User reset", "Change PIN" and "Zeroize" services

3). DRBG Internal State
Description: Values of V and C of HASH DRBG mechanism
Generation: Internally using the SP800-90 HASH DRBG
Entry: N/A
Output: N/A
Zeroization: Actively overwritten via "Self-destruct", "User reset" and "Zeroize" services