FIPS 140-2 Non-Proprietary Security Policy
Aegis Fortress L3 Cryptographic Module

Author: Victor Nguyen
Date: 2019-12-19
Document Issue: 1.3

Table of Contents

Revision History	
1.0	Original Release
1.1	Minor updates per CMVP comments
1.2	Minor updates per CMVP comments
1.3	Minor update per CMVP comment

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, January, 2011
NIST	Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program, February, 2019
NIST	FIPS 197
NIST	FIPS 180-4
NIST	SP800-90A Revision 1
NIST	SP800-38E
NIST	SP800-56A

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 Aegis Fortress L3 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 Aegis Fortress L3 cryptographic module is a multi-chip standalone cryptographic module. Specifically, the module is a USB 3.1 to Data Storage 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 an embedded alpha-numeric keypad whereby the authorized operator inputs a personal identification number (PIN) to access and unlock the secured data. Three (3) LEDs, each a different color, indicate the module status during authentication and operation.

Electronic components containing all critical security parameters (CSPs) are encapsulated within a hard, opaque, tamper-evident, production-grade epoxy. The module also incorporates a strong, tamper-resistant, non-removable, hard metal enclosure that defines the cryptographic boundary.

This software-free, embedded authentication approach allows the module to work with any mass storage compliant operating system whether it has a keyboard or not, and never shares any CSPs with the host.

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 after the initial setup instructions in Section 11.1 are performed (i.e., non-FIPS mode is not supported).

The Aegis Fortress L3 Cryptographic Module (Figure 1 below), represents the physical boundary of the device and the cryptographic boundary as outlined by the red marking.

Figure 1 - Aegis Fortress L3 Cryptographic Module

Aegis Fortress L3 Cryptographic Module	
Firmware Version	3.1
Hardware Version	Rev A
Part Numbers	AFL3-500 AFL3-1TB AFL3-2TB AFL3-3TB* AFL3-4TB* AFL3-5TB* AFL3-S500 AFL3-S1TB AFL3-S2TB AFL3-S4TB AFL3-S8TB* AFL3-S16TB*
** 24.5mm enclosure*	

Table 3 – Cryptographic Module 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
C 556	AES	SP 800-38E	XTS ECB	256-bits	Data Encryption / Decryption Note: XTS mode is only approved for storage applications, and AES-XTS-128 is NOT supported by the cryptographic module.
C 555	AES	SP 800-38A	CBC	256-bits	Data Decryption
Vendor Affirmed	CKG	SP 800-133 Rev 1	Non-modified output		Key Generation Sections 5.2 Key Pairs for Key Establishment, 6.1 “Direct Generation” of Symmetric Keys, 6.3 Symmetric Keys Generated Using Key-Agreement Schemes
C 656	DRBG	SP 800-90A Revision 1	HASH_Based DRBG (SHA-256)	Security strength is 256 bits	Deterministic Random Bit Generation
C 570	ECDSA	FIPS 186-4	PKG, PKV	P-256	Prerequisite to KAS
C 570	KAS EC-DH	SP 800-56A	ECC	P-256	Key Agreement
C 568	SHS	FIPS 180-4	SHA-256		Message Digest

Table 4 – List of All Approved Security Functions

List of all non-Approved but Allowed Security Functions:

Algorithm	Use
Hardware NDRNG	Seeding for the HASH DRBG with 256 bits of security. A 1024-bit seed is used.

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

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 6 – FIPS Security Levels

5. Interfaces and Ports

There are three physical ports on the cryptographic module: a Super Speed Universal Serial Bus (USB 3.1), a Keypad, and three external status LEDs.

Physical Port	Description	Logical Interface
Super Speed Universal Serial Bus (USB 3.1)	Super Speed Universal Serial Bus Signals (USB 3.1)	Data Input/ Data Output/ Power/ Control Input/ Status Output
Keypad	Keypad Input	Data Input/ Control Input (manual controls)
LEDs output (Red, Blue, Green)	Output LEDs	Status Output

Table 7 – 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.

6.2 PIN Access Codes

On the cryptographic module, each personal identification number (PIN) has a minimum of seven (7) digits and maximum of sixteen digits. The module supports one Admin PIN, one User PIN, one Self-Destruct 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.

The Self-Destruct PIN zeroizes all PINs and the AES Master Key, then resets to a new AES Master Key and new Admin 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. Continuous RNG tests are performed on the outputs of the NDRNG.

The HASH DRBG Internal State (V and C) is the DRBG's working state.

The HASH DRBG Seed is used to seed the DRBG. The seed is 1024 bits and includes the Entropy Input and Nonce.

6.4 EC DH Key Establishment

AES-CBC Decryption Key (AES-256) is used to decrypt the data sent from the host.

Client ECDH Public Key (P-256) is used to create secure communication with the host.

Client ECDH Private Key (P-256) is used to create a public key and shared secret.

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

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

Host ECDH Public Key (P-256) is used to create secure communication with the Client.

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

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 individual 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, set or modify all device settings, 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 the data stored within the storage device.

The cryptographic module supports up to two (2) authenticated operators; at least one authenticated operator will be an Administrator.

7.2 Authentication

The cryptographic module requires a minimum of seven (7) digits and maximum of sixteen (16) digits for a personal identification number (PIN). When the module is powered on, it will allow a maximum of ten (10) attempts to correctly enter the PIN code. The individual that takes physical possession of the module and initializes the PIN for the first time is the Administrator.

Upon a total of ten (10) consecutive failed authentication attempts (as described above), the module will lock the keypad and require a pre-defined command sequence (found in the module's user manual) to be entered to allow the Administrator or General User another ten (10) attempts at entering the correct PIN code depending on the settings controlled by the Administrator when the device is setup. Brute Force setting is programmable between 4 - 20 consecutive failed attempts.

If the module does not receive the correct PIN code within the maximum of twenty (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)
	Identity-based	EC Diffie-Hellman
General User (User)	Identity-based	Personal Identification Number (PIN)

Table 8 - Roles and required authentication

Authentication Mechanism	Strength of Mechanism
PIN code verification	A minimum seven-digit PIN is used, with each digit selected from ten (10) possible characters. There are 10^7 (ten million) possible PIN combinations. 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 20/10,000,000 which is much less than 1/100,000.
EC Diffie-Hellman	Since EC Diffie-Hellman with P-256 is used, the probability that a random attempt to authenticate to the module is 1/(2^128) which is much less than 1/1,000,000. Five (5) authentication attempts are allowed before a reboot must occur and a reboot takes approximately 10 seconds, therefore there could be ~30 attempts per minute. Given this, the probability of multiple consecutive attempts to authenticate to the module during a one-minute period is 30/(2^128) which is much less than 1/100,000.

Table 9 – Strengths of authentication mechanisms

8. Access Control Policy

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

Administrator	General User	Unauthenticated	*Service*	*Description*
X	X		Login/Unlock	Authenticates the operator to the module.
X	X		Logout/Lock	De-authenticates the operator and locks the module.
X	X		Write Data	Receive plaintext data from the host and AES XTS encrypt the data to internal storage.
X	X		Read Data	AES XTS decrypt data from internal storage and output plaintext data to the host.
X	X		Establish User PIN	Establish a User PIN if to create a general user role.
X	X		Change PIN	Update the PIN.
X			Set self-destruct	Enable the self-destruct feature.
X	X		Set self-destruct PIN	Prepare the module for duress event.
X	X		Self-destruct	Reinitialize the module.
X			Delete all User PINs	Overwrite and supersede all PINs.
X			Set unattended Auto lock	Set idle timeout value in minutes.
X	X		Set read only	When set does not allow writing of data to the storage. If the Admin sets the device to read only, the user is prevented from overriding this setting.
X			Set Lock override	Sets the device to ignore re-enumeration over the USB bus.
X			Create Recovery PINs	Admin sets a PIN used to create a recovery PIN.
X	X		Use Recovery PIN	Create a new User PIN after using the recovery PIN.
X			Setup Forced enrollment	Admin sets the drive to require a PIN setup on the next use.
X			Set Minimum PIN length	Admin setting for minimum digit length of PINs.
X			Set LED flicker	LED to flash when buttons are pressed.
X*			Configurator	Send configuration data to device from host pc.
X	X	X	Run Diagnostic mode	Verify proper keypad function and check firmware version.
X			Set Brute force attempts	Sets the number of tries before the drive will lock.
X	X	X	Self-Test	Perform required power-up self-tests.
X	X	X	Get Status	Status outputs.
X*			Zeroize	Destroy all CSPs.
X	X	X	User reset	Reset the module and zeroize all CSPs.

*Note: These Admin services use the EC Diffie-Hellman authentication scheme. All others use the PIN.

Table 10 – Roles and Services

The below table shows the how CSPs and Public Keys are accessed by the module's services. The modes of access shown in the table are defined as:

- G = Generate: The service generates or derives the CSP.
- I = Input: The service inputs the CSP from outside of the module.
- O = Output: The service outputs the CSP to outside of the module.
- E = Execute: The service uses the CSP.
- S = Store: The service stores the CSP persistently.
- Z = Zeroize: The service zeroizes the CSP.

	CSPs and Public Keys													
Service	AES Master Key	User PIN	Admin PIN	Recovery PIN	Self-Destruct PIN	HASH DRBG Internal State	HASH DRBG Seed	AES-CBC Decryption Key	Client ECDH Public Key	Client ECDH Private Key	Client ECDH Shared Secret "Z"	Client ECDH Secret Keying Material	Host ECDH Public Key	Client ECDH KDF Internal State
Login/Unlock	E	IE	IE	-	-	-	-	-	-	-	-	-	-	-
Logout/Lock	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Write Data	E	-	-	-	-	-	-	-	-	-	-	-	-	-
Read Data	E	-	-	-	-	-	-	-	-	-	-	-	-	-
Establish User PIN	-	IGES	IGES	-	-	-	-	-	-	-	-	-	-	-
Change PIN	-	ZIGES	ZIGES	-	-	-	-	-	-	-	-	-	-	-
Set self-destruct	-	-	-	-	Z	-	-	-	-	-	-	-	-	-
Set self-destruct PIN	-	-	-	-	IGES	-	-	-	-	-	-	-	-	-
Self-destruct	ZGES	Z	ZGS	Z	ZIE	ZGE	G	-	-	-	-	-	-	-
Delete all User PINs	-	Z	-	Z	Z	-	-	-	-	-	-	-	-	-
Set unattended Auto lock	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Set read only	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Set Lock override	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Create Recovery PINs	-	-	-	IS	-	-	-	-	-	-	-	-	-	-
Use Recovery PIN	-	ZIGS	-	IEZ	-	-	-	-	-	-	-	-	-	-
Setup Forced enrollment	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Set Minimum PIN length	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Set LED flicker	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Configurator	-	IS	IS	IS	IS	GE	G	E	GEO	E	GE	GE	EI	GE
Run Diagnostic mode	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Set Brute force attempts	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Self-Test	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Get Status	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Zeroize	Z	Z	Z	Z	Z	Z	Z	Z	Z	-	Z	Z	-	Z
User reset	ZGS	Z	Z	Z	Z	ZGE	ZG	Z	Z	ZG	Z	Z	-	Z

Table 11 – CSP and Public Key Access by Service

9. Physical Security Policy

Epoxy coating
The module incorporates a hard, opaque, tamper-evident, production-grade epoxy coating encapsulating all electrical components containing critical security parameters. Attempts to remove the epoxy will cause damage to these components.

Tamper-Resistance
The module incorporates a strong, tamper-resistant, non-removable, hard metal enclosure that defines the cryptographic boundary.

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. The internal epoxy coating was not tested as the module meets FIPS Level 3 requirements with the outer metal case.

Physical Security Mechanisms	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Hard, opaque, tamper-evident, production-grade metal enclosure	In accordance with the Administrator's organizational security policy or every three (3) months	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 12 – 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.

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 plugging the device into a USB port to power up. 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 ten (10) attempts
   b. Minimum PIN length: seven (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 always runs in a FIPS Approved mode of operation (i.e., non-FIPS mode is not supported). It is 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 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 LEDs will flash Red and Blue for 5 seconds then all the LEDs will come on for 1 second. Release the 0 key
    4. The LEDs will flash the firmware revision:
        Example:
        a. 3 Blue LED blinks = 3
        b. Then 1 Red blink = **.**
        c. Then 1 Blue blink = 1 (if zero, then no blue blinks)
        d. Then Red LED on solid = end of sequence
        This firmware revision shows **3.1**
- The cryptographic module enforces separation of all data inputs, data outputs, control inputs, status outputs via defined ports and interfaces.
- The cryptographic module receives power via its defined power interface.
- The cryptographic module does not support a maintenance interface or bypass capability.
- The cryptographic module does not support the output of any cryptographic keys or CSPs in any form.
- During the error state, the cryptographic module: enforces the inhibition of all data outputs, ceases to provide any cryptographic or otherwise security relevant services, and provides non-security relevant error status.
- The cryptographic module supports 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 shares his or her PIN, the cryptographic module is deemed non-compliant and unfit for service to protect sensitive but unclassified data.
- The cryptographic module incorporates a strong, tamper-resistant, non-removable, hard metal enclosure that defines the cryptographic boundary.
- The cryptographic module enforces a non-modifiable operational environment.

- The cryptographic module protects all critical security parameters from unauthorized disclosure, modification, and substitution.
- The cryptographic module provides a non-Approved non-deterministic hardware random number generator strictly for the purposes of seeding the Approved deterministic random bit generator.
- The cryptographic module does not support manual key entry.
- The cryptographic module supports zeroization to destroy all critical security parameters. All CSPs are destroyed with the User Reset service.
- The cryptographic module conforms 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 performs all required self-tests:
    - Power-up Self-tests
        1. SHA-256 KAT
        2. SP800-90A HASH DRBG KAT and Health Check
        3. AES-XTS Encrypt KAT
        4. AES-XTS Decrypt KAT
        5. AES-CBC Decrypt KAT
        6. SP 800-56A Self-tests per IG 9.6 (includes Primitive Z test and KDF KAT; prerequisites are tested separately with SHA and DRBG KATs)
        7. Firmware integrity test (16-bit CRC)
    - Conditional Self-tests
        1. NDRNG Continuous Test
        2. ECDH Pairwise Consistency Test
        3. SP 800-56A conditional tests per IG 9.6 (includes assurances per SP 800-56A sections 5.5.2 & 5.6.2.3 and ECDH pairwise consistency test)
        4. DRBG Continuous Test: N/A as allowed by IG 9.8
        5. Firmware load test: N/A
        6. Manual key entry test: N/A
        7. 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 13 – 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
- CRC: Cyclic Redundancy Check
- DRBG: Deterministic Random Bit Generator
- ECDH: Elliptic Curve Diffie-Hellman
- 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
- SHA: Secure Hashing Algorithm
- USB: Universal Serial Bus
- XTS: XEX Tweakable Block Cipher with Ciphertext Stealing