



Apricorn

Aegis Secure Key 3.0 Cryptographic Module

FIPS 140-3 Non-Proprietary Security Policy

Document Version: 1.1
Date: September 3, 2026



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 General	5
1.1 Overview	5
1.2 Security Levels	5
2 Cryptographic Module Specification	5
2.1 Description	5
2.2 Tested and Vendor Affirmed Module Version and Identification	8
2.3 Excluded Components	10
2.4 Modes of Operation	10
2.5 Algorithms	10
2.6 Security Function Implementations	12
2.7 Algorithm Specific Information	13
2.8 RBG and Entropy	13
2.9 Key Generation	13
2.10 Key Establishment	13
2.11 Industry Protocols	14
2.12 Additional Information	14
3 Cryptographic Module Interfaces	14
3.1 Ports and Interfaces	14
3.2 Trusted Channel Specification	14
4 Roles, Services, and Authentication	15
4.1 Authentication Methods	15
4.2 Roles	16
4.3 Approved Services	16
4.4 Non-Approved Services	24
4.5 External Software/Firmware Loaded	24
5 Software/Firmware Security	24
5.1 Integrity Techniques	24
5.2 Initiate on Demand	24
6 Operational Environment	24
6.1 Operational Environment Type and Requirements	24
7 Physical Security	24
7.1 Mechanisms and Actions Required	25
7.2 EFP/EFT Information	25
7.3 Hardness Testing Temperature Ranges	25
8 Non-Invasive Security	25

9 Sensitive Security Parameters Management.....	25
9.1 Storage Areas	25
9.2 SSP Input-Output Methods	26
9.3 SSP Zeroization Methods	26
9.4 SSPs	27
10 Self-Tests.....	32
10.1 Pre-Operational Self-Tests	32
10.2 Conditional Self-Tests.....	32
10.3 Periodic Self-Test Information.....	33
10.4 Error States	34
10.5 Operator Initiation of Self-Tests	36
11 Life-Cycle Assurance	36
11.1 Installation, Initialization, and Startup Procedures.....	36
11.2 Administrator Guidance	37
11.3 Non-Administrator Guidance.....	38
11.4 Design and Rules	38
11.5 End of Life	39
12 Mitigation of Other Attacks	40

List of Tables

Table 1: Security Levels	5
Table 2: Tested Module Identification – Hardware	8
Table 3: Modes List and Description	10
Table 4: Approved Algorithms	11
Table 5: Vendor-Affirmed Algorithms	11
Table 6: Security Function Implementations	13
Table 7: Entropy Certificates	13
Table 8: Entropy Sources	13
Table 9: Ports and Interfaces	14
Table 10: Authentication Methods	16
Table 11: Roles	16
Table 12: Approved Services	24
Table 13: Mechanisms and Actions Required	25
Table 14: EFP/EFT Information	25
Table 15: Hardness Testing Temperatures	25
Table 16: Storage Areas	26
Table 17: SSP Input-Output Methods	26
Table 18: SSP Zeroization Methods	27
Table 19: SSP Table 1	29
Table 20: SSP Table 2	32
Table 21: Pre-Operational Self-Tests	32
Table 22: Conditional Self-Tests	33
Table 23: Pre-Operational Periodic Information	33
Table 24: Conditional Periodic Information	34
Table 25: Error States	35

List of Figures

Figure 1: Cryptographic Boundary and TOEPP	7
Figure 2: Block Diagram	8

1 General

1.1 Overview

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 140-3.

1.2 Security Levels

Section	Title	Security Level
1	General	3
2	Cryptographic module specification	3
3	Cryptographic module interfaces	3
4	Roles, services, and authentication	3
5	Software/Firmware security	3
6	Operational environment	N/A
7	Physical security	3
8	Non-invasive security	N/A
9	Sensitive security parameter management	3
10	Self-tests	3
11	Life-cycle assurance	3
12	Mitigation of other attacks	N/A
	Overall Level	3

Table 1: Security Levels

2 Cryptographic Module Specification

2.1 Description

Purpose and Use:

The cryptographic module is a multi-chip standalone cryptographic module. Specifically, the module is a USB to Solid State Memory Module which implements hardware-based authenticated encryption.

The module provides secure encrypted (XTS-AES-256) storage and ensures 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 critical security parameters (CSPs) are encapsulated within a hard, opaque, tamper-evident, production-grade epoxy. The modules also incorporate a strong, tamper-resistant, non-removable, hard metal enclosure that defines the cryptographic boundary.

This software-free, embedded authentication approach allows the module to be agnostic to the operating system running on the host.

The cryptographic module is designed to meet FIPS 140-3 Level 3 cryptographic module requirements for the storage of user credentials and file systems. The modules will only operate in the “Approved” mode of operation. They must be configured according to the initial setup instructions in Section 11.1 before being operational. A non-Approved mode is not supported.

Module Type: Hardware

Module Embodiment: Multi-Chip Standalone

Cryptographic Boundary:

The entire physical module boundary (including the USB port) is the boundary of the cryptographic module

Tested Operational Environment’s Physical Perimeter (TOEPP):

The TOEPP of the module is the same as the physical cryptographic boundary. The Aegis Secure Key 3.0 (ASK3) is a level 3 multi-chip standalone module, and as such the perimeter of the tested operational environment is the entire module



Figure 1: Cryptographic Boundary and TOEPP

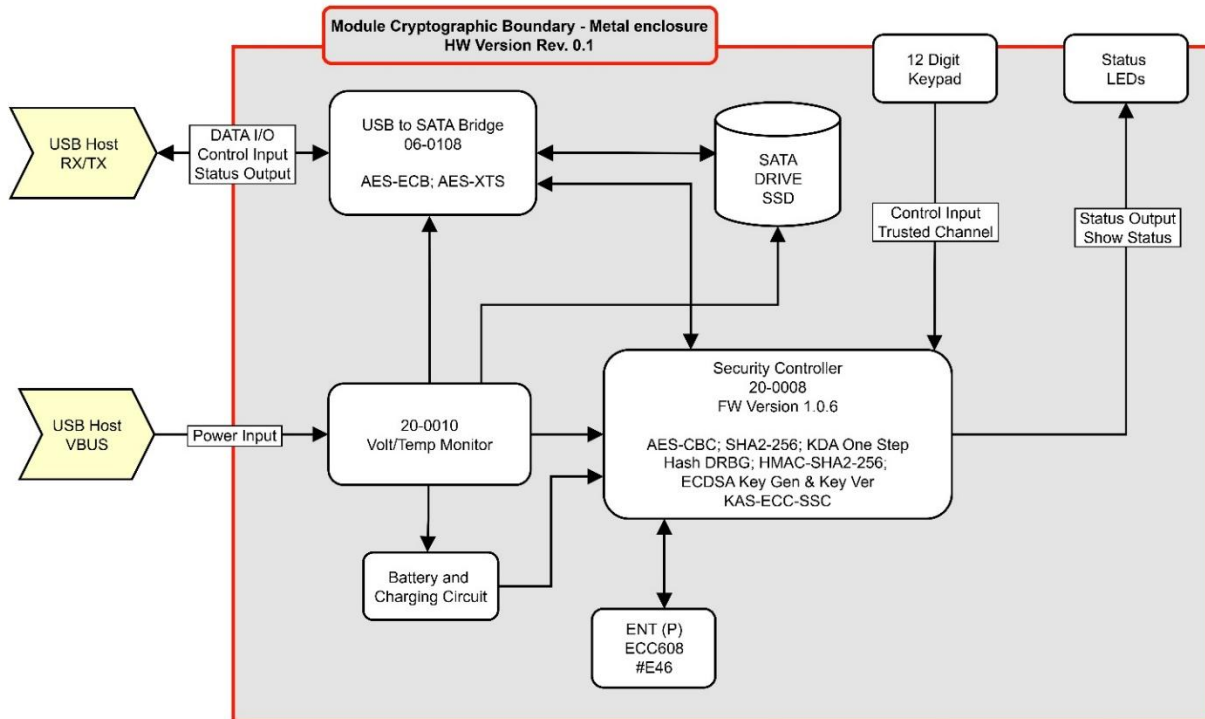


Figure 2: Block Diagram

2.2 Tested and Vendor Affirmed Module Version and Identification

Tested Module Identification – Hardware:

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
ASK3-16GB	Rev. 0.1	1.0.6	AFSC-Q01 06-0108	16GB
ASK3-30GB	Rev. 0.1	1.0.6	AFSC-Q01 06-0108	30GB
ASK3-60GB	Rev. 0.1	1.0.6	AFSC-Q01 06-0108	60GB
ASK3-120GB	Rev. 0.1	1.0.6	AFSC-Q01 06-0108	120GB
ASK3-240GB	Rev. 0.1	1.0.6	AFSC-Q01 06-0108	240GB
ASK3-480GB	Rev. 0.1	1.0.6	AFSC-Q01 06-0108	480GB
ASK3-1TB	Rev. 0.1	1.0.6	AFSC-Q01 06-0108	1TB
ASK3-2TB	Rev. 0.1	1.0.6	AFSC-Q01 06-0108	2TB
ASK3-4TB	Rev. 0.1	1.0.6	AFSC-Q01 06-0108	4TB

Table 2: Tested Module Identification – Hardware

The module's Module identifier can be retrieved by querying the device's USB Device Descriptor fields; specifically, the idProduct field:

- idProduct will display 1407 for the module's PID (Product Identifier)

The module version can be verified by running the show version service (Diagnostics Mode):

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 LEDs will flash Red and Blue for five (5) seconds then all LEDs will illuminate for one second. Release the 0 key.
4. The LEDs will flash the Firmware version (Major.Minor.Patch) and the Hardware version (Major.Minor). Each version number of 1 or greater will blink the Blue LED. If the version is 0, then there is no Blue LED blink and only the Red LED will blink as an indicator of the decimal delimiter (.). The ASK3 module has Firmware version of 1.0.6 and Hardware version Rev. 0.1. After releasing the 0 key, the module will blink the LEDs per the sequence below:

- | | |
|--------------------------------|-----------------|
| a. One Blue LED blink | = 1 |
| b. One Red LED blink | = . (delimiter) |
| c. Zero Blue LED blinks | = 0 |
| d. One Red LED blink | = . (delimiter) |
| e. Six Red LED blinks | = 6 |
| f. One Red LED blink | = . (delimiter) |
| g. Zero Blue LED blinks | = 0 |
| h. One Red LED blink | = . (delimiter) |
| i. One Blue LED blink | = 1 |
| j. One Red LED blink | = . (delimiter) |
| k. X Blue and Y Red LED blinks | = Ignore |

This module version is Firmware 1.0.6; Hardware Rev. 0.1.

Tested Module Identification – Software, Firmware, Hybrid (Executable Code Sets):

N/A for this module.

Tested Module Identification – Hybrid Disjoint Hardware:

N/A for this module.

Tested Operational Environments - Software, Firmware, Hybrid:

N/A for this module.

Vendor-Affirmed Operational Environments - Software, Firmware, Hybrid:

N/A for this module.

2.3 Excluded Components

N/A for this module

2.4 Modes of Operation

Modes List and Description:

Mode Name	Description	Types of Services	Status Indicator
Approved Mode	Module has been initialized per initialization instructions	Approved	Solid RED LED indicating the module is locked and in Approved mode

Table 3: Modes List and Description

The Aegis Secure Key 3.0 only operates in an approved mode of operation when the module is configured according to the initial setup instructions in section 11.1.

2.5 Algorithms

Approved Algorithms:

Algorithm	CAVP Cert	Properties	Reference
AES-CBC, AES-ECB	A5907, A7346	Direction - Decrypt, Encrypt Key Length - 256	SP 800-38A
AES-XTS Testing Revision 2.0	A7346	Direction - Decrypt, Encrypt Key Length - 256 Payload Length - Payload Length: 128-65536 Increment 128 Tweak Mode - Number Data Unit Length - Data Unit Length: 128-4096 Increment 128 Data Unit Length Matches Payload Length - No	SP 800-38E
ECDSA KeyGen (FIPS186-5)	A6008	Curve - P-256 Secret Generation Mode - testing candidates	FIPS 186-5
ECDSA KeyVer (FIPS186-5)	A6008	Curve - P-256	FIPS 186-5
Hash DRBG	A5943	Prediction Resistance - No Supports Reseed - No Mode - SHA2-256 Entropy Input - Entropy Input: 1024 Nonce - Nonce: 0 Personalization String Length - Personalization String Length: 0, 0	SP 800-90A Rev. 1

Algorithm	CAVP Cert	Properties	Reference
		Additional Input - Additional Input: 0, 0 Returned Bits - 256	
HMAC-SHA2-256	A7825	MAC - MAC: 256 Key Length - Key Length: 256 Message Length - Message Length: 64-1536 Increment 8	FIPS 198-1
KAS-ECC-SSC Sp800-56Ar3	A6008	Domain Parameter Generation Methods - P-256 Scheme - ephemeralUnified - KAS Role - responder	SP 800-56A Rev. 3
KDA OneStep SP800-56Cr2	A7826	Auxiliary Function Methods - Auxiliary Function Name - SHA2-256 MAC Salting Methods - default Fixed Info Pattern - algorithmId uPartyInfo vPartyInfo Fixed Info Encoding - concatenation Derived Key Length - 512 Shared Secret Length - Shared Secret Length: 256	SP 800-56C Rev. 2
SHA2-256	A7824	Message Length - Message Length: 64-2048 Increment 8	FIPS 180-4

Table 4: Approved Algorithms

NOTE: Only the algorithms specified in this section are supported by the module in approved mode of operation.

Vendor-Affirmed Algorithms:

Name	Properties	Implementation	Reference
CKG AES	AES:Symmetric	N/A	SP800-133r2 Section 6.3 approved method 1
CKG DRBG	AES:Symmetric ECC-CDH Private Key:Asymmetric	N/A	SP800-133r2 Section 4 example 1

Table 5: Vendor-Affirmed Algorithms

Non-Approved, Allowed Algorithms:

N/A for this module.

Non-Approved, Allowed Algorithms with No Security Claimed:

N/A for this module.

Non-Approved, Not Allowed Algorithms:

N/A for this module.

2.6 Security Function Implementations

Name	Type	Description	Properties	Algorithms
CKG AES	CKG	Derivation of Symmetric Keys using the output of an RBG		CKG AES: () AES: Symmetric
Block Cipher	BC- UnAuthDecrypt BC- UnAuthEncrypt	Block Cipher for data encryption/decryption		AES-XTS Testing Revision 2.0: (A7346) AES-ECB: (A7346)
DRBG Function	DRBG	Deterministic Random Bit Generator		Hash DRBG: (A5943)
Entropy Source - ESV	ENT-ESV	Physical Entropy Source (ESV#46)		
Password Hash	SHA	Used to store passwords in hashed form		SHA2-256: (A7824)
KTS	KTS-Unwrap	AES-CBC + HMAC to unwrap message blob from configurator service	Standard:SP 800-38F IG D.G:approved from IG D.G	AES-CBC: (A5907) HMAC- SHA2-256: (A7825)
CKG DRBG	CKG	Derivation of Symmetric or Asymmetric Keys using the output of an RBG		CKG DRBG: () AES: Symmetric ECC-CDH Private Key: Asymmetric
KAS	KAS-Full	Key Agreement P-256 curve with 128-bits of security strength	IG:IG D.F Scenario 2, path (2), split Key confirmation:No Key derivation:KDA (separately tested) Caveat:Key establishment ,methodology provides 128 bits of security strength	ECDSA KeyGen (FIPS186-5): (A6008) ECDSA KeyVer (FIPS186-5): (A6008) KDA OneStep SP800-56Cr2: (A7826) KAS-ECC-SSC Sp800-56Ar3: (A6008)

Table 6: Security Function Implementations

2.7 Algorithm Specific Information

This section provides additional details regarding the implementation and usage of approved cryptographic algorithms within the Aegis Secure Key 3.0 module:

- **AES-XTS Key Validation:** The module implements AES-XTS in accordance with IG C.I. The module verifies that Key_1 $\neq$ Key_2 prior to usage. If the keys are found to be equal, the module enters a FIPS error state and indicates failure via 16 RED LED blinks.
- **Password Hashing:** PINs and other authentication data are hashed using SHA2-256 prior to storage or verification.

2.8 RBG and Entropy

Cert Number	Vendor Name
E46	Microchip Technology Inc

Table 7: Entropy Certificates

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
NRBG Entropy Source	Physical	ATECC608B	1 bit	0.5071	

Table 8: Entropy Sources

The entropy source produces 0.5071 bits of entropy per sample. For 1024 bits of entropy input the security strength is over 256 bits of entropy strength ($1024 \text{ bits} \times 0.5071 = 519.2704 \text{ bits}$)

2.9 Key Generation

All key generation is performed within the cryptographic boundary of the module. Symmetric keys are generated using the direct output of the SP 800-90A Hash_DRBG. The DRBG is seeded by a non-deterministic entropy source (ATECC608B, ESV (#E46) providing 0.5071 bits of entropy per sample.

2.10 Key Establishment

All key establishment is performed within the cryptographic boundary of the module

- **Key Derivation Function (KDA):** The module uses the SP 800-56C Rev. 2 One-Step KDF with SHA2-256 for deriving keys from shared secrets established via ECDH.

- **Key Agreement Scheme (KAS):** The module supports KAS-ECC-SSC as defined in SP 800-56A Rev. 3 using the P-256 curve. This is used in conjunction with the Configurator service for secure key establishment.

2.11 Industry Protocols

The Aegis Secure Key 3.0 Cryptographic Module follows the Universal Serial Bus protocol requirements.

2.12 Additional Information

The Module design corresponds to the Module security rules. Security rules enforced by the Module are described in the appropriate context of this document.

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

Physical Port	Logical Interface(s)	Data That Passes
Universal Serial Bus (USB) Connector	Data Input Data Output Control Input Status Output Power	Data Stored on the devices hard drive/memory Encrypted data packets from the configurator service during module initialization Status output for module identifier
Physical Keypad	Data Input Control Input	Keypad is used to enter PINs for device authentication, and allows crypto officer to change settings
Status LEDs	Status Output	LEDs used to communicate module state, settings, and module information

Table 9: Ports and Interfaces

Note: The module does not support a Control Output Interface.

3.2 Trusted Channel Specification

The module implements a trusted channel for the input of plaintext authentication data (SSP) in the form of passwords (PINs) via the module's keypad interface. The trusted channel is intended for the operator to both create authentication data in the form of PINs and then use the established authentication data to access the module. The user stays in control of the trusted channel by having full physical control of the module, as the module is a handheld device. The user can prevent unauthorized tampering by checking for evidence of tampering each time the module is used.

Physical characteristics of the trusted channel: Each key is mapped to a dedicated, physically separated channel. The trusted channel is protected by the physical security mechanisms inherent within the module which includes the industrial grade enclosure with tamper evidence.

Controls to maintain the trusted channel: There are no extra controls needed to maintain the trusted channel. The trusted channel (physical keypad) functions as part of the module normal operation without any necessary extra tools required by the CO or user.

Instructions for setup and operation of the trusted channel: to setup and operate the trusted channel, the CO and User can reference PIN creation and PIN use instructions in the ASK3 modules user manual included with the module.

- Trusted channel for PIN establishment – Section 11.1 below specifies specific command procedures required for PIN establishment as well as status LED output indications that occur during PIN establishment
- Trusted channel for module authentication – pressing the unlock button on the module will establish the trusted channel with the status indication of a solid RED LED. The user can then enter their plaintext authentication data and press the unlock button. If authentication data is accepted, the module will Unlock with a Green LED. If the authentication data is not accepted, the module will end the trusted channel and the RED LED will flash.

The modules implementation and use of plaintext authentication data through the trusted channel conforms to FIPS 140-3 IG 10.3.C.

4 Roles, Services, and Authentication

4.1 Authentication Methods

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
PIN Code Verification	A minimum eight-digit PIN is used, with each digit selected from ten (10) possible characters. There are 10^8 (one hundred million) possible PIN combinations	Known Secret	The probability of a random attempt to authenticate to the module is $1/100,000,000$	The probability of multiple consecutive attempts to authenticate to the module during a one-minute period is $20/100,000,000$
Configurator EC Diffie-Hellman	The modules support ECC-CDH public-key based authentication mechanism using a minimum of curve P-256	ECDSA KeyVer (FIPS186-5) (A6008)	Since P-256 curve is used, the probability that a random attempt to authenticate to the module is $1/(2^{128})$ which is much less than $1/1,000,000$.	One authentication attempt is allowed before a User reset must be performed which takes approximately 30 seconds to complete the procedure, therefore there could be ~2 attempts per minute. Given this, the probability of multiple

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
				consecutive attempts to authenticate to the module during a one-minute period is $2/(2^{128})$ which is much less than 1/100,000.

Table 10: Authentication Methods

For more information on the Configurator, see section 11.1

4.2 Roles

Name	Type	Operator Type	Authentication Methods
User	Identity	User	PIN Code Verification
Admin	Identity	Crypto Officer	PIN Code Verification Configurator EC Diffie-Hellman
Unauthenticated	Identity	Unauthenticated	None

Table 11: Roles

The Module supports the Admin (Cryptographic Officer (CO)) operator role and a general User operator role. When authenticating to the module, the Admin and User have access to the same data on the storage media. The Admin has access to alter device settings (services) and manage authentication data (PINs) via the modules admin mode as referenced in the ASK3 user manual.

4.3 Approved Services

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Unlock	Authenticates the operator to the module	Global Indicator	Keypad	None	Password Hash	Admin - AES Encryption Key: E - Admin PIN: W,E,Z - Hashed Admin PIN: E User - AES Encryption Key: E - User PIN: W,E,Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- Hashed User PIN: E
Lock	Locks the module to prevent any access	Global Indicator	Keypad	None	None	Admin User
Write Data	Write user data/files on the disk storage area	Global Indicator	Plaintext Data	None	Block Cipher	Admin - AES Encryption Key: E User - AES Encryption Key: E
Read Data	Read user data/files on the disk storage area	Global Indicator	None	Plaintext Data	Block Cipher	Admin - AES Encryption Key: E User - AES Encryption Key: E
Establish User PINs	Create Admin or User PIN	Global Indicator	Keypad	None	Password Hash	Admin - Admin PIN: W,E,Z - Hashed Admin PIN: G,W User - User PIN: W,E,Z - Hashed User PIN: G,W
Change PINs	Change Admin or User PIN	Global Indicator	Keypad	None	Password Hash	Admin - Admin PIN: W,E,Z - Hashed Admin PIN: G,W,E User - User PIN: W,E,Z - Hashed User PIN: G,W,E
Set Self-Destruct	Enable or Disable Self-	Global Indicator	Keypad	None	None	Admin - Self-Destruct PIN: Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	Destruct feature					- Admin PIN: W,E,Z - Hashed Admin PIN: E - Hashed Self-Destruct PIN: Z
Self-Destruct PIN	Create self destruct PIN (Self destruct must be enabled)	Global Indicator	Keypad	None	Password Hash	- Admin - Self-Destruct PIN: G,W,E,Z - Admin PIN: W,E,Z - Hashed Admin PIN: E - Hashed Self-Destruct PIN: G,W - User - Self-Destruct PIN: W,E,Z - Hashed Self-Destruct PIN: G,W
Self-Destruct	Use self-destruct PIN to zeroize user data/files on disk storage area	Global Indicator	Keypad	None	Block Cipher Password Hash	- Admin - Self-Destruct PIN: W,E,Z - AES Encryption Key: W - Hashed Self-Destruct PIN: E,Z - Hashed Admin PIN: W - Hashed Recovery PIN: Z - Hashed User PIN: Z - User - Self-Destruct PIN: W,E,Z - Hashed Self-Destruct PIN: Z - Hashed Admin PIN: W - AES

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Encryption Key: W - Hashed Recovery PIN: Z - Hashed User PIN: Z
Delete All User PINs	Deletes all user and recovery PINs. Only Admin PIN remains	Global Indicator	Keypad	None	Password Hash	Admin - Admin PIN: W,E,Z - Hashed Admin PIN: E - Hashed User PIN: Z - Hashed Recovery PIN: Z - Hashed Self-Destruct PIN: Z
Set Unattended Auto Lock	Sets a timer to automatically lock the device after a period of inactivity	Global Indicator	Keypad	None	None	Admin - Admin PIN: W,E,Z - Hashed Admin PIN: E
Set Read Only	Set the drive to read only mode	Global Indicator	Keypad	None	None	Admin - Admin PIN: W,E,Z - Hashed Admin PIN: E User - User PIN: W,E,Z - Hashed User PIN: E
Set Lock Override	Setting to prevent device from locking during a system reboot	Global Indicator	Keypad	None	None	Admin - Admin PIN: W,E,Z - Hashed Admin PIN: E
Create Recovery PINs	Create PINs that can be used for a user recovery if a user PIN is forgotten	Global Indicator	Keypad	None	Password Hash	Admin - Recovery PIN: W,Z - Admin PIN: W,E,Z - Hashed Admin PIN: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- Hashed Recovery PIN: G,W
Use Recovery PIN	Use a recovery PIN to allow user to set new PIN	Global Indicator	Keypad	None	Password Hash	Admin - Recovery PIN: W,E,Z - Hashed Recovery PIN: Z - User PIN: G,W,E User - Recovery PIN: W,E,Z - Hashed Recovery PIN: Z - User PIN: G,W,E - Hashed User PIN: W
Setup Forced Enrollment	Puts device in a mode for user to create a PIN before use	Global Indicator	Keypad	None	None	Admin - Admin PIN: W,E,Z - Hashed Admin PIN: E
Set Minimum PIN Length	Set required minimum PIN length for new PINs	Global Indicator	Keypad	None	None	Admin - Admin PIN: W,E,Z - Hashed Admin PIN: E
Set LED Flicker	Set device so LEDs flicker when buttons are pressed	Global Indicator	Keypad	None	None	Admin - Admin PIN: W,E,Z - Hashed Admin PIN: E
Configurator	Allows automated setup of device PINs and features	Global Indicator	Encrypted payloads sent from the configurator or service	ECC-CDH Public Key	DRBG Function Password Hash KTS CKG DRBG KAS	Admin - User PIN: W,E,Z - Hashed User PIN: G,W - Admin PIN: W,E,Z - Hashed Admin PIN: G,W - Recovery

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						PIN: W,E,Z - Hashed Recovery PIN: G,W - Self-Destruct PIN: W,E,Z - Hashed Self-Destruct PIN: G,W - AES-CBC Decryption Key: G,E,Z - ECDH Public Key: G,R,Z - ECDH Private Key: G,E,Z - ECDH Shared Secret "Z": G,E,Z - SP 800-56Cr2 KDF Internal State: G,E,Z - Host EC DH Public Key: W,E - Module HMAC MAC: G,W,E,Z - Host HMAC MAC: W,E,Z - HMAC Shared Key: G,W,E,Z
Show Version	Diagnostics Mode - Unauthenticated service to check module version and test functionality of all keypad buttons	Global Indicator	Keypad	None	None	Unauthenticated
Show Status	LED indication for the status of the module	Global Indicator	None	None	None	User Admin

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Unauthenticated
Set Brute Force Attempts	Sets the number of failed unlock attempts before module zeroizes	Global Indicator	Keypad	None	None	Admin - Admin PIN: W,E,Z - Hashed Admin PIN: E
On-Demand Self Tests	Perform module self-tests on demand	Global Indicator	Keypad	None	None	Unauthenticated
User Reset (FIPS Zeroize)	Zeroize Service	Global Indicator	Keypad	None	CKG AES DRBG Function Entropy Source - ESV CKG DRBG KAS	Admin - AES Encryption Key: G,W,Z - Hashed User PIN: Z - Hashed Admin PIN: Z - Hashed Recovery PIN: Z - Hashed Self-Destruct PIN: Z - HASH-DRBG Internal State: G,E,Z - ECDH Private Key: G,W,Z - SP 800-56Cr2 KDF Internal State: Z - HASH DRBG Seed: G,E,Z - Entropy Input: G,E,Z User - AES Encryption Key: G,W,Z - Hashed User PIN: Z - Hashed

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Admin PIN: Z - Hashed Recovery PIN: Z - Hashed Self-Destruct PIN: Z - HASH-DRBG Internal State: G,E,Z - ECDH Private Key: G,E,Z - SP 800-56Cr2 KDF Internal State: Z - HASH DRBG Seed: G,E,Z - Entropy Input: G,E,Z Unauthenticated - AES Encryption Key: G,W,Z - Hashed User PIN: Z - Hashed Admin PIN: Z - Hashed Recovery PIN: Z - Hashed Self-Destruct PIN: Z - HASH-DRBG Internal State: G,E,Z - ECDH Private Key: G,W,Z - SP 800-56Cr2 KDF Internal State: Z - HASH DRBG Seed: G,E,Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- Entropy Input: G,E,Z
Provision Lock	Changes module function so zeroize can only be called by Admin	Global Indicator	Keypad	None	None	Admin - Admin PIN: W,E,Z - Hashed Admin PIN: E

Table 12: Approved Services

Global Indicator is the successful completion of a service as an implicit indicator for the use of an approved service.

4.4 Non-Approved Services

N/A for this module.

The Aegis Secure Key 3.0 does not support any Non-Approved services.

4.5 External Software/Firmware Loaded

The module does not support external software/firmware loading

5 Software/Firmware Security

5.1 Integrity Techniques

The module Firmware is non-modifiable. A CRC-16 integrity check is run on the module FW during every startup and authentication action. A failure of the integrity check will result in the module being placed into an error state as referenced in section 10.4

5.2 Initiate on Demand

The FW integrity can be checked by performing the on-demand self-test service

6 Operational Environment

6.1 Operational Environment Type and Requirements

Type of Operational Environment: Non-Modifiable

7 Physical Security

Epoxy coating

The modules incorporate 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, hard metal enclosure that defines the cryptographic boundary.

7.1 Mechanisms and Actions Required

Mechanism	Inspection Frequency	Inspection Guidance
Hard, opaque, tamper-evident, production-grade epoxy coating and metal enclosure	In accordance with the Administrator role organizational security policy or every 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 13: Mechanisms and Actions Required

7.2 EFP/EFT Information

Temp/Voltage Type	Temperature or Voltage	EFP or EFT	Result
LowTemperature	-15 C	EFP	Shutdown
HighTemperature	80 C	EFP	Shutdown
LowVoltage	4 VDC	EFP	Shutdown
HighVoltage	5.25 VDC	EFP	Shutdown

Table 14: EFP/EFT Information

7.3 Hardness Testing Temperature Ranges

Temperature Type	Temperature
LowTemperature	-40 C
HighTemperature	85 C

Table 15: Hardness Testing Temperatures

8 Non-Invasive Security

The module does not provide protections against non-invasive security methods.

9 Sensitive Security Parameters Management

9.1 Storage Areas

Storage Area Name	Description	Persistence Type
RAM	Random Access Memory	Dynamic

Storage Area Name	Description	Persistence Type
EEPROM	Electrically Erasable Programmable Read Only Memory	Static

Table 16: Storage Areas

9.2 SSP Input-Output Methods

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
PINs - Keypad	EXT: Trusted Channel	INT	Plaintext	Manual	Direct	Password Hash
PINs - Configurator	EXT: Configurator Service	INT	Encrypted	Automated	Electronic	KTS
Public Key	INT	EXT: Configurator Service	Plaintext	Automated	Electronic	KAS
Host HMAC Authentication Tag	EXT: Configurator Service	INT	Encrypted	Automated	Electronic	KTS

Table 17: SSP Input-Output Methods

9.3 SSP Zeroization Methods

Zeroization Method	Description	Rationale	Operator Initiation
User Reset (FIPS Zeroize)	CO/User issues Reset command	The zeroization command will erase all SSPs stored in storage areas	User reset service
Self-Destruct	Self Destruct service	Self-Destruct shall zeroize the module	Self-Destruct Service
Delete all user PINs	Delete all user PINs service	Deleted PINs are no longer be accessible and are overwritten with zeros	Delete all User PINs service
Change PIN	Change PIN service	PIN is overwritten with new PIN	Change PIN Service
Configurator	Public Key, HMAC Shared Key and HMAC MAC Destruction	Temporary keys used for HMAC and ECDH shall be zeroized when no longer needed	Initialize Module
After Use	Temporary Stored RAM values for Plaintext PINs	Plaintext PINs are only used to create hash values and verify against hashed PIN values	N/A

Table 18: SSP Zeroization Methods

9.4 SSPs

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
AES Encryption Key	256-bit AES-XTS key used to encrypt/decrypt protected data	256-bits - 256-bits	Symmetric Key - CSP	CKG AES Hash DRBG (A5943)		Block Cipher
User PIN	Plaintext authentication data for the General User	8 to 16 digit PIN - 64-bit	Authentication - CSP			Password Hash
Hashed User PIN	SHA2-256 Hashed value of the plaintext PIN	256 bytes - 256	Authentication - CSP	SHA2-256 (A7824)		
Admin PIN	Plaintext authentication data for the Admin (CO)	8 to 16 digit PIN - 64-bit	Authentication - CSP			Password Hash
Hashed Admin PIN	SHA2-256 Hashed value of the plaintext PIN	256 bytes - 256	Authentication - CSP	SHA2-256 (A7824)		
Recovery PIN	Plaintext authentication data for the General User/Administrator	8 to 16 digit PIN - 64-bit	Authentication - CSP			Password Hash
Hashed Recovery PIN	SHA2-256 Hashed value of the plaintext PIN	256 bytes - 256	Authentication - CSP	SHA2-256 (A7824)		
Self-Destruct PIN	Unique PIN that performs a cryptographic erase of the module, deletes PINs and assigns the self-destruct PIN	8 to 16 digit PIN - 64-bit	Authentication - Neither			Password Hash

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	to the admin PIN					
Hashed Self-Destruct PIN	SHA2-256 Hashed value of the plaintext PIN	256 bytes - 256	Authentication - Neither	SHA2-256 (A7824)		
HASH-DRBG Internal State	Values of V and C of HASH DRBG mechanism	880-bit - 256	Critical values of internal state on SP 800-90A - CSP	Hash DRBG (A5943)		CKG AES CKG DRBG
HASH DRBG Seed	Entropy Input from the ECC608B NRBG used to seed the SP 800-90A HASH DRBG	256 - 256	Critical values of internal state on SP 800-90A - CSP	Entropy Source - ESV		DRBG Function
Entropy Input	Input String from the Entropy Source for the DRBG	1024 - 256	Entropy Input to the Approved DRBG - CSP	Entropy Source - ESV		Hash DRBG (A5943)
AES-CBC Decryption Key	256-bit AES-CBC key used to decrypt protected data	256-bit - 256-bit	Symmetric Key - CSP		KDA OneStep SP800-56Cr2 (A7826)	KTS
ECDH Private Key	The module's P-256 SP 800-56A ECDH private key	256-bit - 128	Private - CSP	Hash DRBG (A5943) CKG DRBG		KAS
ECDH Public Key	The module's P-256 SP 800-56A ECDH public key	256-bit - 128	Public - PSP	Hash DRBG (A5943) CKG DRBG		KAS
ECDH Shared Secret "Z"	The module's 256-bit SP 800-56A ECDH Shared Secret "Z" used in ECDH key	256-bit - 256	Public/Private - CSP		KAS-ECC-SSC Sp800-56Ar3 (A6008)	KAS

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
Host EC DH Public Key	Host's P-256 SP 800-56A EC DH Public Key	256-bit - 128	Public/Private - PSP			KAS
Module HMAC MAC	used to authenticate the encrypted message from Configurator service	256-bit - 256	Public/Private - CSP		KAS KAS-ECC-SSC Sp800-56Ar3 (A6008) KDA OneStep SP800-56Cr2 (A7826)	KTS
Host HMAC MAC	received from the Configurator service	256-bit - 256	Public/Private - CSP			KTS
HMAC Shared Key	Mac Key for HMAC	256-bit - 256	Public/Private - CSP		KAS KAS-ECC-SSC Sp800-56Ar3 (A6008) KDA OneStep SP800-56Cr2 (A7826)	KTS
SP 800-56Cr2 KDF Internal State	Client's Internal state of the ECC CDH One step key derivation function (SHA2-256)	256 - 256	KDF Internal State - CSP		KDA OneStep SP800-56Cr2 (A7826)	

Table 19: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
AES Encryption Key		EEPROM:Plaintext RAM:Plaintext		User Reset (FIPS Zeroize) Self-Destruct	HASH-DRBG Internal State:Derived From

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
User PIN	PINs - Keypad PINs - Configurator	RAM:Plaintext	Usage Session	After Use	
Hashed User PIN		EEPROM:Obfuscated		User Reset (FIPS Zeroize) Self-Destruct Delete all user PINs Change PIN	User PIN:Derived From
Admin PIN	PINs - Keypad PINs - Configurator	RAM:Plaintext	Usage Session	After Use	
Hashed Admin PIN		EEPROM:Obfuscated		User Reset (FIPS Zeroize) Self-Destruct Change PIN	Admin PIN:Derived From
Recovery PIN	PINs - Keypad PINs - Configurator	RAM:Plaintext	Usage Session	After Use	
Hashed Recovery PIN		EEPROM:Obfuscated		User Reset (FIPS Zeroize) Self-Destruct Delete all user PINs Change PIN	Recovery PIN:Derived From
Self-Destruct PIN	PINs - Keypad PINs - Configurator	RAM:Plaintext	Usage Session	After Use	Hashed Admin PIN:Derived From
Hashed Self-Destruct PIN		EEPROM:Obfuscated		User Reset (FIPS Zeroize) Delete all user PINs	

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
HASH-DRBG Internal State		RAM:Plaintext		User Reset (FIPS Zeroize)	
HASH DRBG Seed		RAM:Plaintext		User Reset (FIPS Zeroize)	
Entropy Input		RAM:Plaintext		User Reset (FIPS Zeroize) After Use	HASH-DRBG Internal State:generates HASH DRBG Seed:generates
AES-CBC Decryption Key		RAM:Plaintext	Configurator Usage Session	Configurator	SP 800-56Cr2 KDF Internal State:Derived From
ECDH Private Key	Public Key	EEPROM:Plaintext	Configurator Usage Session	User Reset (FIPS Zeroize) Configurator	ECDH Public Key:Paired With HASH-DRBG Internal State:Derived From
ECDH Public Key	Public Key	RAM:Plaintext	Configurator Usage Session	Configurator	ECDH Private Key:Derived From
ECDH Shared Secret "Z"		RAM:Plaintext	Configurator Usage Session	Configurator	Host ECC CDH Public Key:Derived From Client ECC CDH Private Key:Derived From
Host ECDH Public Key		RAM:Plaintext	Configurator Usage Session	Configurator	
Module HMAC MAC		RAM:Plaintext	Configurator Usage Session	Configurator	HMAC Shared Key:Derived From
Host HMAC MAC	Host HMAC Authentication Tag	RAM:Plaintext	Configurator Usage Session	Configurator	
HMAC Shared Key		RAM:Plaintext	Configurator Usage Session	Configurator	SP 800-56Cr2 KDF Internal

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
					State:Derived From
SP 800-56Cr2 KDF Internal State		RAM:Plaintext	Configurator Usage Session	User Reset (FIPS Zeroize)	

Table 20: SSP Table 2

10 Self-Tests

10.1 Pre-Operational Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
16-Bit FW Integrity Tests	CRC-16	KAT	SW/FW Integrity	Global Indicator	Verify

Table 21: Pre-Operational Self-Tests

10.2 Conditional Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
SHA2-256	SHA2-256	KAT	CAST	Global Indicator	Verify	Power up & Authenticate
Hash_DRBG	SHA2-256; SP 800-90A Section 11.3 health tests for Instantiate and Generate functions	KAT	CAST	Global Indicator	Verify	Power up & Authenticate
ECDH PCT	Module Key Pair	PCT	PCT	Global Indicator	Verify	Configurator Service
HMAC-SHA2-256	HMAC-SHA2-256	KAT	CAST	Global Indicator	Verify	Power up & Authenticate
AES-256 CBC Encrypt	256-bit	KAT	CAST	Global Indicator	Encrypt	Power up & Authenticate
AES-256 CBC Decrypt	256-bit	KAT	CAST	Global Indicator	Decrypt	Power up & Authenticate
ECDH	P-256	KAT	CAST	Global Indicator	Verify	Power up

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
One Step KDF	SHA2-256	KAT	CAST	Global Indicator	N/A	Power up
90B RCT & APT Health tests	1024-bit	APT/RCT	Critical Function	Global Indicator	Health-Test with sub-elements	Power up & Authenticate
XTS-AES 256 Encrypt	256-bit	KAT	CAST	Global Indicator	Encrypt	Power up & Authenticate
XTS-AES 256 Decrypt	256-bit	KAT	CAST	Global Indicator	Decrypt	Power up & Authenticate
Partial Key Validation 1	Module Public Key P-256	PCT	PCT	Global Indicator	Verify	Power up
Partial Key Validation 2	Host Public Key P-256	PCT	PCT	Global Indicator	Verify	Power up
XTS-AES Key Compare	256-bit	Comparison	Critical Function	Global Indicator	Verify	Zeroization
Manual PIN Entry	N/A	Duplicate Key Entry	Manual Entry	Global Indicator	Requires PINs be entered twice	Establishing PINs

Table 22: Conditional Self-Tests

10.3 Periodic Self-Test Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
16-Bit FW Integrity Tests	KAT	SW/FW Integrity	Power Up; Authenticate	Manual

Table 23: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
SHA2-256	KAT	CAST	Authenticate	Manual
Hash_DRBG	KAT	CAST	Authenticate	Manual
ECDH PCT	PCT	PCT	On-Demand self-test or Key Generation	Manual
HMAC-SHA2-256	KAT	CAST	Authenticate	Manual
AES-256 CBC Encrypt	KAT	CAST	Authenticate	Manual
AES-256 CBC Decrypt	KAT	CAST	Authenticate	Manual
ECDH	KAT	CAST	Key Generation	Manual
One Step KDF	KAT	CAST	Key Generation	Manual

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
90B RCT & APT Health tests	APT/RCT	Critical Function	Authenticate	Manual
XTS-AES 256 Encrypt	KAT	CAST	Authenticate	Manual
XTS-AES 256 Decrypt	KAT	CAST	Authenticate	Manual
Partial Key Validation 1	PCT	PCT	Key Generation	Manual
Partial Key Validation 2	PCT	PCT	Configurator Service	Manual
XTS-AES Key Compare	Comparison	Critical Function	Key Generation	Manual
Manual PIN Entry	Duplicate Key Entry	Manual Entry	PIN Establishment	Manual

Table 24: Conditional Periodic Information

10.4 Error States

Name	Description	Conditions	Recovery Method	Indicator
WDT Reset	Watch Dog Timer Reset - Communication error	Power up Authenticate	On-Demand Self-Tests or Device Reset (zeroization)	RED LED Blinks 3 times followed by BLUE LED Blink
Configurator	Configurator Service Failure	Power up	On-Demand Self-Tests or Device Reset (zeroization)	RED LED Blinks 4 times followed by BLUE LED Blink
FW Integrity	Computed Checksum does not match stored checksum	Power up Authenticate	On-Demand Self-Tests or Device Reset (zeroization)	RED LED Blinks 5 times followed by BLUE LED Blink
SHA2-256 KAT	SHA2-256 KAT failure	Power up Authenticate	On-Demand Self-Tests or Device Reset (zeroization)	RED LED Blinks 6 times followed by BLUE LED Blink
HASH-DRBG KAT	HASH-DRBG KAT failure	Power up Authenticate	On-Demand Self-Tests or Device Reset (zeroization)	RED LED Blinks 7 times followed by BLUE LED Blink

Name	Description	Conditions	Recovery Method	Indicator
XTS-AES 256 Self-test	XTS-AES 256 Self-test failure	Power up Authenticate	On-Demand Self-Tests or Device Reset (zeroization)	RED LED Blinks 8 times followed by BLUE LED Blink
AES-256-CBC KAT	AES-256-CBC KAT failure	Power up Authenticate	On-Demand Self-Tests or Device Reset (zeroization)	RED LED Blinks 9 times followed by BLUE LED Blink
KAS or KDF KAT	KAS or KDF KAT failure	Power up Authenticate	On-Demand Self-Tests or Device Reset (zeroization)	RED LED Blinks 10 times followed by BLUE LED Blink
ECC Public Key Generation	Failed to Generate Public Key	Power up	On-Demand Self-Tests or Device Reset (zeroization)	RED LED Blinks 11 times followed by BLUE LED Blink
HMAC-SHA2-256 KAT	HMAC-SHA2-256 KAT failure	Power up Authenticate	On-Demand Self-Tests or Device Reset (zeroization)	RED LED Blinks 12 times followed by BLUE LED Blink
SP800-90B Health Test	SP800-90B health test failure	Power up Authenticate	On-Demand Self-Tests or Device Reset (zeroization)	RED LED Blinks 13 times followed by BLUE LED Blink
Key Comparison	XTS-AES Key Comparison failure	Power up Authenticate	On-Demand Self-Tests or Device Reset (zeroization)	RED LED Blinks 16 times followed by BLUE LED Blink
EEPROM Load	Failed to load XTS-AES key during unlock	Power up Authenticate	On-Demand Self-Tests or Device Reset (zeroization)	RED LED Blinks 20 times followed by BLUE LED Blink

Table 25: Error States

The module design prohibits cryptographic operations while the module is in any error state, until such a time as error recovery occurs. Data output and control output information are also inhibited while in the error state; only status output is allowed.

The module does not log or store previous error occurrences. When the module is in an error state, it cannot be operated normally and will continuously report the error until error recovery is

attempted through an invocation of on-demand self-tests or by performing a user reset (zeroize) service. If self-tests pass, the module will transition to an operational state, otherwise, the error state shall persist.

The module's error operation and logging function meets the resolutions set forth in FIPS 140-3 IG 10.3.D as of the publication of this security policy.

To recover from an error state, the operator can perform a complete reset or invoke the on-demand self-tests. Only if all self-tests are completed successfully, will the module transition to an operational state.

10.5 Operator Initiation of Self-Tests

On-demand self-tests can be performed from the standby state. To invoke these tests, first ensure the device is not plugged into a powered USB port (this prevents damaging the USB plug) and wake the device by pressing the UNLOCK button. Next press the LOCK + 8 buttons simultaneously. The solid red LED will transition to a blinking green LED for ten (10) seconds. Within these ten seconds, plug the device into a powered USB port and the device will automatically perform on-demand self-tests. Otherwise, the device will time out and return to standby state. Successful self-tests completion will be indicated by the following LED sequence: solid RED followed by solid GREEN followed by solid BLUE. The device will then return to standby state.

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

The Administrator role (CO) is responsible for the overall security of the module and initializing the cryptographic module into the Approved mode of operation and adding an additional user role to the module.

The Administrator shall perform one (1) of the following two (2) procedures to set the initial Admin PIN and initialize the module into Approved 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 (this establishes the trusted channel for PIN creation).
 - 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 (this ends the trusted channel for PIN creation).
 - d. Push the Lock button.

2. Execute the “Configurator” service to perform the initialization of the module and set the admin PIN and setup a user role by either establishing a PIN or setting the module into user forced enrollment.

If the module was set to approved mode manually (not using the configurator service), the CO can add a user role following this method:

1. Place the module in admin mode using the following method:
 - a. From locked standby (solid RED LED), Press and hold UNLOCK + 0 together for five seconds until the RED LED blinks once per second.
 - b. Enter the Admin PIN and press the UNLOCK button.
 - c. The Aegis Secure Product is now in Admin Mode, indicated by a solid BLUE LED.
2. Manually set the PIN for the user
 - a. In admin mode Press the UNLOCK + 1 buttons together, to initiate User Enrollment Mode. The BLUE LED will be solid and the GREEN LED will be flashing.
 - b. Enter the desired User PIN and press UNLOCK. The GREEN LED will blink three times by itself, then the BLUE LED will glow solidly as the GREEN LED continues blinking.
 - c. Re-enter that same PIN and press the UNLOCK button again. The GREEN LED will flash solid for 3 seconds and the module will return to admin mode (solid BLUE LED).

The Configurator GUI application is outside of the module’s FIPS 140-3 validation scope. It resides on the host pc used by the Cryptographic Officer during module initialization. The Configurator GUI application is the Configurator service that is used for module initialization that is an alternative to manual initialization using the module’s keypad trusted channel. The module authenticates the Configurator GUI application using an SP800-56Ar3 ECC-CDH KAS. Each message that is sent from the Configurator GUI application to the module is further protected using the KTS SFI. After module initialization, the Configurator GUI application cannot communicate with the module unless the module is in it’s factory OOB state (post user reset).

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

The cryptographic module only supports an Approved mode of operation, therefore a non-compliant configuration is not possible and out of scope for this validation.

11.2 Administrator Guidance

Upon receipt of the module an operator must follow the initialization procedure outlined in Section 11.1. This establishes the operator as the Admin (Cryptographic Officer (CO)) with a PIN.

The module is designed to securely store authorized user’s data files using physical and logical security methods. A user may transfer files to the device via a compatible PC or similar device. Over the life of the device an operator may:

- Initialize the device as a single operator (CO only).
- Initialize the device for multiple operators (CO and User).
- Transfer files to the device for secure storage.
- Reset the device effectively cryptographically zeroizing all data, CSPs and SSPs.

Services available to the CO role are listed in section 4.3.

Further Administrator Guidance that is not in this security policy for this module can be found in the owner's manual for the ASK3 product at the link below under "MANUALS AND DATASHEETS"

<https://apricorn.com/aegis-secure-key-3>

11.3 Non-Administrator Guidance

The cryptographic officer must establish access for a general user role. An operator under the User role shall authenticate and transfer files to the device via a compatible PC or similar device. Services available to the User role are listed in section 4.3.

Further Non-Administrator Guidance that is not in this security policy for this module can be found in the owner's manual for the ASK3 product at the link below under "MANUALS AND DATASHEETS"

<https://apricorn.com/aegis-secure-key-3>

11.4 Design and Rules

- The cryptographic module always runs in an Approved mode of operation (i.e., non-Approved is not supported). It is possible to determine that the module is in Approved mode by waking up the module and observing LED status as follows: RED LED is solid to indicate self-tests completed successfully; RED LED flashes to indicate an error state, including failure of a power-up self-test as well as failure of a conditional self-test.
- Power on self-tests are run automatically when the device is initially powered. This can happen at the time of manufacture or when power is applied through the USB and the batteries have been depleted.
- On-demand self-tests can be performed from the standby state. To invoke these tests, first ensure the device is not plugged into a powered USB port (this prevents damaging the USB plug) and wake the device by pressing the UNLOCK button. Next press the LOCK + 8 buttons simultaneously. The solid red LED will transition to a blinking green LED for ten (10) seconds. Within these ten seconds, plug the device into a powered USB port and the device will automatically perform on-demand self-tests. Otherwise, the device will time out and return to standby state. Successful self-tests completion will be indicated by the following LED sequence: solid RED followed by solid GREEN followed by solid BLUE. The device will then return to standby state.
- 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 either via USB or the internal battery.

- The cryptographic module does not support a maintenance interface or bypass capability.
- The cryptographic module does not support Firmware loading capability.
- The cryptographic module does not support the output of any secret keys, private keys, or CSPs in any form.
- During error states, 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. To recover from an error state, the operator can perform a complete reset or invoke the on-demand self-tests. Only if all self-tests are completed successfully, will the module transition to an operational state.
- The cryptographic module supports Identity-based authentication.
- The Administrator (Crypto Officer) 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 provides a hard, opaque, tamper-evident, production-grade epoxy encapsulating all electrical components containing CSPs.
- 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 obscures feedback of authentication data – the module does not provide any feedback on which buttons are being pressed to help prevent eavesdropping when entering authentication data.
- The cryptographic module provides a non-deterministic hardware random number generator strictly for the purposes of seeding the deterministic random bit generator.
- The cryptographic module supports zeroization to destroy all critical security parameters. All CSPs are destroyed with the User Reset (FIPS Zeroize) 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 $\neq$ Key_2, before the keys are to be used. If the test fails, the module will enter a FIPS error state, and blink the RED LED 15 times.

11.5 End of Life

Secure Sanitation

The ASK3 Zeroization (User Reset) service sanitizes the module as per SP800-88r1

Secure Destruction

To physically destroy the module in a secure manner, it is recommended that the module be returned to Apricorn for secure destruction and proof of destruction. Alternatively, a third-party data/electronics destruction company may be used for module destruction.

12 Mitigation of Other Attacks

This module is not designed to mitigate other attacks beyond the scope of FIPS 140-3 requirements.