Apricorn Aegis Secure Key

Security Policy

FIPS 140-2 SECURITY POLICY VERSION 6

Definitions and Acronyms

- AES – Advanced Encryption Standard
- CBC – Cipher Block Chaining
- CRC – Cyclic Redundancy Check
- CSP – Critical Security Parameter
- DRBG – Deterministic Random Bit Generator
- DRNG – Deterministic Random Number Generator
- FIPS – Federal Information Processing Protocol
- NDRNG – Non-deterministic Random Number Generator
- SHA – Secure Hash Algorithm

Product Overview

Apricorn Aegis Secure Key ("Aegis Secure Key" or "ASK") is an encrypted storage device that provides organizations a secure way to store and transfer data. User authentication is self-contained via an on-board keypad. Stored data is secured by hardware-based 256-bit AES encryption to guard sensitive information in case the drive is lost or stolen.

Encryption keys are not stored in memory, but rather created from a combination of random data and user supplied PIN each time the drive is put to use. Random data is generated from a hardware-based random number generator feeding the FIPS approved random number generator.

Capacity	PCB revision	USB controller firmware revision	Security controller firmware revision
4 GB	ASK-256-4GB	V01.12A13-F05	iStorage v6
8 GB	ASK-256-8GB	V01.12A13-F04	iStorage v6
16 GB	ASK-256-16GB	V01.12A15 Code Package—111130	iStorage v6

Figure 1 – Apricorn Aegis Secure Key cryptographic boundary showing input buttons and status LEDs

Validation Level

The cryptographic module meets the overall requirements applicable to Level 3 Security of FIPS 140-2.

Security Requirements	Level
Cryptographic Module Specification	3
Module Ports and Interfaces	3
Roles, Services, and Authentication	3
Finite State Model	3
Physical Security	3
Operational Environment	N/A
Cryptographic Key Management	3
EMI / EMC	3
Self-Tests	3
Design Assurance	3
Mitigation of other Attacks	N/A
Overall	3

Table 1: Module Security Level Specification

Cryptographic Algorithms

The following algorithms are used all capacities: 4GB, 8GB, and 16GB

Approved Algorithm	CAVP Certificate	Use
AES 256 bit CBC	#1514	Encryption / decryption of data (used on all drive capacities)
SHA 256 hash	#1728	Password hash DRBG
SP800-90 hash DRBG	#177	Creation of encryption key

Table 2 – Approved algorithms

Non-Approved Algorithms

A hardware-based random number generator is used to seed hash_DRBG FIPS approved algorithm.

Cryptographic Module Specification

The Aegis Secure Key module is a multi-chip standalone cryptographic module, as defined by FIPS 140-2 and consists of an Initio 1861 USB controller, NAND Flash memory and a Microchip PIC16LF1825 security controller. All components are packaged in opaque, production grade integrated circuit packaging. The cryptographic boundary is defined as the boundary of the module's metal enclosure (see Figure 1)

Module Interfaces

The cryptographic module provides the following physical ports and logical interfaces:

Physical Port	Logical Interface Definition	Description
USB Port	- Data input - Data output - Control input - Status output	Send and receive control / data packets that support the standard mass storage class. Control and status parameters are only those required to support the USB protocol. No connection exists between a locked drive and host computer.
Alphanumeric buttons	- Data input	Connects to PIN input buttons used for PIN entry to security controller.
Key button	- Control input	Connects to Key button used to wake module from sleep state, identify role, and terminate PIN entry.
LEDs 3 ea. (RGB)	- Status output	See table 3 for status states
Power	- USB	+5 volts from USB port charges internal battery

Table 3 – Physical ports and logical interfaces

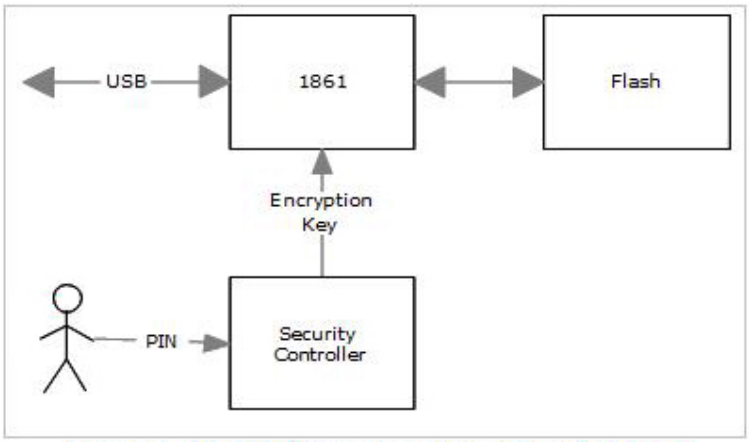

Figure 2 - Main component architecture of Aegis Secure Key

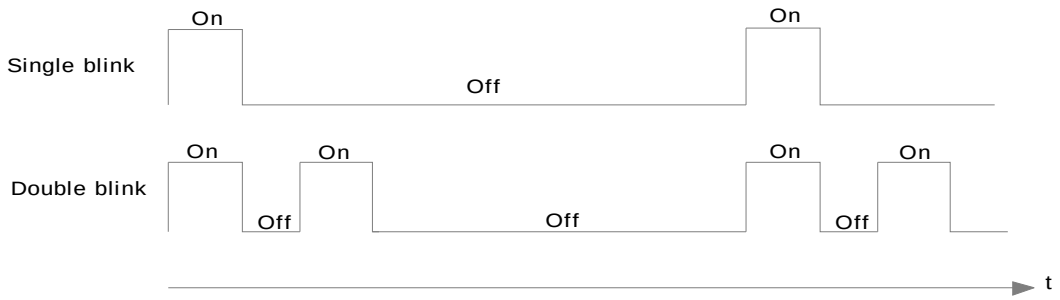

Figure 3 - Blinking patterns for user and crypto-officer

LED State	Description
Red single blink	Module is locked, inaccessible
Green single blink	Module unlocked in user mode
Green double blink	Module unlocked in CO mode
Red constant state	No user PIN defined
All indicators off	Module is in sleep state
Red & Green in constant state	Change of PIN initiated
Red & Green concurrent single blink	Accepting user PIN input
Red & green concurrent double blink	Accepting CO PIN
Blue constant state	USB controller has logical connection with host
Blue blinking	Data packets being read / written
Red & Green fade on and off	Unit failed power-on self test. Module can no longer be used.

Table 4 – Status Output

Roles and Services

Aegis Secure Key supports level 3 identity based authentication.

Role	Authentication Type	Authentication Data	Description
User	Identity-based operator authentication	7-15 digit PIN	User has full access to all services.
Crypto-officer	Identity-based operator authentication	7-15 digit PIN	CO has full access to all services. Plus can zeroize user PIN.

Table 5 – Roles and required identification and authentication

The Aegis Secure Key drive comes with a preset user PIN of 1-1-2-2-3-3-4-4 and comes formatted from the factory with an encryption key generated by hash_DRBG.

The Aegis Secure Key supports 2 distinct and separate roles: user and cryptographic officer. The role is explicitly selected during authentication:

- User – press KEY button, enter valid PIN, press KEY
- CO – double press KEY to identify CO, enter valid PIN, press KEY

Operator	Services
User role	- Open private partition to allow read/write access - Lock private partition to disallow read/write access - Set user PIN - Change user PIN - Read/write to private partition
CO role	- Open private partition to allow read/write access - Lock private partition to disallow read/write access - Set CO PIN - Change CO PIN - Read/write to private partition - Zeroize user PIN
Unauthenticated (no role required)	- Show status - Self-tests - Zeroize all crypto-parameters

Table 6 – Services authorized for each role

Authentication

The Crypto Officer and User roles authenticate via the module's keypad. There is no visible display of Crypto Officer or User authentication data during data entry.

PIN Strength

Authentication strength of both user and CO is determined by a 7 digit PIN (minimum PIN length). Probability of a random guess is slightly more than 10^7 or 1/10,000,000*. The user is locked out after 10 consecutive login failures. The probability of guessing 10 consecutive tries is 1/1,000,000.

> *Note: Sequential and repeating PINs are not allowed. For example, the unit will reject a PIN of 1-2-3-4-5-6-7 or 6-5-4-3-2-1-0. Attempts to define such a PIN will cause the unit to indicate an error.*

PIN lengths up to 15 digits are allowed.

Critical Security Parameters

CSP	Description
AES encryption key	256 bit key used encrypt the entire drive and generated by the hash_DRBG algorithm
User PIN	Used to authenticate user.
Crypto-officer PIN	Used to authenticate CO.
hash_DRBG states	Intermediate values such as V, C, and nonce
hash_DRBG seed	Seed values for DRBG

Table 7 - Critical security parameters

CSP definitions

CSP	Use	Creation	Storage	Destruction	Privileges
AES Key	Encryption / Decryption	SP800-90 DRBG output	RAM of both USB and security controllers; EEPROM	Zeroization	User and CO
User PIN	Authenticate User	Defined by user	Created in RAM and compared to EEPROM	Zeroization	User
CO PIN	Authenticate CO	Defined by user	Created in RAM and compared to EEPROM	Zeroization	CO
Hash_DRBG intermediate values (V, C, nonce)	Creating random numbers	Upon drive reset	RAM	Zeroization or battery removal	User and CO
hash_DRBG seed	Seeding RNG	Based on timer / button press events	RAM	Used only once then destroyed	User and CO

Table 8 - Services to CSP mapping

Zeroization

Zeroization occurs upon the detection of a brute-force attack: 10 consecutive unsuccessful attempts to unlock. Variables are zeroized by writing a value of 0xFF to all byte locations.

Power-On Self-Tests

Self-tests are run upon emerging from a sleep state (when the KEY button is pressed). If one of the self-tests fail, the module will enter an error state and no services are available.

- Firmware CRC
- AES KAT (encryption and decryption)
- SHA-256 KAT
- hash_DRBG KAT

Conditional Self-tests

- Continuous test on NDRNG and DRBG

Security Rules

This section documents the security rules enforced by the cryptographic module to implement the security requirements of FIPS 140-2 level 3:

1. The cryptographic module provides two distinct operator roles: user and cryptographic officer.

2. The cryptographic module provides identity-based authentication.

3. When the module has not been placed in a valid role, the operator shall not have access to any cryptographic service.

4. The cryptographic module performs the following tests:

   a) Power on self-tests
      i. AES known answer test
      ii. Firmware integrity test (16 bit cyclic redundancy check)
      iii. hash_DRBG known answer test
      iv. SHA256 known answer test as part of hash_DRBG KAT

   b) Conditional tests
      i. hash_DRBG continuous random number generator test
      ii. NDRNG continuous random number generator test

5. The operator shall be capable of commanding the module to perform the power-up self-test at any time by waking the module from sleep mode.

6. Data output is inhibited during self-tests, zeroization, and authentication.

7. No CSPs are ever output in any form from the module.

Physical Security Policy

The multi-chip standalone cryptographic module includes the following physical security mechanisms:

- Production grade components
- Hard, opaque epoxy covering all security relevant components
- EEPROM memory protect fuse is set in the security controller (disables the ability to externally read memory contents)
- Flash memory protect fuse set (disables the ability to externally read memory contents)

The operator should, on a periodic basis, visually inspect the module to determine if it has been compromised. The following steps should be followed:

- Grasp module in one hand and lightly pull the lanyard with the opposite hand
- If the module separates, the operator should suspect that the module has been tampered with
- If the module remains intact, no tamper should be suspected

Note: The module epoxy hardness testing was only performed at ambient temperature; no assurance is provided for level 3 hardness conformance at any other temperature.

10. Mitigation of Other Attacks Policy

The module has not been designed to mitigate attacks not addressed by the security requirements of FIPS 140-2.

References

Reference Number	Reference Title
[1]	FIPS PUB 140-2 Security Requirements for Cryptographic Modules / NIST May 2001
[2]	Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program / NIST May 22, 2008
[3]	FIPS PUB 800-90 Recommendation for Random Number Generation Using Deterministic Random Bit Generators May 2011