FSM-2 Flash Storage Cryptographic Module

Hardware Version Number: A8
Firmware Version: 4.0

FIPS 140-2 Non-Proprietary Security Policy

Document Version: 1.1
Last Update: 2021-4-19

Prepared by:
Gossamer Security Solutions
9176 Red Branch Road, Suite L,
Columbia, MD 21045
www.gossamersec.com

Table of Contents

1 Introduction

1.1 Purpose

This is a non-proprietary cryptographic module Security Policy for the FSM-2 Flash Storage Cryptographic Module from Curtiss-Wright Defense Solutions. The firmware version running on the module is v4.0. This Security Policy describes how the module meets the security requirements of Federal Information Processing Standards (FIPS) Publication 140-2, which details the U.S. and Canadian Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the National Institute of Standards and Technology (NIST) and the Canadian Centre for Cyber Security (CCCS) Cryptographic Module Validation Program (CMVP) website at https://csrc.nist.gov/projects/cryptographic-module-validation-program.

This document also describes how to run the module in a secure FIPS-Approved mode of operation. This policy was prepared as part of the Level 2 FIPS 140-2 validation of the modules. The FSM-2 Flash Storage Cryptographic Module, which includes the hardware version, is referred to in this document as FSM-2 or the module.

1.2 Module Validation Level

The following table lists the level of validation for each area in the FIPS PUB 140-2.

No.	Area Title	Level
1	Cryptographic Module Specification	2
2	Cryptographic Module Ports and Interfaces	2
3	Roles, Services, and Authentication	3
4	Finite State Model	2
5	Physical Security	2
6	Operational Environment	N/A
7	Cryptographic Key management	2
8	Electromagnetic Interface/Electromagnetic Compatibility	2
9	Self-Tests	2
10	Design Assurance	2
11	Mitigation of Other Attacks	N/A
	Overall module validation level	**2**

Table 1. Module Validation Level

1.3 References

This document deals only with operations and capabilities of the module in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the module from the following sources:

- The Curtiss-Wright website (http://www.curtisswright.com) contains information on the full line of products from Curtiss-Wright. The website (https://www.curtisswrightds.com/products/) contains information on the full line of products from Curtiss-Wright Defense Solutions.
- The CMVP website (https://csrc.nist.gov/projects/cryptographic-module-validation-program) contains contact information for individuals to answer technical or sales-related questions for the module.

1.4 Terminology

In this document, the Curtiss-Wright FSM-2 Storage Cryptographic Module identified is referred to as the Cryptographic Module, Module or FSM-2.

1.5 Document Organization

The Security Policy document is one document in a FIPS 140-2 Submission Package provided to the test laboratory. In addition to this document, the Submission Package contains:

- Vendor Evidence Document
- Finite State Model
- Validation Submission Summary
- Other supporting documentation as additional references

This Security Policy and other validation submission documentation were produced by Gossamer Security Solutions under contract to Curtiss-Wright. With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Submission Package is proprietary to Curtiss-Wright and is releasable only under appropriate non- disclosure agreements. For access to these documents, please contact Curtiss-Wright.

2 FSM-2 Flash Storage Cryptographic Module

This section describes the FSM-2 Flash Storage Cryptographic Module from Curtiss-Wright Defense Solutions.

2.1 Overview

Curtiss-Wright Defense Solutions, a division of Curtiss-Wright Corporation, is the trusted, proven leader for comprehensive, rugged, and secure mission-critical solutions for defense and aerospace applications. The Defense Solutions business unit produces the FSM-2 Flash Storage Cryptographic Module.

The FSM-2 (Figure 1) is a rugged, compact data storage device that can be plugged into any chassis that accommodates conduction-cooled modules with a 3U form factor.

It uses a frame and covers to create the conduction cooled enclosure.

Figure 1. FSM-2 Flash Storage Cryptographic Module

The FSM contains 2 TB of solid-state memory utilizing SLC NAND flash components. The design includes over-provisioning for faster write operations and improved reliability. It also supports dynamic and static data wear-leveling for even distribution of erase/write cycles. This prevents excessive writes to the same locations extending the life cycle of the flash.

The FSM-2 supports key generation, user authentication and authorization, and full disk encryption using Advanced Encryption Standard (AES). Key management can be handled internally on the FSM-2 controller PCB or externally by a host system.

The frame and covers are designed to dissipate component heat, provide rigidity, and move heat to the outer enclosure. This closed conduction-cooled structure makes the FSM-2 less susceptible to problems due to adverse environments and provides silent vibration-free operation. The module complies with standards for a 3U (6.3-inch/160-mm) wide 1-inch pitch form factor.

2.2 Module Specification

The FSM-2 is a hardware module with a multi-chip embedded embodiment. The overall security level of the module is 2. The module supports two types of FIPS-Approved modes of operation. Instructions on how to invoke these two modes of operation are provided in Section 3.2.

2.3 Cryptographic Boundary

The module's cryptographic boundary is the same as the physical boundary, which is defined by the anodized aluminum covers that enclose the module and surround all the hardware and software components. It includes the "top," "front," "left," "right," "rear" and "bottom" surfaces of the case representing the module's physical perimeter.

2.4 Module Interfaces

The FSM-2 supports the four logical interfaces defined in FIPS 140-2: Data Input, Data Output, Control Input, and Status Output. In addition, the module supports a Power Input interface. Figure 2 shows the FSM-2 physical ports, controls, and indicators. Table 2 explains the mapping of the module's physical ports to the FIPS logical interfaces.

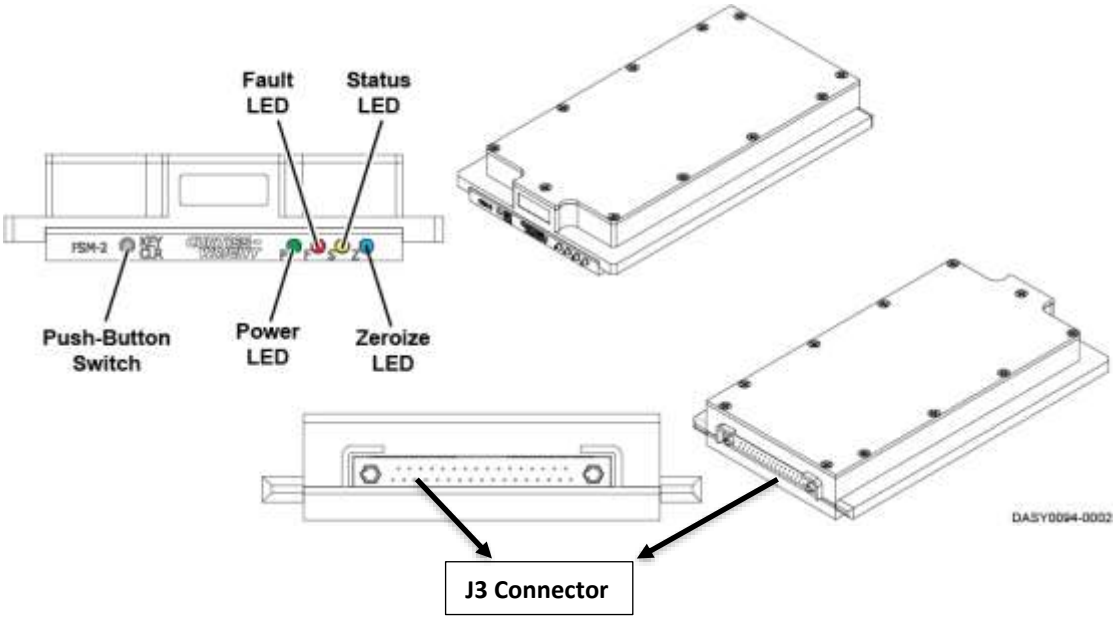

Figure 2. FSM-2 Connector, Control, and Indicators Locations

J3 Connector Pin	Signal Name	Logical Interface	Active / Reserved	Description
1, 3	5V_IN	Power Input	Active	+5V power supply
2	RS232_TX	Data Output, Control Input, Status Output	Reserved	PIN NOT USED (reserved for RS-232 - Host Management [Transmit]).
4	RS232_RX	Data Input, Control Input, Status Output	Reserved	PIN NOT USED (reserved for RS-232 - Host Management [Receive]).
5	ERROR_ST	Status Output	Active	FSM-2 ERROR Status - Asserted HI to indicate an error.

6	ZEROIZE_BP	Control Input	Active	Assert this pin HI to zeroize the FSM-2
7	EXT_I2C_SCL	Control Input	Active	I2C Clock
9	EXT_I2C_SDA	Data Input & Output, Control Input, Status Output	Active	I2C Data
8	SYS_RST_IN	Control Input	Active	System Reset - Assert pin low to reset FSM-2 unit
10, 11, 16, 17, 22, 23, 28, 29	GROUND	Power Return	Active	Digital Ground
12, 14	HOST_3TX+/-	Data Input	Active	SATA Data Lane 3 - Host Transmit
18, 20	HOST_2TX+/-	Data Input	Active	SATA Data Lane 2 - Host Transmit
24, 26	HOST_1TX+/-	Data Input	Active	SATA Data Lane 1 - Host Transmit
30, 32	HOST_0TX+/-	Data Input	Active	SATA Data Lane 0 - Host Transmit
13, 15	HOST_3RX+/-	Data Output	Active	SATA Data Lane 3 - Host Receive
19, 21	HOST_2RX+/-	Data Output	Active	SATA Data Lane 2 - Host Receive
25, 27	HOST_1RX+/-	Data Output	Active	SATA Data Lane 1 - Host Receive
31, 33	HOST_0RX+/-	Data Output	Active	SATA Data Lane 0 - Host Receive

Table 2. Hardware/Physical Boundary Interfaces

2.5 Roles, Services, and Authentication

In both FIPS-Approved modes, the module supports Identity-based authentication by using UserID and Password. The module can be accessed via the serial console interface located on the I2C data interface. As required by FIPS 140-2, there are two roles that operators may assume: Crypto Officer role and User role. The CO installs the module and can execute all of the module's services. The User can execute a subset of the module's services. Both the CO and User manage the device by authenticating to the module and issuing commands through the User Control Interface (UCI). Descriptions of the services available in each Approved mode are provided in Table 3 below. The approved mode that the service is available in is shown in the "Security Mode" column. Please note that the CSPs listed in the table indicate the type of access required using the following notation:

- R – Read: The plaintext CSP is read by the service.
- W – Write: The CSP is established, generated, modified, or zeroized by the service.
- X – Execute: The CSP is used within an Approved or allowed security function or authentication mechanism.

The User and Crypto Officer passwords and all shared secrets must each be at a minimum eight (8) characters long. Passwords are ONLY alphanumeric - numbers, lowercase, uppercase. NO special characters (!@#$%^&*..etc). Passwords must be between 8-64 characters with 1 upper, 1 lower, and 1 number. See the Secure Operation section for more information. Given these restrictions, the probability of randomly guessing the correct sequence is one (1) in 6,193,057,944,320 (this calculation is based on the assumption that the typical standard American QWERTY computer keyboard has 10 Integer digits, 26 Upper and 26 Lower alphabetic characters providing 62 characters to choose from in total). The calculation should be 62x62x62x62x62x26x26x10 = 6,193,057,944,320. Therefore, the associated probability of a successful random attempt is approximately 1 in 6,193,057,944,320, which is less than the 1 in 1,000,000 required by FIPS 140-2.

In addition, for multiple attempts to use the authentication mechanism during a one-minute period, under the optimal modern network condition, if an attacker would only get 60,000 guesses per minute. Therefore, the associated probability of a successful random attempt during a one-minute period is 60,000/ 6,193,057,944,320= 1/ 103,217,632, which is less than 1 in 100,000 required by FIPS 140-2.

Service	Role	Security Mode	Description	CSP and Type of Access
Push Button Switch	CO User	1, 2	Zeroize keys, configuration data, and all user authentication data via front panel	All Keys and CSPs
Security Trigger	CO User	1, 2	Zeroize keys, configuration data, and all user authentication data via backplane signal	All Keys and CSPs
System Reset	CO User	1, 2	Reboot the module via backplane signal	All Keys and CSPs stored in the DRAM listed in table 5
Sanitize (UCI)	CO User	1, 2	Zeroize keys, configuration data, and all user authentication data	All Keys and CSPs
Clear DEK (UCI)	CO User	1, 2	Zeroize DEK only	DEK – W
Clear Key (UCI)	CO User	1, 2	Zeroize all keys and CSPs stored in the module.	All Keys and CSPs
Clear all (UCI)	CO User	1, 2	Zeroize all cryptographic keys including the hardcoded PSK, configuration data, and all user authentication data	All Keys and CSPs
Setup user accounts (UCI)	CO	1, 2	Display, create, modify, or delete user accounts	Passwords – W
Set security mode (UCI)	CO	1, 2	Specify if DEK is entered into module or generated internally. A security mode change causes zeroization.	DEK – W KEK – W Passwords – W

Table 3. Mapping of Services to Roles, Inputs, Outputs, CSPs, and Type of Access

Service	Role	Security Mode	Description	CSP and Type of Access
View temperature status (UCI)	CO User	1, 2	Display output from temperature sensors	None
View DEK status (UCI)	CO User	1, 2	Display DEK load status and storage location	None
View KEK status (UCI)	CO User	1, 2	Display KEK load status and storage locations	None
View FSM ID (UCI)	CO User	1, 2	Display the FSM module ID	None

View Security Mode (UCI)	CO User	1, 2	View the current security mode of the FSM	None
View error status (UCI)	CO User	1, 2	Display error conditions (including POSTs and BISTs) and log history	None
Clear error status (UCI)	CO	1, 2	Clear log history	None
Logoff (UCI)	CO User	1, 2	Logoff	None
Generate KEK (UCI)	CO	1, 2	Generate a new KEK	KEK - RWX
Store KEK (UCI)	CO	1, 2	Stores the latest generated KEK	KEK-R
Output KEK (UCI)	CO	1, 2	Output KEK wrapped with PSK or an old KEK (PSK is only used if there is no previous KEK stored in the module)	KEK - RWX PSK – RX
Generate DEK (UCI)	CO	1	Generate DEK internally and storage	DEK – RW
Enter DEK (UCI)	CO	2	DEK (wrapped with KEK) entry and storage	DEK – RW KEK – RWX
Set password (UCI)	CO User	1, 2	Set passwords	Password – RW

Table 4. Mapping of Services to Roles, Inputs, Outputs, CSPs, and Type of Access (Continued)

2.6 Unauthenticated Services

The services for someone without an authorized role are to view the status output from the module's LED pins, perform the zeroization service by pushing the KeyCLR button, and cycle the power.

2.7 Operational Environment

The module is a hardware module. The module's operating system is nonmodifiable operating system. Thus, the requirements from FIPS 140-2 level 2, section 4.6.1, are not applicable to the module.

2.8 Cryptographic Key/CSP Management

The Crypto Officer administers both cryptographic keys and other critical security parameters such as passwords. All keys and CSPs are protected by the password-protection of the Crypto Officer login. Zeroization consists of overwriting the memory that stored the key or refreshing the volatile memory. Keys are electronically entered and distributed. The entropy source (NDRNG) within the module provides at least 256 bits of entropy to seed SP800-90a DRBG for use in key generation. The cryptographic keys and other CSPs used by the module in both FIPS-Approved modes are shown in Table 5 below.

Name	CSP Type	Size	Description/Generation/Derivation	Storage	Zeroization
DRBG entropy input	SP800-90A HMAC_DRBG (HMAC-SHA-256)	440-bits	This is the entropy for SP 800-90A HMAC_DRBG (HMAC-SHA-256). This key is established from the module's entropy source and used to construct the seed. This key is never output from the module.	DRAM (plaintext)	Please see section 3.5 in this document.
DRBG seed	SP800-90A HMAC_DRBG (HMAC-SHA-256)	440-bits	Input to the DRBG that determines the internal state of the DRBG. Generated using DRBG derivation function that includes the entropy input from the entropy source. This key is never output from the module.	DRAM (plaintext)	Please see section 3.5 in this document
DRBG V	SP800-90A HMAC_DRBG (HMAC-SHA-256)	128-bits	The DRBG V is one of the critical values of the internal state upon which the security of this DRBG mechanism depends. Generated first during DRBG instantiation and then subsequently updated using the DRBG update function. This key is never output from the module.	DRAM (plaintext)	Please see section 3.5 in this document
DRBG key	SP800-90A HMAC_DRBG (HMAC-SHA-256)	256-bits	Internal critical value used as part of SP 800-90A HMAC_DRBG (HMAC-SHA-256). Established per SP 800-90A HMAC_DRBG. This key is never output from the module.	DRAM (plaintext)	Please see section 3.5 in this document
PSK (Pre-shared key)	Secret	256-bits	This key is hard coded in the module during manufacturing. This key is never output from the module.	NVRAM (plaintext)	Please see section 3.5 in this document
KEK (Key encryption key)	AES-KW	256-bits	This key is generated by calling approved SP800-90A DRBG. This key can be output from the module wrapped with PSK if there is no previously generated KEK existing in the module. or wrapped with the existing KEK in the module.	DRAM (plaintext)	Please see section 3.5 in this document
DEK (Data encryption key)	AES	256-bits	This key can be generated by calling approved SP800-90A DRBG internally in Security Mode 1, or injected from outside wrapped with KEK in Security Mode 2. This key is never output from the module.	NVRAM (encrypted by Wrap key)	Please see section 3.5 in this document
HMAC key	HMAC-SHA-256	256-bits	This key is generated by calling approved SP800-90A DRBG. It is used for message authentication. This key is never output from the module.	DRAM (plaintext)	Please see section 3.5 in this document

Name	CSP Type	Size	Description/Generation/Derivation	Storage	Zeroization
CO/User password	Password	64 to 512-bits	Used to authenticate the CO or User. In addition, the password is also used to derive Wrap key with SP800-132 PBKDF algorithm. This CSP is never output from the module.	DRAM (plaintext)	Please see section 3.5 in this document
PBKDF Salt	Keying material	256-bits	This key is generated by calling approved SP800-90A DRBG. This keying material is used for derive the Wrap key in compliance with SP800-132 PBKDF. This key is used to protect the DEK in the NVRAM. It is never output from the module.	NVRAM (plaintext)	Please see section 3.5 in this document
Wrap key	SP800-132 PBKDF	320-bits	The module generates this key in compliance with SP800-132 PBKDF with HMAC-SHA-256 and a number of iterations and a 256-bits salt to transform the operator's password. This key is used to protect the DEK. It is never output from the module.	DRAM (plaintext)	Please see section 3.5 in this document

Table 5. Cryptographic Keys and CSPs

2.9 Cryptographic Algorithms

The module implements a variety of approved and non-approved algorithms.

Approved Cryptographic Algorithms

The module supports the following FIPS 140-2 approved algorithm implementations:

Algorithm	Curtiss-Wright Crypto Firmware	Enova HW
AES (256 bits; ECB)	Cert. #5767	
AES (256 bits; CBC)		Cert. #250
DRBG (HMAC-SHA-256_DRBG)	Cert. #2362	
HMAC (SHA-256)	Cert. #3815	
KTS (AES-KW)	AES Cert. #5767	
SHS (SHA-256)	Cert. #4590	
CKG (vendor affirmed)	N/A	
PBKDF (vendor affirmed)	N/A	

Table 6. Approved Cryptographic Algorithms and Associated Certificate Number

Note:

- There are key sizes that have been CAVP tested but not used by the module. Only the key lengths/curves/moduli shown in this table are used by the module.

- In accordance with FIPS 140-2 IG D.12, the cryptographic module performs Cryptographic Key Generation as per scenario 1 of section 6 in SP800-133. The resulting generated symmetric key is the unmodified output from SP800-90A HMAC_DRBG.

- The module deploys a SP800-132 Password Based Key Derivation Function (PBKDF).
  - The module complies with Option 1a within SP800-132.
  - The minimum password length is set between 8-64 characters with 1 upper, 1 lower, and 1 number.
  - The module generates ephemeral Wrap Key (referred to Master Key in SP800-132) by passing a Password and associated KDF salt though an underlying pseudorandom function (HMAC-SHA-256).
  - The function has an iteration count of 10,000.
  - The module uses the SP800-90A HMAC_DRBG to generate unique 256-bit salts.
  - The module generates and assigns a unique MEK and KEK to each LBA Band.
  - The sole use of a Wrap Key is to protect the Data Encryption Key (DEK), which was stored in the NVRAM. Please note that both Wrap Key and DEK cannot be output and shall not leave the module.

Non-FIPS Approved, but Allowed Algorithms in FIPS Mode
The module supports the following non-FIPS approved, but allowed in the FIPS approved mode.

- NDRNG (entropy source)

Non-Approved Cryptographic Algorithms
The module does not support non-approved/allowed cryptographic algorithm.

2.10 Self-Tests

The modules include an array of self-tests that are run during startup and periodically during operations to prevent any secure data from being released and to ensure all components are functioning correctly.

Self-tests performed

- Curtiss-Wright Crypto Firmware POSTs
  - AES-ECB Encrypt/Decrypt KATs
  - AES-KW Encrypt/Decrypt KATs
  - DRBG KATs (Note: DRBG Health Tests as specified in SP800-90A Section 11.3 are performed)
  - Firmware Integrity Test (EDC)
  - HMAC-SHA-256 KAT
  - SHA-256 KAT

- Enova HW POST
  - AES-CBC Encrypt/Decrypt KATs

- Curtiss-Wright Crypto Firmware Conditional tests
  - CRNGT for SP800-90A DRBG
  - CRNGT for NDRNG

The module performs all power-on self-tests automatically when the power is applied. If an error occurs during a power-up self-test, the module will enter a critical error state. Data output from the module will be inhibited. The module will log the error into an error log and the Fault LED will illuminate. To correct the error, the CO must restart the module.

2.11 Physical Security

Four tamper-evident labels are applied by the vendor during manufacturing. Upon initialization of the module, the Crypto Officer shall visually inspect the labels to ensure that they are in the proper locations and that they do not show any signs of tampering. Labels will be placed on the two center screws located on the top and bottom of the module. Figures 3-8 below show the proper seal placement for the module. Actions to be taken when any evidence of tampering should be addressed within the site security program. Any deviation of the TELs placement by unauthorized operators such as tearing, misconfiguration, removal, change, replacement or any other change in the TELs from its original configuration as depicted below shall mean the module is no longer in FIPS mode of operation. The device must be returned to Curtiss-Wright for service before it can operate in the Approved mode of operation again. Below are the photos for the module with TELs while in the FIPS mode of operation.

Figure 3. FSM-2 Front view

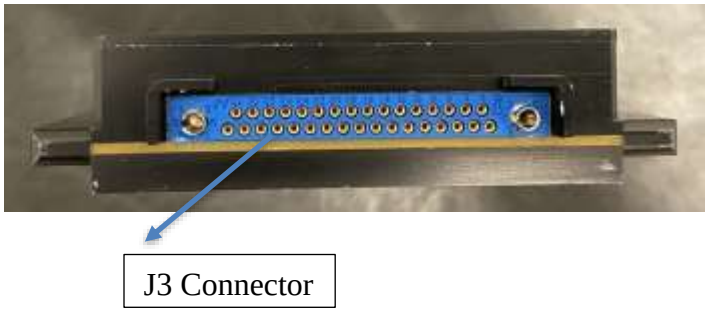

Figure 4: FSM-2 Back view

Figure 5: FSM-2 Left view

Figure 6: FSM-2 Right view

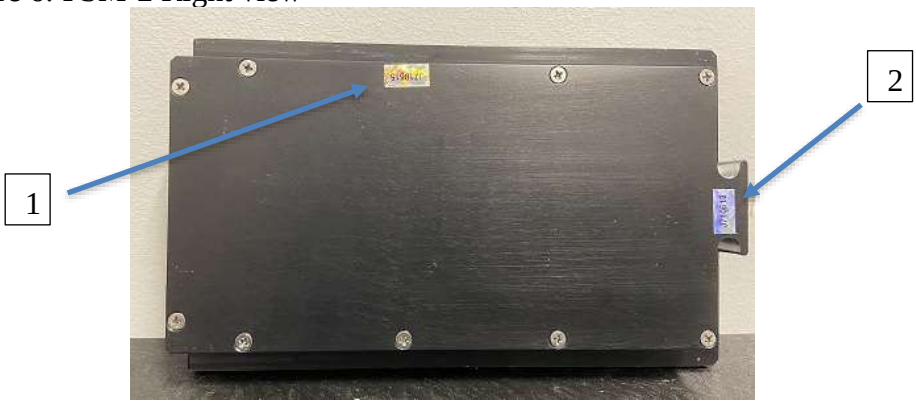

Figure 7: FSM-2 Top view

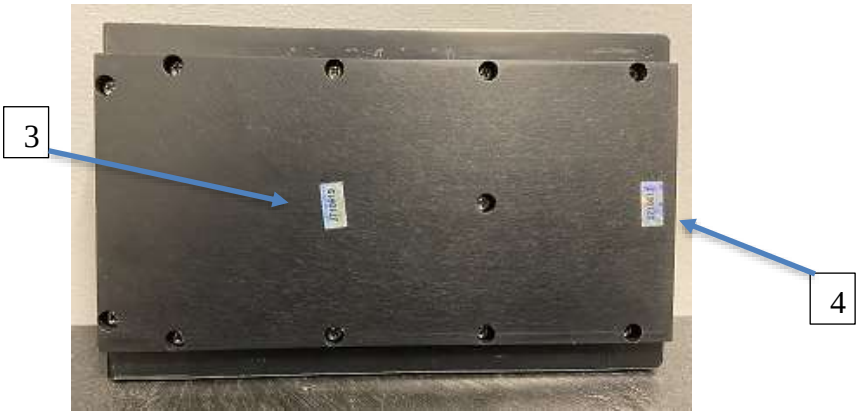

Figure 8: FSM-2 Bottom view

3 Secure Operation

The sections below describe how the module operates in the FIPS mode.

3.1 Multiple Approved Modes

The module supports two FIPS-Approved modes of operation, which are defined as Security Mode 1 and Security Mode 2. Section 3.2 provides instructions on how to configure the module in one of the two Approved modes. The description of the two Approved modes is provided in Section 3.2 (step #5) and Section 3.4.

3.2 Initial Set-up

The module meets Overall Level 2 requirements for FIPS 140-2. The firmware version running in the module is 4.0, which is the only allowed firmware in FIPS mode. The firmware was programmed into the module while in manufacturing. Follow the setting instructions provided below to operate the module in each FIPS-approved mode of operation. Operating this module without maintaining the following settings will remove the module from the FIPS approved mode of operation. The steps are summarized below.

1. After unpacking the module, a physical inspection should be conducted to:
   - Identify any damage to the assemblage or tamper-evident seals
   - Verify the correct seating of all screws and front panel switches.

2. The FSM-2 is not a freestanding device. Therefore, mount the module into a chassis frame that can accommodate a 1-inch pitch bay with slots for conduction-cooled module. Align the FSM-2 module rails with the chassis slides and push the FSM-2 module in until the connector makes contact. Apply pressure on the FSM-2 module handles to seat the connector into the backplane connector.

3. Establish serial communication to the device using I2C bus.

4. Ensure that the firmware version 4.0 is running in the module (This is the only allowed firmware version in FIPS mode)

5. Configure the module by:

   - There is no default login username and password
   - Creating CO and User accounts (See Section 3.3)
   - Setting the Security Mode (see Section 3.3 below)
   - In Internal Key Generation Mode (Security Mode 1), request the module to generate an AES encryption key
   - In External Key Generation Mode (Security Mode 2), enter an externally generated AES encryption key into the module.

3.3 CO and User Account Setup

The Crypto Officer is responsible for initialization and security-relevant configuration and management of the module. The CO shall configure the module security mode, the storage device for the DEK, and a CO username and password. Passwords shall be between 8 and 64 characters and must consist of at least 1 upper- and lower-case letters and 1 number. The first account created is always the CO and during account creation, the user specifies which key generation mode they desire. The CO will then log on using the newly set credentials. The current firmware does not support RS-232 therefore the FSM> prompt does not exist. If any future customer desires this, then we would need to activate the RS-232 lines to interface with the FSM-2. The CO may then add additional User accounts.

3.4 Secure Management

The module operates in FIPS-Approved mode when used as specified within this Security Policy. Each mode defines how the Data Encryption Key (DEK) used for SATA device protection is generated. Following each power cycle, the FSM-2 software will determine the appropriate key generation mode to determine the method of injecting the DEKs. The key generation method for each security mode is described below:

- Internal Key Generation Mode (Security Mode 1) - Data Encryption Key (DEK) for SATA flash storage is to be generated internally. The CO commands the module to generate DEK directly from the output of HMAC_DRBG (Cert. #2362), and then injects it into the hardware encryptor.

- External Key Generation Mode (Security Mode 2) - Data Encryption Key (DEK) for SATA flash storage is to be generated externally and entered into the module wrapped with KEK. The CO enters the encrypted DEK with its associated HMAC into the module, and then injects it into the hardware encryptor.

Please note that switching between security modes requires the user to zeroize all stored cryptographic Keys/CSPs listed in Table 5, and create a new CO account (See Section 3.3.2). Upon entering the new security mode, the module will perform the power-up self-tests to all supported algorithms listed in Section 2.10.

3.5 Zeroization

Cryptographic keys are zeroized in DRAM memory upon power-up after the module is power-cycled or rebooted. Keys and all other CSPs stored NVRAM can be zeroized by the following methods:

- Pressing the Push Button Switch on the front panel (labeled KEY CLR)
- Sending a Security Trigger signal from the host device via the backplane connector.
- Using the “Sanitize” services as listed in Table 3.
- Using the “Clear DEK” service as listed in Table 3. This only zeroizes the DEK used to protect the data stored on flash.
- Automatic zeroization of keys and CSPs occurs when changing the security mode, which designates if the DEK is internally generated or externally entered into the module.
- The FSM-2 module is able to be zeroized via the KEY CLR button after main power is off for up to 30 minutes. The CO or User must wait until the module has been successfully returned a success or error in order to verify that zeroization has completed.