Curtiss-Wright Controls Defense Solutions

3U VPX-1TB FSM Flash Storage Module

Hardware Part Number: RHFS-3UR1024-F, RHFS-3UJ1024-F, Firmware Version: 1.11

FIPS 140-2 Non-Proprietary Security Policy

FIPS Security Level: 2
Document Version: 1.2

Prepared for:

Curtiss-Wright Controls Defense Solutions
2600 Paramount Place, Suite 200
Fairborn, OH 45324
United States of America

Phone: +1 (937) 252-5601
http://www.cwcdefense.com

Prepared by:

Corsec Security, Inc.
13135 Lee Jackson Memorial Highway, Suite 220
Fairfax, Virginia 22033
United States of America

Phone: +1 (703) 267-6050
http://www.corsec.com

Table of Contents

Table of Figures

List of Tables

1 Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the 3U VPX-1TB FSM Flash Storage Module from Curtiss-Wright Controls Defense Solutions. This Security Policy describes how the 3U VPX-1TB FSM Flash Storage 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 Communications Security Establishment Canada (CSEC) Cryptographic Module Validation Program (CMVP) website at http://csrc.nist.gov/groups/STM/cmvp.

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 3U VPX-1TB FSM Flash Storage Module, which includes both hardware versions, is referred to in this document as VPX3-FSM or the module.

1.2 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 (http://www.cwcdefense.com) contains information on the full line of products from Curtiss-Wright Controls Defense Solutions.
- The CMVP website (http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm) contains contact information for individuals to answer technical or sales-related questions for the module.

1.3 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 the other validation submission documentation were produced by Corsec Security, Inc. 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 VPX3-FSM

This section describes the 3U VPX-1TB FSM Flash Storage Module from Curtiss-Wright Controls Defense Solutions.

2.1 Overview

Curtiss-Wright Controls Defense Solutions is the Motion Control business segment of Curtiss-Wright Corporation. It manufactures sophisticated, high-performance mechanical actuation and drive systems, specialized sensors, motors, and electronic controller units, and mission-critical embedded computing components and control systems. With manufacturing facilities that span the globe, Curtiss-Wright Controls delivers cost-effective and innovative products and services to its diverse customer base, including the aerospace, defense, and industrial markets. Their proven technical expertise and industry-leading capabilities provide complex motion control subsystems that operate at maximum performance and efficiency levels. The Defense Solutions business unit of Curtiss-Wright Controls, which produces the 3U VPX-1TB FSM Flash Storage Module, creates and integrates state-of-the-art rugged electronics for aerospace and defense applications.

2.1.1 3U VPX-1TB FSM Flash Storage Module

The VPX3-FSM is a rugged, compact, and efficient one TB[1] data storage device that complies with the VITA[2] 46/48 standards. It is a VPX-REDI[3] Type 2 module that can be plugged into any VPX[4] chassis that accommodates conduction-cooled modules with a 3U[5] form factor and only requires 5-volts from the VPX backplane. The VPX3-FSM is available in two hardware configurations, supporting either a single SATA[6] lane (RAID[7]0) (Hardware Version: RHFS-3UR1024-F) or four independent SATA lanes (JBOD[8]) (Hardware Version: RHFS-3UJ1024-F). The VPX3-FSM unit can augment or replace an existing rotating data storage device in a VPX chassis and provide greater reliability due to its solid-state storage and conduction-cooled structure.

Figure 1 represents the 3U VPX-1TB FSM Flash Storage Module in both configurations. A label with the VPX3-FSM hardware version number is placed on the upper-left corner of up the bottom cover for quick identification of the module.

[1] TB – Terabyte
[2] VITA – VME International Trade Association
[3] VPX-REDI – Versatile Performance Switching-Ruggedized Enhanced Design Implementation
[4] VPX – Versatile Performance Switching
[5] U – Rack Unit
[6] SATA – Serial Advanced Technology Attachment
[7] RAID – Redundant Array of Independent Disks
[8] JBOD – Just a Bunch Of Drives

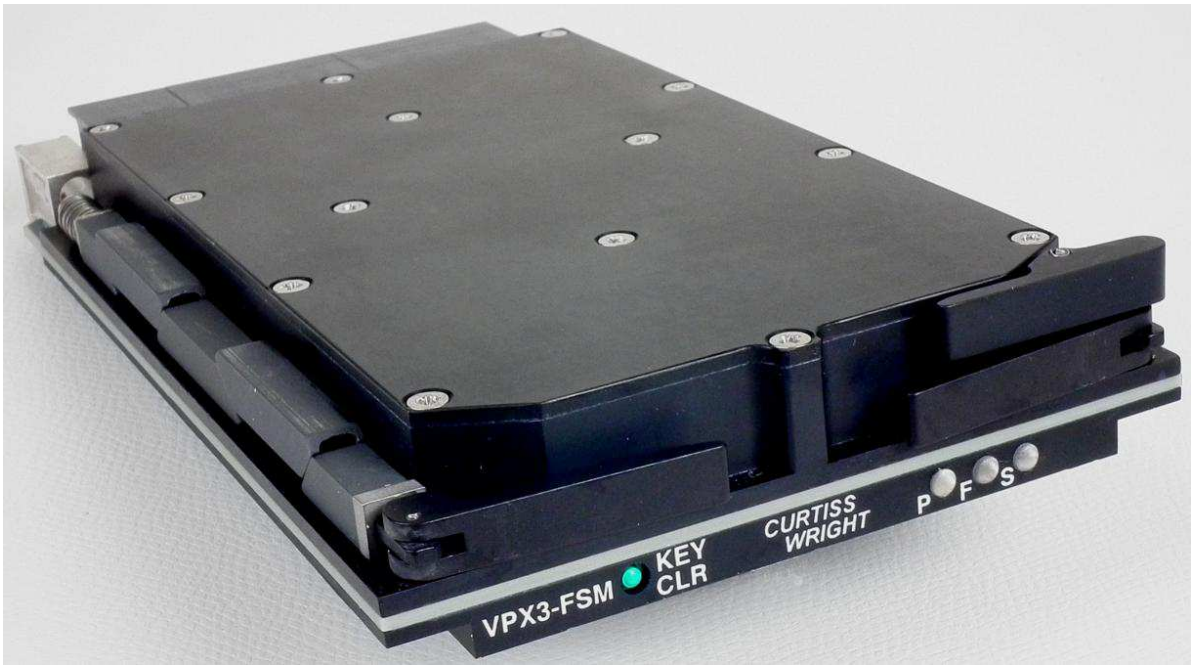

Figure 1 – 3U VPX-1TB FSM Flash Storage Module

The VPX3-FSM provides an effective capacity after flash over-provisioning of 800 GB[9] of solid-state memory utilizing SLC[10] NAND[11] 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 VPX3-FSM supports key generation, user authentication and authorization, and full disk encryption using Advanced Encryption Standard (AES). Key management can be handled internally on VPX3-FSM or externally by a host system. An on-board microcontroller monitors temperature, power, and error conditions. The internal structure is designed to dissipate component heat, provide rigidity, and move heat to the outer enclosure. This closed conduction-cooled structure makes the VPX3-FSM less susceptible to problems due to adverse environments and provides silent vibration-free operation.

The 3U VPX-1TB FSM Flash Storage Module is validated at the following FIPS 140-2 Section levels:

Table 1 – Security Level Per FIPS 140-2 Section

Section	Section Title	Level
1	Cryptographic Module Specification	3
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

[9] GB – Gigabyte
[10] SLC – Single-Level Cell
[11] NAND – Not AND

Section	Section Title	Level
7	Cryptographic Key Management	2
8	EMI/EMC[12]	2
9	Self-tests	2
10	Design Assurance	3
11	Mitigation of Other Attacks	N/A

2.2 Module Specification

The 3U VPX-1TB FSM Flash Storage Module is a hardware module with a multi-chip embedded embodiment. The overall security level of the module is 2. The module supports two FIPS-Approved modes of operation. The first Approved mode of operation is defined as *Security Mode 1* and generates an AES Data Encryption Key (DEK) internally. The second Approved mode of operation is defined as *Security Mode 2*. *Security Mode 2* does not generate an AES DEK internally; instead it accepts externally generated DEKs. Instructions on how to invoke these two modes are provided in Section 3.2.

The cryptographic boundary of the 3U VPX-1TB FSM Flash Storage Module is defined by the anodized aluminum covers that enclose the module and surround all the hardware and software components. Please note that references to the module in this document refer to both the RAID0 and JBOD versions of the module.

2.3 Module Interfaces

The VPX3-FSM 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. Table 2 explains the mapping of the module's physical ports to the FIPS interfaces and Figure 2 and Figure 3 depict the physical ports of the VPX3-FSM.

Table 2 – Mapping of VPX3-FSM Physical Interfaces to FIPS 140-2 Logical Interfaces

Physical Port	VPX Port	Description	FIPS 140-2 Interfaces
VPX 5V	P0	Connection to VPX chassis for power supply	Power Input
I2C[13] Primary	P0	I2C system management	Data Input, Data Output, Control Input, Status Output
System Reset	P0	Reboot signal from host via VPX backplane	Control Input
+3.3V auxiliary supply	P0	Auxiliary power supply	Power Input
VBAT	P1	Battery voltage power supply	Power Input
SATA Lane 4	P1	SATA transmit and receive	Data Input, Data Output
SATA Lane 5	P1	SATA transmit and receive	Data Input, Data Output

[12] EMI/EMC – Electromagnetic Interference / Electromagnetic Compatibility
[13] I2C – Inter-Integrated Circuit

Physical Port	VPX Port	Description	FIPS 140-2 Interfaces
SATA Lane 0	P2	SATA transmit and receive	Data Input, Data Output
SATA Lane 1	P2	SATA transmit and receive	Data Input, Data Output
SATA Lane 2	P2	SATA transmit and receive	Data Input, Data Output
SATA Lane 3	P2	SATA transmit and receive	Data Input, Data Output
RS232	P2	Serial communications	Data Input, Data Output, Control Input, Status Output
I2C Secondary	P2	I2C system management	Data Input, Data Output, Control Input, Status Output
Security Trigger	P2	External trigger signal from host via VPX backplane to zeroize keys and user account information	Control Input
RTM CardFail Signal	P2	Asserted when: Internal or external error condition	Status Output
RTM Status Signal	P2	Indicates when AES key is loaded into encryption processor	Status Output
Push Button Switch	N/A	Front panel button to zeroize keys and user account information (labeled KEY CLR on front panel)	Control Input
Fault LED[14]	N/A	Asserted when: Internal or external error condition	Status Output
Power LED	N/A	Illuminates GREEN when module is powered up	Status Output
Status LED	N/A	Illuminates YELLOW when an AES key has been successfully loaded for encryption/decryption processing	Status Output

[14] LED – Light Emitting Diode

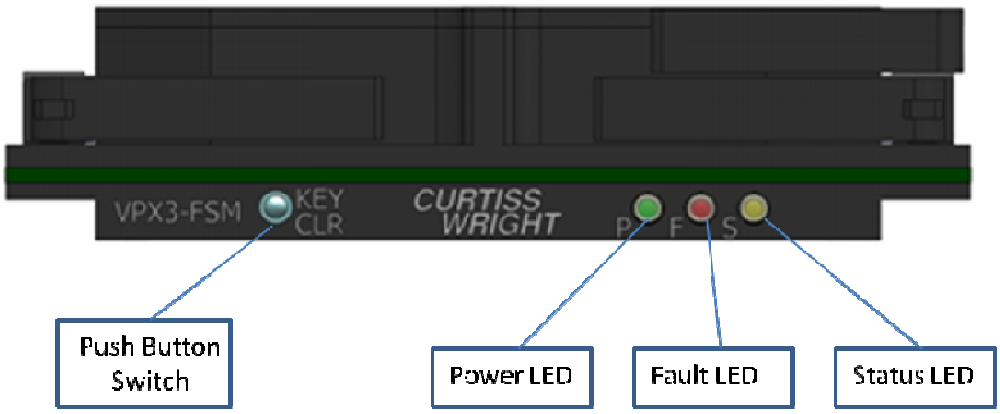

Figure 2 – VPX3-FSM Front Panel Port Interfaces

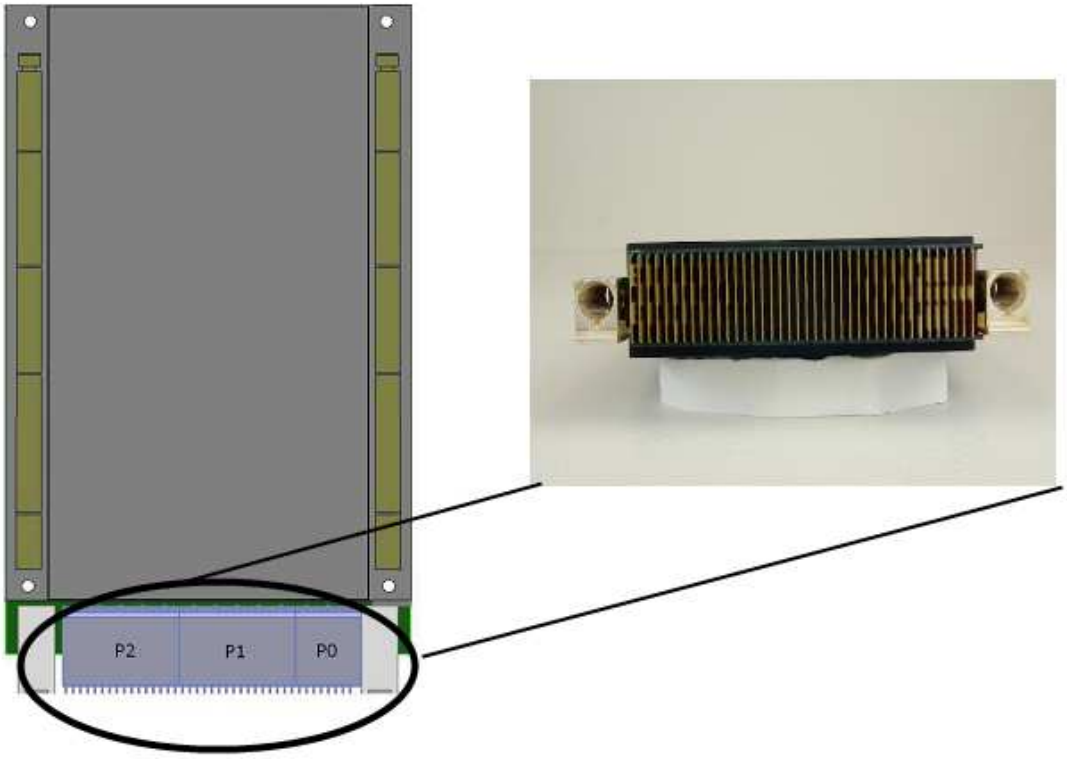

Figure 3 – VPX3-FSM VPX Port Location

2.4 Roles and Services

In both FIPS-Approved modes, the module supports identity-based authentication and authorization using a Userid and password. There are two roles in the VPX3-FSM (as required by FIPS 140-2) that operators

may assume: a Crypto Officer (CO) role and a 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 via the RS232 or I2C ports 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[15] 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.*

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

Service	Role	Security Mode	Description	Input	Output	CSP and Type of Access
Push Button Switch	CO User	1, 2	Zeroize keys, configuration data, and all user authentication data via front panel	Command	Status	DEK – W KEK[16] – W Passwords – W
Security Trigger	CO User	1, 2	Zeroize keys, configuration data, and all user authentication data via VPX backplane signal	Command	Status	DEK – W KEK – W Passwords – W
System Reset	CO User	1, 2	Reboot the module via VPX backplane signal	Command	Status	None
Sanitize (UCI)	CO User	1, 2	Zeroize keys, configuration data, and all user authentication data	Command	Status	DEK – W KEK – W Passwords – W
Clear DEK (UCI)	CO User	1, 2	Zeroize DEK only	Command	Status	DEK – W
Clear Key (UCI)	CO User	1, 2	Zeroize DEK only, DEK+KEK, or DEK+KEK+Passwords	Command	Status	KEK – W DEK – W Passwords – W
Clear all (UCI)	CO User	1, 2	Zeroize keys, including the PSK[17], configuration data, and all user authentication data	Command	Status	DEK – W KEK – W PSK – W Passwords – W
Setup user accounts (UCI)	CO	1, 2	Display, create, modify, or delete user accounts	Command	Status	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.	Command	Status	DEK – W KEK – W Passwords – W
Generate DEK (UCI)	CO	1	Generate and store a new DEK	Command	Status	DEK – RW

[15] CSP – Critical Security Parameter
[16] KEK – Key Encryption Key
[17] PSK – Pre-Shared Key

Service	Role	Security Mode	Description	Input	Output	CSP and Type of Access
Generate KEK (UCI)	CO	1, 2	Generate a new KEK. Encrypts new KEK with old KEK and exports it	Command	Status, key	KEK - RWX
Store KEK (UCI)	CO	1, 2	Stores the latest generated KEK	Command	Status	KEK-R
Enter DEK (UCI)	CO	2	DEK entry and storage	Command, key	Status	DEK – RW KEK – RWX PSK – RX
Set password (UCI)	CO User	1, 2	Set/change passwords	Password	Status	Password – RW
Select SATA port configuration	CO User	1, 2	Configure SATA port configuration	Command	Status	None
Select UCI communication port (UCI)	CO User	1, 2	Display or configure communication settings	Command	Status	None
Set I2C slave address (UCI)	CO	1, 2	I2C node address setup	Command	Status	None
View SATA connection status (UCI)	CO User	1, 2	Display SATA lane configuration	Command	Status	None
View temperature status (UCI)	CO User	1, 2	Display output from temperature sensors	Command	Status	None
View DEK status (UCI)	CO User	1, 2	Display DEK load status and storage location	Command	Status	None
View KEK status (UCI)	CO User	1, 2	Display KEK load status and storage locations	Command	Status	None
View FSM ID (UCI)	CO User	1, 2	Display the FSM module ID	Command	Status	None
View Security Mode (UCI)	CO User	1, 2	View the current security mode of the FSM	Command	Status	None
View error status (UCI)	CO User	1, 2	Display error conditions (including POST[18]s and BIST[19]s) and log history	Command	Status	None
Clear error status (UCI)	CO	1, 2	Clear log history	Command	Status	None
Logoff (UCI)	CO User	1, 2	Logoff	Command	None	None

2.4.1 Authentication

The 3U VPX-1TB FSM Flash Storage Module supports identity-based authentication to control all of the services it provides. To access the services on the module for each approved mode, the operator must

[18] POST – Power-On Self-Test
[19] BIST – Built-In Self-Test

provide the correct Userid and password combination to the module in order to gain access to the module. Each username is a unique identity to each operator of the module. The Userid provides access to either CO or User services depending on the role that it was assigned. CO and User account setup is covered in Section 3.2.1.

2.4.1.1 Authentication Data Protection

The VPX3-FSM does not allow the disclosure, modification, or substitution of authentication data to unauthorized operators. Authentication data can only be modified by the operator who has assumed the CO role.

2.4.1.2 Authentication Mechanism Strength

Passwords created for the CO and User shall be between 8 and 15 characters long and may consist of upper- and lower-case letters and numbers, for a total character space of 62 characters. There are, at minimum, 62^8 ($2.18x10^{14}$) possible password combinations. This means there is a 1 in $2.18x10^{14}$ chance that a random access attempt will succeed, surpassing the 1 in 1,000,000 requirement.

User accounts will be locked out after 10 contiguously failed login attempts. After an account is locked out, the CO must log in and reset the password for that Userid. Because user accounts are locked out after only 10 attempts, the probability of guessing the password to a Userid in a one minute period is less than 1 in 100,000.

2.5 Physical Security

The 3U VPX-1TB FSM Flash Storage Module is a multi-chip embedded cryptographic module. The module consists of production-grade components that include standard passivation techniques. The VPX3-FSM enclosure is constructed of two custom-machined 6061-T6 anodized aluminum covers. The top and bottom covers enclose this assembly and fasten together to form a rugged conduction-cooled VPX U3, 1" pitch data storage device. The case is sealed using tamper-evident warranty labels in order to prevent the covers from being removed without signs of tampering.

2.6 Operational Environment

The operational environment requirements do not apply to the 3U VPX-1TB FSM Flash Storage Module.

2.7 Cryptographic Key Management

The module implements the FIPS-Approved algorithms listed in Table 4 below in both FIPS-Approved modes of operation.

Table 4 – FIPS-Approved Algorithm Implementations

Algorithm	Certificate Number
Symmetric Key Algorithm	
AES-CBC, 128-, 192-, and 256-bit key sizes (hardware implementation)	#250
AES-ECB 256-bit key sizes (software implementation)	#1978
Secure Hashing Algorithm (SHA)	
SHA-256	#1732

Algorithm	Certificate Number
Message Authentication Code (MAC) Function	
HMAC-SHA-256	#1191
Deterministic Random Bit Generator (DRBG)	
SP 800-90 HMAC_DRBG	#180

The module also implements the following non-Approved algorithm which is allowed in the FIPS-Approved mode of operation:

- TRNG (True Random Number Generator; as the entropy source for SP800-90 HMAC_DRBG)

The cryptographic keys and other CSPs used by the module in both FIPS-Approved modes are shown in Table 5 below:

Table 5 – VPX3-FSM Keys, Key Components, and CSPs

CSP/Key	Type	Input	Output	Storage	Zeroization	Use
PSK (Pre-shared key)	AES 256-bit key	Pre-installed at factory	Never	Plaintext in RAM[20] or EEPROM[21]	See Section 3.3.2	Encrypt the KEK
KEK (Key encryption key)	AES 256-bit key	Generated internally	Encrypted with PSK or KEK	Plaintext in RAM, SRAM[22], or EEPROM	See Section 3.3.2	Decrypt the DEK
DEK (Data encryption key)	AES 256-bit key	Encrypted with KEK or generated internally	Never	Plaintext in RAM, SRAM, or EEPROM	See Section 3.3.2	Encrypt and decrypt the data on SATA flash
HMAC key	HMAC SHA-256 key	Generated internally	Never	Plaintext in RAM	See Section 3.3.2	Message Authentication with SHS[23]
CO/User password	Password	Plaintext	Never	Plaintext in RAM, SRAM, or EEPROM	See Section 3.3.2	Login to the UCI for module management
DRBG seed	Random value	Generated internally	Never	Plaintext in RAM	See Section 3.3.2	Seed input to SP 800-90 HMAC_DRBG

[20] RAM – Random Access Memory
[21] EEPROM – Electrically Erasable Programmable Read-Only Memory
[22] SRAM – Static Random Access Memory
[23] SHS – Secure Hash Standard

2.8 Self-Tests

2.8.1 Power-Up Self-Tests

In both FIPS-Approved modes, the 3U VPX-1TB FSM Flash Storage Module performs the following self-tests at power-up:

- Firmware integrity check (16-bit CRC[24])
- Known Answer Tests (KATs)
    - AES encryption and decryption
    - SHA-256
    - HMAC-SHA-256
    - HMAC_DRBG

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.

2.8.2 Conditional Self-Tests

In both FIPS-Approved modes, the 3U VPX-1TB FSM Flash Storage Module performs the following conditional self-tests:

- Continuous Random Number Generator (RNG) test for HMAC_DRBG
- Continuous RNG test for TRNG

If an error occurs during a conditional 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.

2.9 Mitigation of Other Attacks

This section is not applicable. The module does not claim to mitigate any attacks beyond the FIPS 140-2 Level 2 requirements for this validation.

[24] CRC – Cyclic Redundancy Check

3 Secure Operation

The 3U VPX-1TB FSM Flash Storage Module meets Level 2 requirements for FIPS 140-2. The sections below describe how to place and keep the module in FIPS-approved mode of operation.

3.1 Multiple Approved Modes

The 3U VPX-1TB FSM Flash Storage Module provides two FIPS-Approved modes of operation. The two Approved modes of operation 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. A description of the two Approved modes is provided in Section 3.3.

3.2 Initial Set-up

Sections 3 and 4 of the *VPX3-FSM FIPS Flash Storage Module User Guide* provide detailed instructions on how to unpack, install, and setup the module for the first time. The steps are summarized below.

1. After unpacking the module, a physical inspection should be conducted to:
    a. Identify any damage to the assemblage or tamper-evident seals
    b. Verify the correct seating of all screws and front panel switches.
2. The VPX-FSM is not a freestanding device. Therefore, mount the module into a VPX chassis frame that can accommodate a 3U, 1" pitch bay with wedgelock slots for conduction-cooled modules. Push the wedgelock handles in until each wedgelock expands enough to make contact with the conduction cooled chassis rails and verify the board is locked in place.
3. Establish serial communication to the device using either the RS-232 connection or I2C bus.
4. Configure the module by:
    a. Establishing CO and User accounts (See Section 3.2.1)
    b. Selecting the VPX I/O SATA lanes
    c. Setting the *Security Mode* (see Section 3.3 below)
    d. Selecting a storage option for the AES encryption key
    e. In *Security Mode 1*, request the module to generate an AES encryption key
    f. In *Security Mode 2*, enter an externally generated AES encryption key into the module.

3.2.1 CO and User Account Setup

The startup account on the VPX3-FSM unit is “guest” with a default password of “xxxxxxxx”. After logging in as “guest”, another login prompt appears. At this point, the CO will configure the module security mode, the storage device for the DEK, and a CO (Admin) username and password. Passwords shall be between 8 and 15 characters and may consist of upper- and lower-case letters and numbers. The CO will then log on using the newly set Admin credentials. The “FSM>” prompt will appear indicating that initial log on and account establishment has been completed. The CO may then add additional CO or User accounts. The “guest” Userid and default password are deleted after the first successful authentication by the CO. The “guest” Userid and password will be available again after zeroization.

3.3 Secure Management

The module operates in FIPS-Approved mode when used as specified within this Security Policy. The “mode” command will report if the module is in the FIPS-Approved mode. The *VPX3-FSM FIPS Flash Storage Module User Guide* specifies two *Security Modes* for the VPX3-FSM that both operate in FIPS-Approved mode. Each mode defines how the SATA flash encryption key management is performed. Following each power cycle or key zeroization, the VPX3-FSM software will determine the appropriate *Security Mode* to run based on configuration settings. The *Security Modes* are defined as follows:

- *Security Mode 1* – AES encryption key for SATA flash storage is to be generated internally.
  - When operating in *Security Mode 2*, the CO can issue the "`mode 1`" command to switch to this Approved mode*
- *Security Mode 2* – AES encryption key for SATA flash storage is to be generated externally and entered into the module.
  - When operating in *Security Mode 1*, the CO can issue the "`mode 2`" command to switch to this Approved mode*

* Switching between security modes will cause the module to reboot and zeroize all stored keying material (See Section 3.3.2). Upon entering the new security mode, the module will perform the power-up self-tests listed in Section 2.8.1.

3.3.1 Initialization

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. Figure 4 and Figure 5 show the proper seal placement for the module.

Figure 4 – VPX3-FSM Tamper-Evident Seal Placement (Top)

Figure 5 – VPX3-FSM Tamper-Evident Seal Placement (Bottom)

3.3.2 Zeroization

Cryptographic keys are zeroized in memory upon power-up after the module is power-cycled or rebooted. Keys and all other CSPs stored in SRAM or EEPROM 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 VPX backplane
- 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 AES encryption key will be internally generated or externally entered into the module.
- Automatic zeroization of keys and CSPs occurs when battery power is too low.

If the Push Button Switch is pressed or the Security Trigger is activated when the module is powered off, then zeroization will occur upon power up. The CO or User must wait until the module has been successfully rebooted in order to verify that zeroization has completed. The VPX3-FSM monitors the zeroization process, and if the process is interrupted, it will begin again upon reboot or power up.

3.4 CO and User Guidance

The Crypto Officer is responsible for initialization and security-relevant configuration and management of the module. Both the CO and User shall examine the enclosure regularly and see if there are signs of tamper attempts. If damage to the tamper-evident seals is found, then the device is not considered operating in the Approved mode of operation. The device must be returned to Curtiss-Wright for service before it can operate in the Approved mode of operation again.

4 Acronyms

Table 6 describes the acronyms used in this document.

Table 6 – Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
ASCII	American Standard Code for Information Interchange
BIST	Built-In Self-Test
CBC	Cipher Block Chaining
CMVP	Cryptographic Module Validation Program
CO	Crypto Officer
CSEC	Communications Security Establishment Canada
CSP	Critical Security Parameter
DRBG	Deterministic Random Bit Generator
DEK	Data Encryption Key
EEPROM	Electrically Erasable Programmable Read-Only Memory
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FIPS	Federal Information Processing Standard
GB	Gigabyte
HMAC	(Keyed-) Hash Message Authentication Code
I2C	Inter-Integrated Circuit
I/O	Input/Output
JBOD	Just a Bunch Of Drives
KAT	Known Answer Test
KEK	Key Encryption Key
LED	Light Emitting Diode
MAC	Message Authentication Code
NAND	Not AND
NIST	National Institute of Standards and Technology
NVLAP	National Voluntary Laboratory Accreditation Program
POST	Power-On Self-Test
PSK	Pre-Shared Key
RAID	Redundant Array of Independent Disks
RAM	Random Access Memory

Acronym	Definition
REDI	Ruggedized Enhanced Design Implementation
RNG	Random Number Generator
SATA	Serial Advanced Technology Attachment
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
SLC	Single-Level Cell
SRAM	Static Random Access Memory
TB	Terabyte
TRNG	True Random Number Generator
U	Rack Unit
UCI	User Control Interface
VITA	VMEbus International Trade Association
VME	Versa Module Eurocard
VPX	Versatile Performance Switching

Prepared by:
Corsec Security, Inc.

13135 Lee Jackson Memorial Highway, Suite 220
Fairfax, Virginia 22033
United States of America

Phone: +1 (703) 267-6050
Email: info@corsec.com
http://www.corsec.com