Hewlett-Packard Enterprise Development LP

HPE P-Class Smart Array RAID Controllers

Hardware Models: P230i, P430, P431, P731m, P830, and P830i
Firmware Version: 1.66

FIPS 140-2 Non-Proprietary Security Policy

FIPS Security Level: 2
Document Version: 0.11

Prepared for:

Hewlett-Packard Enterprise Development LP
11445 Compaq Center Dr. W.
Houston, TX 77070
United States of America

Phone: +1 (281) 370-0670
http://www.hpe.com

Prepared by:

Corsec Security, Inc.
13921 Park Center Road, Suite 460
Herndon, VA 20171
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 HPE P-Class Smart Array RAID Controllers (Hardware Models: P230i, P430, P431, P731m, P830, and P830i; Firmware Version: 1.66) from Hewlett-Packard Enterprise Development LP This Security Policy describes how the HPE P-Class Smart Array RAID Controllers meet 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 U.S. National Institute of Standards and Technology (NIST) and Canada's Communications Security Establishment (CSE) Cryptographic Module Validation Program (CMVP) website at http://csrc.nist.gov/groups/STM/cmvp.

This document also describes how to run the modules 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 HPE P-Class Smart Array RAID Controllers are referred to in this document as Smart Array Controllers, crypto modules, or the modules.

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 modules from the following sources:

- The HPE website (http://www.hp.com) contains information on the full line of products from HPE.
- 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. In addition to this document, the Submission Package contains:

- Vendor Evidence document
- Finite State Model document
- Other supporting documentation as additional references

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

2 HPE P-Class Smart Array RAID Controllers

2.1 Overview

The HPE P-Class Smart Array RAID Controllers are a family of serial-attached SCSI[1] host bus adapters that provide intelligent control for storage array. The controllers can be card-based or embedded within an HPE server, and provide a high-speed data path, on-board storage cache, remote management, and encryption of data at rest. Additional drives can be easily added to increase capacity. The purpose of the controller is to transform an application's high-level 'read' or 'write' disk operations into the individual instructions required for a RAID[2] array using an embedded RAID-on-Chip (ROC) processor. Disk operations are protected in transit via the Smart Array Controllers' on-board memory cache that acts as a buffer for disk input/output operations. When a controller detects a power loss, any data in the cache is written to the flash memory for retrieval when the power returns.

Caching allows the controller to use write-back caching that informs the operating system of a completed write when data is written to the cache instead of waiting until it is written to disk. Smart Array Controllers also implement a read-ahead caching algorithm that detects sequential read activity and predicts when a sequential-read will follow. This allows the controller to anticipate data needs and reduce wait times. The read-ahead caching is disabled when a non-sequential read activity is detected to reduce any slowdown for random read requests.

Controllers can be stand-up cards, mezzanine, or embedded within an HPE server. Each controller contains a PCIe[3] connector, multiple serial attached SCSI (SAS) ports, and a cryptographic state LED[4]. Controllers can have factory- or user-installed physical security kits that include hardcovers and tamper-evident seals. The HPE server provides a Smart Storage Administrator GUI and CLI that are used to manage the controllers. For a list of servers compatible with the HPE P-Class Smart Array RAID Controllers, refer to the *HPE Smart Array Controllers Compatibility Matrix for HPE Gen8 Servers* datasheet.

The Smart Array Controllers provide encryption for data at rest. Each controller includes a PMC-Sierra ASIC[5] that generates the keys to be used for encryption. The controllers utilize a front-end strategy to encrypt all host data. Data from the host first enters the encryption engine before moving to the cache module and then to the RAID storage. The controllers also include a key management framework for managing disk encryption keys. Each logical drive in the storage array is encrypted with its own disk encryption key. These keys are then encrypted with a second key for storage on the drive. Smart Array stores keys in encrypted form in multiple locations to provide data storage that is secure and mobile.

The HPE P-Class Smart Array RAID Controllers are validated at the FIPS 140-2 Section levels shown in Table 1.

Table 1 – Security Level Per FIPS 140-2 Section

Section	Section Title	Level
1	Cryptographic Module Specification	2
2	Cryptographic Module Ports and Interfaces	2
3	Roles, Services, and Authentication	2

[1] SCSI – Small Computer System Interface
[2] RAID – Redundant Array of Independent Disks
[3] PCIe – Peripheral Copmonent Interconnect Express
[4] LED – Light Emitting Diode
[5] ASIC – Application-Specific Integrated Circuit

Section	Section Title	Level
4	Finite State Model	2
5	Physical Security	2
6	Operational Environment	N/A
7	Cryptographic Key Management	2
8	EMI/EMC[6]	2
9	Self-tests	2
10	Design Assurance	2
11	Mitigation of Other Attacks	N/A

2.2 Module Specification

The HPE P-Class Smart Array RAID Controllers are hardware modules with a multi-chip embedded embodiment. The overall security level of the modules is 2. The cryptographic boundary of the HPE P-Class Smart Array RAID Controllers is defined by the hard metal and plastic physical security kit that surrounds all hardware and firmware components. The modules are primarily composed of the following components:

- PMC-Sierra 806X ROC processor
- Flash NVRAM[7]
- Dual in-line memory (DIMM) Module
- Bootstrap and Crypto NVRAM
- SAS Support Logic module
- PCIe Connector
- A multistate LED

In addition, there is a Manufacturing, Local, and SAS Mfg ID NVRAM that do not process any cryptographic information.

The controllers are delivered in several form factors (mezzanine card, stand-up card, daughter card, and embedded on the main logic board in an HPE Gen8 server platform) and appear in a variety of physical layouts (depending on the form factor). Each module includes the Smart Array firmware v1.66 and Express Logic's ThreadX RTOS[8] v5.5. The module firmware is stored in the Flash NVRAM until the system is initialized. After a successful integrity check the run-time firmware is unpacked and loaded onto the DIMM module for execution by the ROC. Table 2 below provides details regarding the form factor and embedded ROC for each controller model.

Table 2 – Controller Form Factor/Processor Configurations

Controller Model	Form Factor	Embedded ROC
P230i	embedded	PMC-Sierra 8062
P430	stand-up card	PMC-Sierra 8061
P431	stand-up card	PMC-Sierra 8061

[6] EMI/EMC – Electromagnetic Interference / Electromagnetic Compatibility
[7] NVRAM – Non-Volatile Random Access Memory
[8] RTOS – Real-Time Operating System

Controller Model	Form Factor	Embedded ROC
P731m	mezzanine card	PMC-Sierra 8061
P830	stand-up card	PMC-Sierra 8064
P830i	daughter card	PMC-Sierra 8064

The modules implement the FIPS-Approved algorithms listed in Table 3 below.

Table 3 – FIPS-Approved Algorithm Implementations

Algorithm	Certificate Number		
	PM8601	PM8602	PM8604
AES[9] ECB[10], encryption/decryption with 256-bit keys	#2902	#2903	#2904
XTS[11,12,13]-AES encryption/decryption with XTS_256-bit keys	#2902	#2903	#2904
SHA[14]-256	#2442	#2443	#2444
HMAC[15] with SHA-256	#1837	#1838	#1839
SP[16] 800-90A CTR DRBG[17]	#529	#530	#531

The modules include the FIPS-Approved Password-Based Key Derivation Function (PBKDF2) specified in SP 800-132 option 2 as a key establishment technique. CO and User passwords shall be at least 10 characters to ensure a sufficient strength for the PBKDF2-derived keys. Keys derived from the PBKDF2 function shall only be used for storage applications.

The module also employs the following non-Approved algorithms:

- Non-Deterministic Random Number Generator (NDRNG) which is a free running oscillator, used to generate entropy for the CTR DRBG

2.3 Module Interfaces

The module's physical ports can be categorized into the following logical interfaces defined by FIPS 140-2:

- Data Input Interface
- Data Output Interface
- Control Input Interface
- Status Output Interface

Each interface is mapped to the module in Figure 1, which shows the physical boundary and associated interfaces.

[9] AES – Advance Encryption Service
[10] ECB – Electronic Code Book
[11] XTS – XEX-based tweaked-codebook mode with ciphertext stealing
[12] XEX – XOR-Encrypt-XOR
[13] XOR – Exclusive Or
[14] SHA – Secure Hash Algorithm
[15] HMAC – (keyed-) Hashed Message Authentication Code
[16] SP – Special Publication
[17] DBRG – Deterministic Random Bit Generator

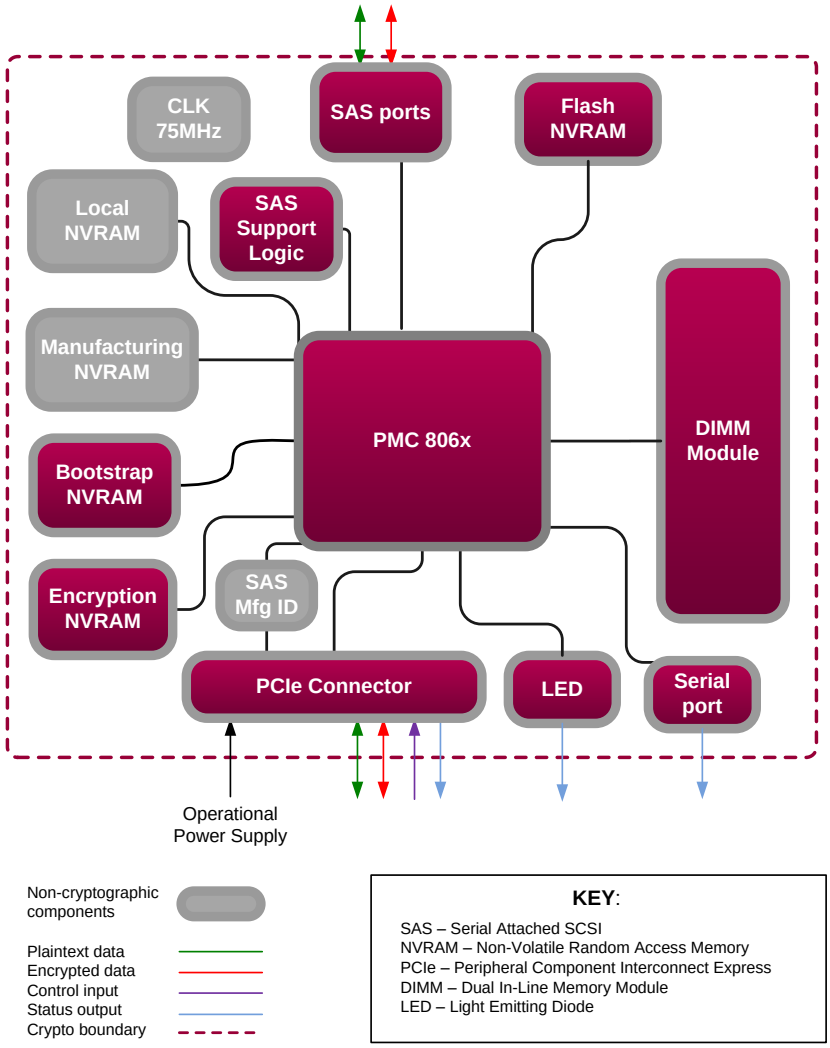

Figure 1 – HPE Smart Array Block Diagram

The HPE P-Class Smart Array RAID Controllers have the following physical interfaces (which map to the FIPS-required logical interfaces as shown in Table 4):

- PCIe connector
- SAS ports
  - P230i – 1 x4 port
  - P430 – 1 x8 port
  - P431 – 2 x4 ports
  - P731m – 4 x2 ports
  - P830 – 2 x8 ports
  - P830i – 2 x8 ports
- DIMM bus (in remote mode only)
- Multistate LED
- Serial port
- Power

Table 4 – FIPS 140-2 Logical Interface Mappings

Physical Port/Interface	FIPS 140-2 Interface
PCIe Connector	Data Input Data Output Control Input Status Output Power Input
SAS port(s)	Data Input Data Output
DIMM bus (remote mode only)	Data Input Data Output Status Output
Multistate LED	Status Output
Serial port	Status Output

2.4 Roles and Services

The modules support role-based authentication. There are two roles in each module (as required by FIPS 140-2) that operators may assume: a Crypto Officer (CO) role and a User role. Roles are assumed explicitly by means of a username and password. The password is sent with every command listed in the CO and User services. Please note that the keys and Critical Security Parameters (CSPs) listed in the table indicate the type of access required using the following notation:

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

Operator services are listed and described in Table 5.

Table 5 – Mapping of Operator Services to Inputs, Outputs, CSPs, and Type of Access

Service[18]	Operator		Description	Input	Output	CSP and Type of Access
	CO	User				
Initialize module	x		Configure the module for operation	Command and password	Command response and status output	CO password – X
Set/reset Local Master Key	x		Set or reset Local Master Key	Command and password	Command response and status output	Local Master Key – W CO password – X
Enable encryption	x		Turn encryption on for the controller as part of initialization	Command and password	Command response and status output	DEK[19] – R, X CO password – X

[18] Note that the "Show status" and "Perform self-test" services are allocated to the Crypto Officer and User roles. However, module operators are not required to assume an authorized role to perform these services, as these services do not affect the security of the module (refer to FIPS Implementation Guidance 5.2 for details).

[19] DEK – Data Encryption Key

Service[18]	Operator		Description	Input	Output	CSP and Type of Access
	CO	User				
Enable User role	x		Create User and assign a password	Command and password	Command response and status output	User password – W CO password – X
Key management mode	x		Select key management mode on GUI	Command and password	Command response and status output	Local Master Key – R, W, X CO password – X
Rekey	x		Rekey DEK	Command and parameters	Command response	DEK – R, W CO password – X
Change password	x	x	Change operator password	Command	Command response and status output	CO password – W User password – W
Lock firmware	x	x	Lock firmware so that it cannot be flashed	Command	Command response	CO password – X User password – X
Allow/Disallow plaintext logical drive creation	x		Disallow ensures all new logical drive are created with encryption enabled. Allow lets the CO choose to create plaintext volumes	Command	Command response and status output	CO password – X
Reset CO password	x		Allow CO to reset password by answering a preset security question	Command	Command response and status output	CO password – R, W
Clear Encryption	x		Zeroize all CSPs via the Clear Encryption Configuration button under utilities on the Encryption Manager GUI	Command	Command response and status output	All CSPs – W
Show status	x	x	Show status through LEDs and the Encryption Manager GUI page	None	Status output	None
Perform self-tests	x	x	Run all power-up self-tests	Reboot controller	Status output	None

2.4.1 Authentication

The modules support role-based authentication. Module operators must input a password when requesting the services listed in Table 5. Each command is passed to the module with the associated operator password. The module verifies the password to ensure the operator is authorized to perform the requested command. Table 6 lists the strength of the authentication mechanism used by the modules.

Table 6 – Authentication Mechanism

Authentication Type	Strength
Username/Password	The minimum length of the password is ten characters, with 94 different case-sensitive alphanumeric characters and symbols possible for usage. The module imposes character type and case restrictions so that the password must have a number, upper case letter, lower case letter, and special character. The remaining 6 characters could be any of the 94 choices. The chance of a random attempt falsely succeeding is 1: ($10*26*26*32*94^6$), or 1: 149,232,631,038,033,920; which is less than 1:1,000,000 as required by FIPS 140-2. In addition, the module imposes a restriction on the number of passwords that can be entered into the module. After ten failures, there is a 15 minute delay before another attempt can be made. So, in effect and at most, 10 passwords can be tried per 15 minutes. The probability that a random attempt will succeed or a false acceptance will occur in one minute is = 1 : (149,232,631,038,033,920 possible passwords / 10 passwords per minute) = 1: 14.9233 x 10^15 which is less than 1:100,000 as required by FIPS 140-2.

2.5 Physical Security

The HPE P-Class Smart Array RAID Controllers consist of production-grade components that include standard passivation techniques. Each module is pre-installed with a FIPS physical security kit that consists of metal covers for all ports and components in the module. The covers are opaque within the visible spectrum and are designed to satisfy Level 2 physical security requirements. These covers prevent visibility from the vent holes in the front of the standalone controllers. Tamper-evident seals are applied to the covers to provide physical evidence of attempts to remove the covers. The tamper-evident seals must be inspected periodically for tamper evidence. The placement of covers and tamper-evident seals can be found in the Secure Operations section of this document.

If any evidence of tampering is observed on the covers or tamper-evident seals, the module shall be considered to be in a non-compliant state. Upon such discovery, the CO shall immediately take the module out of operation and return to the vendor.

2.6 Operational Environment

The requirements in this section are not applicable. The modules do not provide a general-purpose operating system (OS) to module operators. Each module employs the ThreadX v5.5 OS, which provides only a limited operational environment. Only the modules' firmware can be executed by the modules.

2.7 Cryptographic Key Management

The controllers offer two key management modes: local or remote. In local mode, the modules generate and store all of its keys. For Approved mode operation, the modules shall be configured to operate in local key management mode. Please refer to section **Error! Reference source not found.** for the required configuration steps.

The module supports the CSPs listed in Table 7.

Table 7 – List of Cryptographic Keys, Cryptographic Key Components, and CSPs

CSP	CSP Type	Generation / Input	Output	Storage	Zeroization	Use
DEK	256-bit AES-XTS key	Generated internally	Never exits the module	Stored in plaintext in volatile DIMM module	Reboot Logical drive deleted	Used for encryption and decryption of logical drives
Crypto Officer password	10 – 16 character password	Entered electronically	Never exits the module	Stored in encrypted form in NVRAM Stored in plaintext in volatile DIMM module	Return to factory reset Reboot	Used for authenticating Crypto Officer role operators
User password	10 – 16 character password	Entered electronically	Never exits the module	Stored in encrypted form in NVRAM Stored in plaintext in volatile DIMM module	Return to factory reset Reboot	Used for authenticating User role operators
CTR_DRBG seed	384-bit random value	Generated internally	Never exits the module	Stored temporarily in volatile DIMM module in plaintext	Automatically upon completion of CTR_DRBG seed operation	Used to seed the CTR_DRBG
CTR_DRBG entropy input	256-bit random value	Generated internally	Never exits the module	Stored temporarily in volatile DIMM module in plaintext	Automatically upon completion of CTR_DRBG seed operation	Used in the process of generating a random number
Local Master Key	256-bit AES key	Derived as per SP 800-132 using PBKDF (with HMAC SHA-256)	Never exits the module	Stored in plaintext in NVRAM	Return to factory reset	Used for encryption and decryption of KEKs

2.8 EMI/EMC

HPE P-Class Smart Array RAID Controllers were tested and found conformant to the Electromagnetic Interference (EMI)/Electromagnetic Compatibility (EMC) requirements specified by 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class A (business use).

2.9 Self-Tests

Cryptographic self-tests are performed by the modules when the modules are first powered up and loaded into memory. Additional cryptographic self-tests are performed when a random number is created. The following sections list the self-tests performed by the modules, their expected error statuses, and error resolutions.

2.9.1 Power-Up Self-Tests

The HPE P-Class Smart Array RAID Controllers perform the following self-tests at power-up:

- Firmware integrity check – a 32-bit Cyclic Redundancy Check (CRC)
- Known Answer Tests (KATs)
    - AES-ECB encrypt KAT
    - AES-ECB decrypt KAT
    - AES-XTS encrypt KAT
    - AES-XTS decrypt KAT
    - SHA-256 KAT
    - HMAC SHA-256 KAT
    - CTR DRBG KAT

If any of these self-test fail, encrypted drives are taken offline and the modules enter a critical error state. An error message of the failure is logged.

2.9.2 Conditional Self-Tests

The HPE P-Class Smart Array RAID Controllers perform the following conditional self-tests:

- Continuous RNG for NDRNG
- Continuous RNG for CTR DRBG

If any of the RNG conditional self-tests fail, key generation is halted and the module enters a soft error state. The RNG is re-instantiated and the test is run a second time. If the test fails again, the module enters a critical error and all cryptographic operations are halted. An error message of each failure is logged.

2.9.3 Critical Functions Self-Tests

The following critical function tests, which are described in SP 800-90A are performed by the modules:

- DRBG Instantiate Test is performed at start-up or anytime the DRBG is instantiated.
- DRBG Generate Test is performed whenever the DRBG is requested to generate a random number.
- DRBG Reseed Test is performed whenever the DRBG is re-seeded.
- DRBG Un-instantiate test is performed whenever the DRBG is un-instantiated.

A failure of any of these tests results in a critical error for the DRBG, requiring that the module be replaced. When the DRBG is in error, no new keys can be generated.

2.10 Mitigation of Other Attacks

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

3 Secure Operation

The HPE P-Class Smart Array RAID Controllers meet Level 2 requirements for FIPS 140-2. The sections below describe how to place and keep the modules in FIPS-Approved mode of operation.

3.1 Initial Setup

The P230i and P830i controllers are pre-installed in the target server. The P430, P431, and P731m controllers must be installed in a supported server. The *HPE Smart Array P430 Controller User Guide*, *HPE Smart Array P431 Controller User Guide*, and *HPE Smart Array P731m Controller User Guide* include the sets to install the controllers in a supported server.

The modules are delivered in a non-operational factory state. The CO is responsible for installation (as applicable), initialization, and security-relevant configuration and management activities for each module. Since the modules must be configured for encrypted use only, the CO should first determine that no plaintext volumes are present at the time of initialization. If no plaintext volumes are present, the CO may begin performing the initialization steps described below. If plaintext volumes are present, the CO shall convert all plaintext volumes to encrypted volumes prior to performing those steps.

Configuration and management of the modules must be performed using the underlying server's Smart Storage Administrator (SSA) Secure Encryption GUI. The commands and buttons used in this interface translate to commands that enter the modules over the PCIe bus.

To configure the modules for their Approved mode of operation, the CO must:

1. Verify physical security mechanisms are properly installed
2. Set the CO password, key management mode, encryption mode, and disallow plaintext volumes
3. Enable volatile data encryption keys
4. Enable the User role
5. Verify and lock the firmware

Guidance for performing these tasks through the SSA GUI can be found in the *HPE Secure Encryption Installation and User Guide* and in this FIPS 140-2 Security Policy.

To initialize each module using the SSA GUI, start the HPE SSA utility and select the controller to be configured. Then follow the steps below to complete the initial setup.

- Ensure physical security mechanisms are properly installed

  The modules are delivered with physical security kits pre-installed by HP. These physical security kits include metal port/component covers and tamper-evident tape. The CO shall inspect the modules upon receipt to ensure that the kits are properly installed. Diagrams and descriptions of the installed kits are provided below.

  a. The P230i is an embedded controller and is shown in Figure 2 with the physical security kit installed. The P431 is shown with the required one (1) metal cover and three (3) strips of tamper-evident tape.

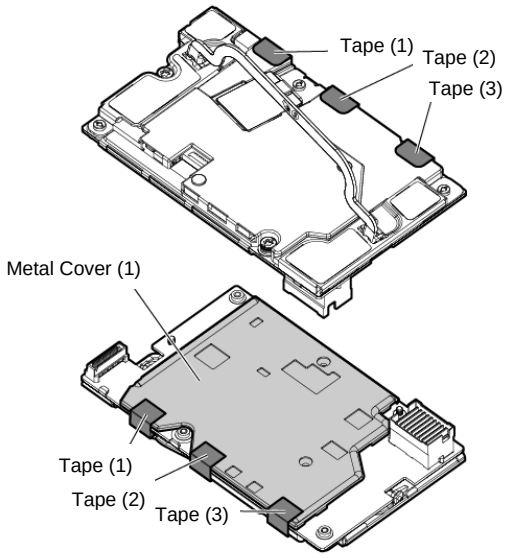

Figure 2 – P230i Controller

b. The P430 and P431 are stand-up cards and are shown in Figure 3 and Figure 4 with the physical security kit installed. The P430 is shown with the required one (1) metal cover and one (1) section of tamper-evident tape. The P431 is shown with the required one (1) metal cover and one (1) section of tamper-evident tape.

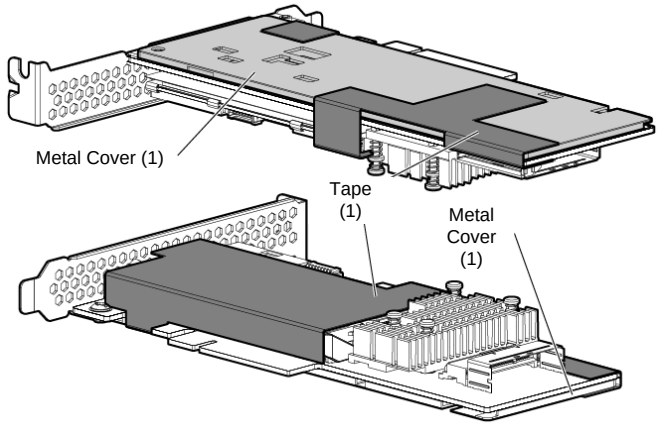

Figure 3 – P430 Controller

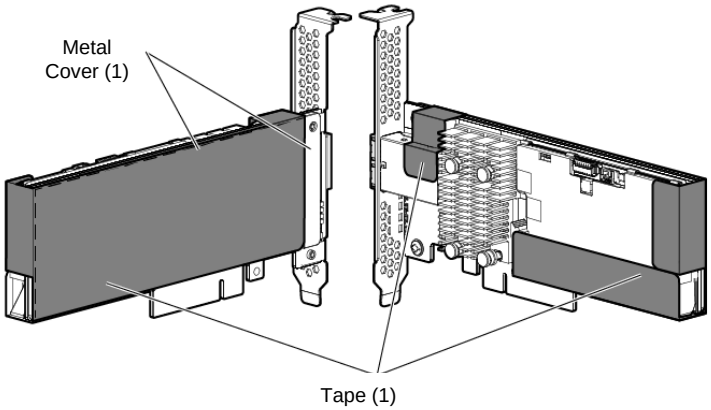

Figure 4 – P431 Controller

c. The P731m controller is a mezzanine card and is depicted in Figure 5 with the physical security kit installed. The P731m is shown with the required one (1) metal cover and one (1) section of tamper-evident tape.

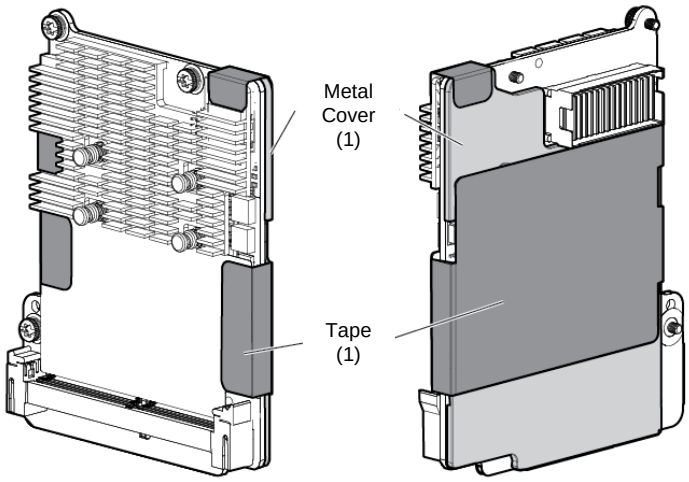

Figure 5 – P731m Controller

d. The P830 is a stand-up card and is shown in Figure 6 with the physical security kit installed. The P830 is shown with the required one (1) metal cover and three (3) sections of tamper-evident tape.

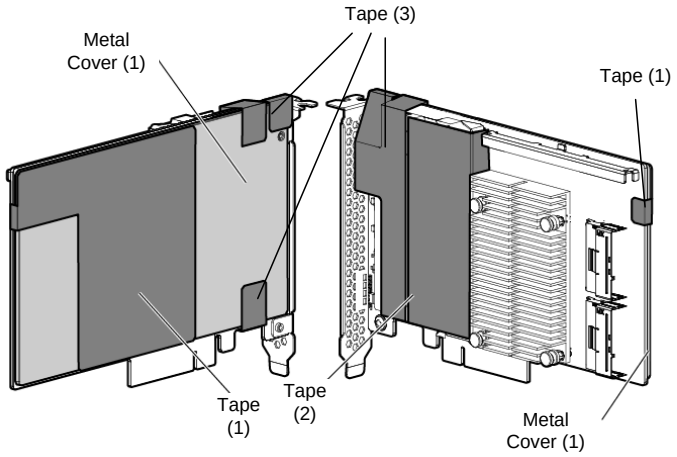

Figure 6 – P830 Controller

e. The P830i is a daughter card and is shown in Figure 7 with the physical security kit installed. The P830i is shown with the required one (1) metal cover and one (1) section of tamper-evident tape.

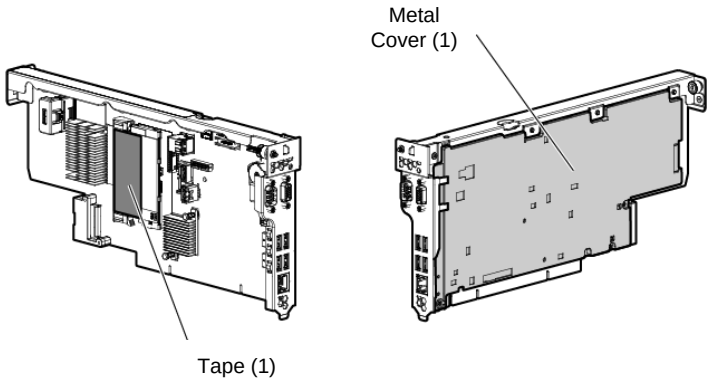

Figure 7 – P830i Controller

- Set the CO password, key management mode, encryption mode, and disallow plaintext volumes

1. Under **Tools**, click **Encryption Manager**.
2. Select "Perform Initial Setup". This will display the **Perform Initial Setup** screen
3. Under **Create Crypto Officer Password**, click **Show**.
4. Enter (then re-enter) the desired password in the **Create Crypto Officer Password** fields. CO password is required to be at least 10 characters.
5. Under **Encryption Mode**, select "Enable and Disallow Future Plaintext Volumes".
6. Under **Master Key**, enter the name of the Master Key in the field provided.
7. Under **Key Management Mode**, select the desired key management mode.
8. Click **OK**.

In Local mode, this password will be used to generate the Local Master Key.

- Enable volatile data encryption keys

1. Select the controller to be configured and click **Configure**.
2. Under **Controller Devices**, click **Arrays** and select a logical drive.
3. Under **Actions**, click **Encryption Volatile Key.**
4. A new window appears. Select "Enabled". To continue, click **OK**.
5. A warning window appears. To continue, click **Yes**.
6. A summary page appears, confirming that volatile keys are enabled. continue, click **Finish**.

A banner will appear over the HPE SSA main menu, indicating that volatile keys are enabled for the selected controller and will remain while volatile keys are enabled. The CO shall ensure that volatile data encryption keys are enabled on all logical drives.

- Enable the User role

1. Under **Tools**, click **Encryption Manager**.
2. Select "Set/Change User Password". This will display the **Set/Change User Password** screen.
3. Under **New Password**, click **Show**.
4. Enter (then re-enter) the desired password in the **New Password** fields. User password is required to be at least 10 characters.
5. Click **OK**.

- Verify and lock firmware

The modules require the proper firmware version be installed. To check if a module is currently running the correct version, the CO must go to the 'More info' page for the controller on the GUI.

If the version is not v1.66, the firmware must be updated to the v1.66 version. To perform a firmware update, the updated firmware must be imported and applied to the controller. The controller will verify the firmware signature and then perform the update.

Once the firmware version is set to v1.66, the CO must lock the firmware. The firmware can be locked using the GUI Secure Management page by clicking the 'Lock Firmware' link. Locking the firmware prevents any further updates to the firmware, and ensures that the module is operating with the validated firmware.

3.2 Secure Management

The Crypto Officer is responsible for ensuring that the modules are operating in their FIPS-Approved mode of operation.

3.2.1 Management

When configured according to the Crypto Officer guidance in this Security Policy, the modules only run in their Approved mode of operation. The Crypto Officer shall configure the modules via the SSA GUI, SSA CLI utilities, or SSA Scripting interface. The Crypto Officer shall monitor and manage the modules only through the SSA GUI. The CO password shall be at least 10 characters in length. The Crypto Officer shall not set the controller password or disable encryption. Plaintext volumes shall not be allowed and shall not be moved to the controller. The CO shall configure the modules to use local key management mode only.

Detailed instructions to monitor and troubleshoot the systems are provided in the *HPE Secure Encryption Installation and User Guide.*

3.2.2 Physical Inspection

For the modules to operate in their FIPS-Approved mode of operation, the factory-installed physical security kits must be in place as specified in Section 3.1. Upon receipt, the CO shall inspect the module to ensure the physical security kit has been properly installed.

Per FIPS 140-2 Implementation Guidance (IG 14.4), the CO is also responsible for direct control and observation of any changes to the modules where the tamper-evident seals are removed or installed to ensure that the security of the modules is maintained during such changes and that the modules are returned to their Approved state.

The CO is also required to periodically inspect the modules for evidence of tampering at intervals specified per end-user policy. The CO must visually inspect the tamper-evident seals for tears, rips, dissolved adhesive, and other signs of tampering. If evidence of tampering is found during periodic inspection, the Crypto Officer must zeroize the keys and contact HPE Customer Service via email at service@hp.com. The Crypto Officer must be sure to include contact information and the shipping address, as well as the controller serial number. HPE Customer Service will instruct the CO on how to return the module to HPE for installation of new tamper-evident labels.

3.2.3 Monitoring Status

The Crypto Officer should monitor the modules' status regularly for Approved mode of operation. When configured according to the Crypto Officer's guidance, the modules only operate in the Approved mode.

To monitor the controller's encryption status, each controller has an encryption LED that will be on to show that encryption is enabled and all attached logical drives are encrypted. In addition, the SSA GUI will indicate the controller's encryption status on the **Encryption Manager** page in the section marked "Settings". When properly configured, the controller's encryption status will be shown as 'Enabled'. All attached logical drives shall have a lock icon next to them, to indicate they are encrypted drives. Only encrypted drives shall be allowed.

3.2.4 Zeroization

In order to zeroize all keys and CSPs the modules must be returned to the factory mode. On the GUI, this is done using the 'Clear Encryption Configuration' button. No encrypted logical drives can be attached for either of these commands to succeed. These commands will zeroize all keys and CSPs. The modules will need to be re-initialized to return to operation.

3.3 User Guidance

The User can reset his or her password and shall be responsible for ensuring that the new password meets the criteria listed in Section 3.1. The User can also lock the firmware. A User can also perform zeroization as discussed in 3.2.4 and view the controller's encryption status using the methods discussed in 3.2.3. A User can move logical volumes to the controller. These volumes must be set to encrypt prior to moving to the controller.

3.4 Non-Approved Mode of Operation

When configured according to the Crypto Officer guidance in this Security Policy, the modules do not support a non-Approved mode of operation.

4 Acronyms

Table 8 provides definitions for the acronyms used in this document.

Table 8 – Acronyms

Acronym	Definition
AES	Advanced Encryption System
CLI	Command Line Interface
CMVP	Cryptographic Module Validation Program
CO	Crypto Officer
CSE	Communications Security Establishment
CSP	Critical Security Parameter
DEK	Data Encryption Key
DIMM	Dual in-line Memory
DRBG	Deterministic Random Bit Generator
ECB	Electronic Code Book
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
ESKM	Enterprise Secure Key Manager
FIPS	Federal Information Processing Standard
GUI	Graphical User Interface
HMAC	(keyed-) Hash Message Authentication Code
I/O	Input/Output
IG	Implementation Guidance
KAT	Known Answer Test
LED	Light Emitting Diode
Mbps	Megabits per Second
NDRNG	Non-Deterministic Random Number Generator
NIST	National Institute of Standards and Technology
NVRAM	Non-Volatile Random Access Memory
OS	Operating System
PBKDF2	Password Based Key Derivation Function
PCI	Peripheral Component Interconnect
PCIe	PCI Express
RAID	Redundant Array of Independent Disks

Acronym	Definition
RNG	Random Number Generator
ROC	RAID-on-Chip
RTOS	Real-Time Operating System
SAS	Serial Attached SCSI
SCSI	Small Computer System Interface
SHA	Secure Hash Algorithm
SP	Special Publication
SSA	Smart Storage Administrator
XEX	XOR-Encrypt-XOR
XOR	Exclusive Or
XTS	XEX-Based Tweaked-Codebook Mode with Ciphertext Stealing

Prepared by:
Corsec Security, Inc.

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

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