Hewlett-Packard Enterprise Development LP

HP P-Class Smart Array Gen9 RAID Controllers

Hardware Models: P244br, P246br, P440, P441, and P741m
Firmware Version: 2.52

FIPS 140-2 Non-Proprietary Security Policy

FIPS Security Level: 1
Document Version: 0.5

Prepared for:

Hewlett Packard Enterprise

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

Phone: +1 281 370 0670
www.hpe.com

Prepared by:

Corsec

Corsec Security, Inc.

13291 Park Center Road, Suite 460
Herndon, VA 20171
United States of America

Phone: +1 703 267 6050
www.corsec.com

Table of Contents

List of Tables

List of Figures

1. Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the HP P-Class Smart Array Gen9 RAID Controllers from Hewlett-Packard Enterprise Development LP (HPE). This Security Policy describes how the HP P-Class Smart Array Gen9 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 National Institute of Standards and Technology (NIST) and the 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 module in a secure FIPS-Approved mode of operation. This policy was prepared as part of the Level 1 FIPS 140-2 validation of the module. The HP P-Class Smart Array Gen9 RAID Controllers are referred to in this document as “Smart Array Controllers”, “controllers”, or “modules”.

1.2 References

This document deals only with operations and capabilities of the modules 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 (www.hpe.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 organized into two (2) primary sections. Section 2 provides an overview of the validated modules. This includes a general description of the capabilities and the use of cryptography, as well as a presentation of the validation level achieved in each applicable functional areas of the FIPS standard. It also provides high-level descriptions of how the modules meet FIPS requirements in each functional area. Section 3 documents the guidance needed for the secure use of the module, including initial setup instructions and management methods and policies.

2. Smart Array Controllers

2.1 Overview

The HP P-Class Smart Array RAID Controllers make up 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 HP server, and provide a high speed data path, on-board storage cache, remote management, and encryption of data at rest, for the controlled storage arrays. Additional drives can be easily added to increase throughput. The purpose of the controllers 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 controllers 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 slow down for random read requests.

The controllers are delivered in several form factors, including mezzanine cards, stand-up cards, and embedded on the main logic board in an HP Proliant Gen9 server platform (see Figure 1 through Figure 5). Each controller contains a PCIe[3] connector, multiple serial attached SCSI (SAS) ports, and a cryptographic state LED[4]. The HP server provides a Smart Storage Administrator GUI and CLI that are used to manage the controllers. For a list of servers compatible with the HP P-Class Smart Array RAID Controllers, refer to the *HP Smart Array Controllers Compatibility Matrix for HP Gen9 Servers* datasheet.

[1] SCSI – Small Computer System Interface
[2] RAID – Redundant Array of Independent Disks
[3] PCIe – Peripheral Component Interconnect Express
[4] LED – Light Emitting Diode

Figure 1 – P244br Controller

Figure 2 – P246br Controller

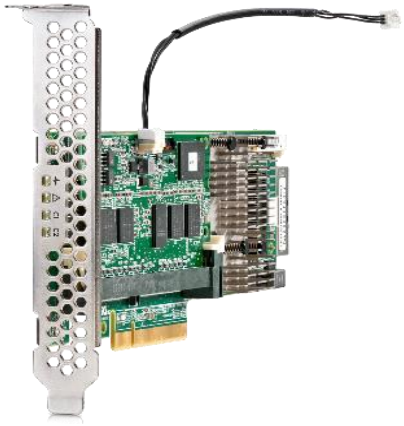

Figure 3 – P440 Controller

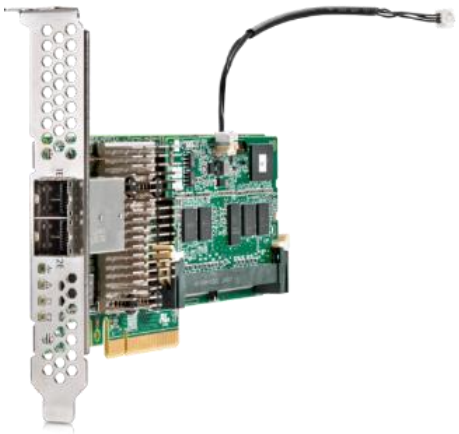

Figure 4 – P441 Controller

Figure 5 – P741m Controller

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 Smart Array Controllers are validated at the FIPS 140-2 section levels shown in Table 1.

[5] ASIC – Application-Specific Integrated Circuit

Table 1 – Security Level per FIPS 140-2 Section

Section	Section Title	Level
1	Cryptographic Module Specification	1
2	Cryptographic Module Ports and Interfaces	1
3	Roles, Services, and Authentication	2
4	Finite State Model	1
5	Physical Security	1
6	Operational Environment	N/A
7	Cryptographic Key Management	1
8	EMI/EMC[6]	1
9	Self-tests	1
10	Design Assurance	2
11	Mitigation of Other Attacks	N/A

2.2 Module Specification

Each controller is a hardware module with a multiple-chip embedded embodiment. The overall security level of the modules is 1. Each controller consists of a printed circuit board (PCB) with connectors, making up the modules' physical cryptographic boundary. Each module includes the Smart Array firmware v2.52 and Express Logic's ThreadX RTOS[7] v5.5.

The modules are primarily composed of the following components:

- PMC-Sierra 806x ROC processor
- Flash NVRAM[8]
- Dual in-line memory (DIMM) Module
- Bootstrap and Crypto NVRAM
- SAS Support Logic module
- PCIe Connector
- A multistate LED

A block diagram of the Smart Array Controllers, including major physical components and logical interfaces, is provided as Figure 6. Note that there are Manufacturing NVRAM, Local NVRAM, and SAS Mfg ID NVRAM components that do not process any cryptographic information.

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

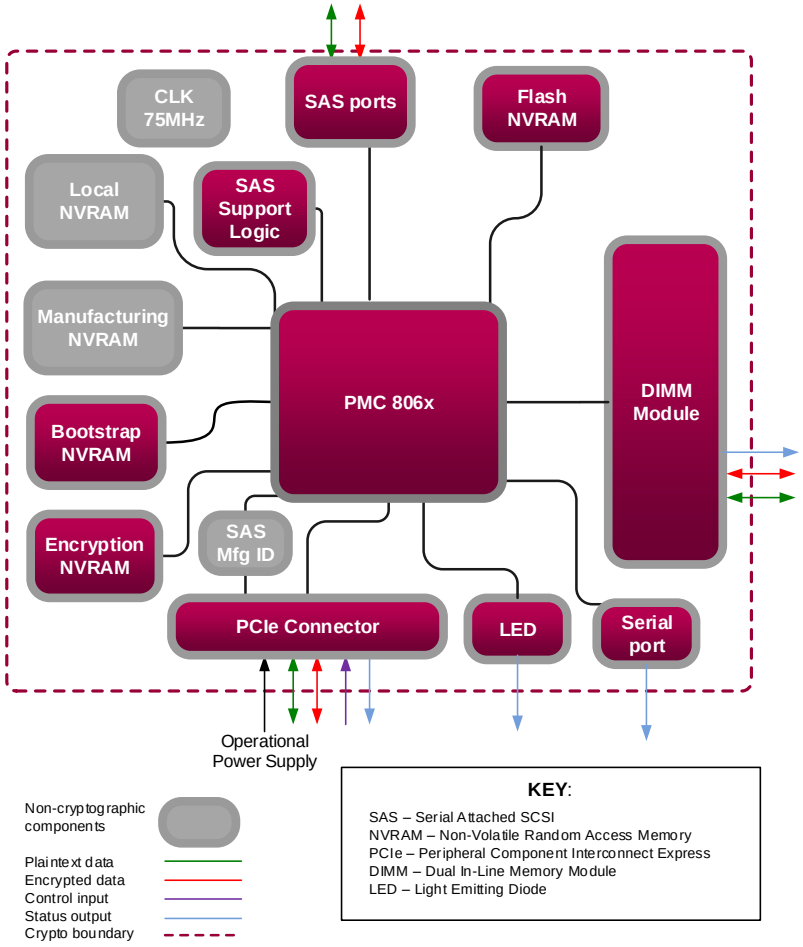

Figure 6 – Smart Array Controllers Block Diagram

These components appear in a variety of physical layouts depending on the module form factor. 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
P244br	embedded	PMC-Sierra 8062
P246br	embedded	PMC-Sierra 8062
P440	stand-up card	PMC-Sierra 8061
P441	stand-up card	PMC-Sierra 8061
P741m	mezzanine	PMC-Sierra 8061

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

Table 3 – FIPS-Approved Algorithm Implementations

Algorithm	Certificate Number	
	PM8061	PM8062
AES[9] ECB[10], encryption/decryption with 256-bit keys	#2902	#2903
XTS[11,12,13]-AES encryption/decryption with XTS_256-bit keys	#2902	#2903
SHA[14]-256	#2442	#2443
HMAC[15] with SHA-256	#1837	#1838
SP[16] 800-90A CTR DRBG[17]	#529	#530

NOTE: AES XTS is only Approved for storage applications.

The controllers include the FIPS-Approved Password-Based Key Derivation Function (PBKDF2) specified in SP 800-132 option 2 as a key establishment technique. Passwords for authorized operators shall be at least 8 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 controllers also employ the following non-Approved algorithms that are allowed in a FIPS mode of operation:

- A non-deterministic random number generator (NDRNG), in the form of a free running oscillator, is used to generate entropy for the CTR DRBG.
- 256-bit AES in ECB mode is used for key wrapping (wrap and unwrap). This functionality is not compliant with SP 800-38F “Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping”.

2.3 Module Interfaces

The modules’ 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

The modules have the following physical interfaces (which map to the FIPS-required logical interfaces as shown in Figure 6):

[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

- PCIe connector
- SAS ports
  - P244br – 2 x 1 port
  - P246br – 4 x 1 port
  - P440 – 1 x 8 port
  - P441 – 2 x4 ports
  - P741m – 4 x2 ports
- DIMM bus (in remote mode only)
- Multistate LED
- Serial port
- Power

Table 4 – FIPS 140-2 Logical Interface Mappings

Physical Port/Interface	Quantity	FIPS 140-2 Interface
PCIe Connector	1	Data Input Data Output Control Input Status Output Power Input
SAS port(s)	variable	Data Input Data Output
DIMM bus (remote mode only)	1	Data Input Data Output Status Output
Multistate LED	1	Status Output
Serial port	1	Status Output

2.4 Roles, Services, and Authentication

There are two roles 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 module does not support multiple concurrent operators. 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. Access to these services requires the operator to assume one of the supported authorized roles.

Table 5 – Operator Services

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 IKEK[19]	x		Set or reset IKEK	Command and password	Command response and status output	IKEK – W 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[20] – R, X KEK[21] – R, X CO password – X
Set key cache policies	x		Establish policies for where cache storage exists and what keys are stored there	Command	Command response and status output	KEK – R CO password – X
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 'Local Key Management Mode' or 'Remote 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 or KEK	Command and parameters	Command response	DEK – R, W KEK – R, W CO password – X
Set 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

[18] Note that the "Show status" and "Perform self-tests" 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] IKEK – an initial key encryption key that is referred to as the Master Key in HP documentation
[20] DEK – Data Encryption Key
[21] KEK – Key Encryption Key (also referred to as the Drive Encryption Key in HP documentation)

Service[18]	Operator		Description	Input	Output	CSP and Type of Access
	CO	User				
Clear Encryption	x	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

The module also offers services that do not require the assumption of an authorized role. These services are listed and described in Table 6. Note that these services do not affect the security of the module, nor do they modify, disclose, or substitute any keys or CSPs.

Table 6 – Unallocated Services

Service	Description	Input	Output
Perform data transformations	Modify the distribution or contents of one or more logical drives, including: • adding/removing a physical drive • deleting a logical drive • adding an encrypted logical drive • moving a logical drive from one array to another • changing a logical drive's RAID level or stripe size • optimizing alignment for logical drives • encrypting data destined for an encrypted logical drive	Command	Command response and status output
Show Master Key reset date	Provide the date of when the Master key was last reset.	Command	Status output
Show Drive or Volume Key "last rekey" date	Provide the date when the Drive or Volume Key was last rekeyed	Command	Status output
Check encryption status	Indicate the module's encryption status	Command	Status output
Reboot the controller	Reboot the controller	Reboot controller	Status output

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. Table 7 lists the strength of the authentication mechanism used by the modules.

Table 7 – Authentication Mechanism

Authentication Type	Strength
CO/User Password	The minimum length of the password is 8 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 4 characters could be any of the 94 choices. The chance of a random attempt falsely succeeding is = 1 : (10*26*26*32*94^4), or 1 : 16,889,161,502,720 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 : (16,889,161,502,720 possible passwords / 10 passwords per minute) = 1 : 16.8891 x 10^{11} which is less than 1:100,000 as required by FIPS 140-2.

2.5 Physical Security

The Smart Array Controllers are multiple-chip embedded cryptographic modules. Each module consists of production-grade components that include standard passivation techniques.

2.6 Operational Environment

The modules employ a non-modifiable operating environment. The modules' firmware (Firmware version: 2.52) is executed by the module's PMC processor. The modules do not provide a general purpose operating system to module operators.

2.7 Cryptographic Key Management

The modules can operate in either of two different modes: local or remote. In local mode, the modules generate and store all keys. In remote mode, an external Enterprise Secure Key Manager (ESKM) is used to generate an IKEK and to store KEKs and Controller Keys.

Controller Keys, KEKs, and DEKs are generated internally, but can all be stored outside of the module. For protection during export, the module wraps these keys using AES key wrap (in remote mode, AES key wrap is also used to unwrap the KEK upon being re-input into the module). The Controller Key and KEK are wrapped

with the IKEK prior to output for storage on the external ESKM, while the DEK is wrapped with the KEK prior to output for storage on an attached disk.

Table 8 below describes the keys and CSPs supported by the module as they apply to these modes.

Table 8 – List of Cryptographic Keys, Cryptographic Key Components, and CSPs

CSP	CSP Type	Generation / Input	Output	Storage	Zeroization	Use
Local and Remote Mode						
DEK	256-bit AES-XTS key	Generated internally	Exits the module in encrypted form for storage	Stored in plaintext in volatile DIMM module	Reboot Delete logical drive	Encryption and decryption of logical drives
Crypto Officer Password	8 – 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	Authenticate Crypto Officer
User Password	8 – 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	Authenticate User
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
Remote Mode Only						
KEK	256-bit AES-XTS key	Generated internally and may be re-input electronically in encrypted form	May exit the module in encrypted form for storage	Stored in volatile DIMM module in plaintext Stored in encrypted form in NVRAM by caching policy	Return to factory reset Reboot	Encryption and decryption of DEKs in remote mode only. There is one KEK per physical drive

CSP	CSP Type	Generation / Input	Output	Storage	Zeroization	Use
IKEK	256-bit AES-ECB key	Imported over shared memory interface	Never exits the module	Stored in plaintext in NVRAM	Return to factory reset	Initial key used for encryption and decryption of KEKs and User and CO passwords
Controller Key	256-bit AES-ECB key	Generated internally	Exits the module in encrypted form for storage	Stored in volatile DIMM module in plaintext form	Return to factory reset Reboot	Performs encryption and decryption per controller at initialization of the controller
Local Mode Only						
Local Master Key	256-bit AES key	Derived as per SP 800-132 using PBKDF2 and HMAC-SHA-256	Never exits the module	Stored in plaintext in NVRAM	Return to factory reset.	Encryption and decryption of DEKs

2.8 EMI / EMC

The Smart Array Controllers were tested and found conformant to the EMI/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 each module when first powered up as well as when a random number is generated. The following sections list the self-tests performed by the modules, their expected error status, and error resolutions.

2.9.1 Power-Up Self-Tests

The HP 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 HP 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, the modules enter 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 DRBG Instantiate, Generate, and Reseed Tests, which are described in SP 800-90A, are performed by the modules at start-up or anytime the DRBG is instantiated. These tests are critical function self-tests.

A failure of any of these tests results in a critical error for the DRBG, requiring that the modules 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 1 requirements for this validation.

3. Secure Operation

The Smart Array Controllers meet Level 1 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 P244br and P246br controllers are pre-installed in the target server. The P440, P441, and P741m controllers must be installed in a supported server. The *HP Smart Array Controllers User Guide for HP ProLiant Gen9 Servers* include the steps 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. The modules can be configured through the underlying server's Smart Storage Administrator (SSA), Secure Encryption Graphical User Interface (GUI), HP SSA Scripting interface, or through the SSA Command Line Interface (CLI) utility. Once initialized, only the Secure Encryption GUI can be used to manage the module. The commands and buttons used in these interfaces 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. Set the CO password, key management mode, encryption mode, and disallow plaintext volumes[22]
2. Enable the User role
3. Verify and lock the firmware

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

3.1.1 Initial Setup using the Server GUI

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

- 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. The CO password is required to be at least 8 characters.
    5. Under **Encryption Mode**, select "Enable and Disallow Future Plaintext Volumes".

[22] Operators have the ability to move plaintext volumes via the unallocated service "Perform data transformations". Once the modules are configured for FIPS operation, plaintext volumes shall not be allowed and shall not be moved to the controller.

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 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. The User password is required to be at least 8 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 2.52, the firmware must be updated to the 2.52 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 2.52, 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.

3.1.2 Initial Setup using the SSA Scripting Interface

To initialize each module using the SSA Scripting interface, follow the steps in the *HP Smart Storage Administrator User Guide,* section "Accessing HP SSA in the online environment" to download and launch the application. Then follow the steps below to complete the initial setup.

- This is a scripting interface, so all configurations can be set with one script. This requires that the module firmware be verified prior to running the script. To check if a module is currently running the correct version, the CO must verify the firmware through the SSA CLI or SSA GUI. This Set the CO password, key management mode, encryption mode, disallow plaintext volumes, set User password, and lock the firmware using the following script:

```
Action= Configure
Method= Custom
Controller= [SLOT n]
AcceptEULA=yes
EncryptionCryptoPasswordSet= [CO Password]
EncryptionMasterKey= [IKEK name]
EncryptionKeyManager= [Local| Remote]
AllowPlainText= False
```

```
Encryption= Enable
EncryptionUserPasswordSet= [User Password]
Firmwarelock= On
```

Where:

1. `Controller= [SLOT n]` where 'n' identifies the slot of the controller that the script is configuring.
2. `EncryptionCryptoPasswordSet` sets the CO's password. The CO password must be at least 8 characters long.
3. `EncryptionKeyManager` sets the encryption mode to either 'Local' or 'Remote'.
4. `AllowPlainText` is set to 'False' so that all new volumes created will be encrypted.
5. `Encryption` is set to 'Enable'. This initiates self-tests and the module is capable of encrypted data.
6. `EncryptionUserPasswordSet` sets the User password. The User password must be at least 8 characters long.
7. `Firmwarelock is set to 'On'`. Locking the firmware prevents any further updates to the firmware, and ensures that the module is operating with the validated firmware.

3.1.3 Initial Setup using the SSA CLI

To initialize the module using the SSA CLI, follow the steps in the *HP Smart Storage Administrator User Guide,* section "Accessing HP SSA in the online environment" to download and launch the application. Then open the HP Smart Storage Administrator CLI. Then follow the steps below to complete the initial setup.

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

  To set these configuration items, use the following command sequence:

  ```
  Controller slot=[PCI slot number] enableencryption [eula=yes]
  encryption=on localkeymanagermode=[on|off] mixedvolumes=off
  [password=PASSWORD STRING] masterkey=MASTERKEY
  ```

  where:

  1. `encryption=on` enables the encryption mode for the module
  2. `localkeymanagermode` sets the local mode when 'on' and the remote mode when 'off'
  3. `mixedvolumes=off` allows only encrypted logical disk creation.
  4. `password` allows the operator to input the CO password. The CO password must be at least 8 characters long.

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

- Enable the User role

  To enable the User role, use the following command sequence:

  ```
  Controller slot=[PCI slot number]setpasswd suser=user
  spassword=PASSWORD STRING
  ```

The User password is required to be at least 8 characters long.

- 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 enter

  ```
  ctrl slot=N show detail
  ```

  through the SSA CLI (where `N` is the slot that contains the controller). The output displayed on the screen will include the firmware version installed on the specified controller.

  If the version is not 2.52, the firmware must be updated to the 2.52 version. To perform a firmware update, use the appropriate Smart Components to import the updated firmware and apply it to the controller. The controller will verify the firmware signature and then perform the update.

  Once the firmware version is set to 2.52, the CO must lock the firmware. The firmware can be locked using the command

  ```
  ctrl slot=N modify fwlock=on
  ```

  where N is again the slot of the controller whose firmware is being locked. 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 as prescribed in this Security Policy. The Crypto Officer shall monitor and manage the modules only through the SSA GUI. The CO password shall be at least eight characters in length. The Crypto Officer shall not set the controller password or disable encryption.

3.2.2 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 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 a 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.

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

3.2.3 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. A User can also perform zeroization as discussed in 3.2.3 and view the controller's encryption status using the methods discussed in 3.2.2.

3.4 Non-FIPS-Approved Mode

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 9 provides definitions for the acronyms used in this document.

Table 9 – 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
IKEK	Initial KEK Encryption Key or Master Key
KAT	Known Answer Test
KEK	Key Encryption Key or Drive Encryption Key
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

Acronym	Definition
PCIe	PCI Express
RAID	Redundant Array of Independent Disks
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.

13921 Park Center Road, Suite 460
Herndon, VA 20171
United States of America

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