

Hewlett Packard Enterprise Development LP

HPE Smart Array Gen10 P-Class RAID Controllers

Hardware Models: P408i-p SR Gen10, P408e-p SR Gen10, P408i-a SR Gen10, P816i-a SR Gen10, P204i-b SR Gen10, P408e-m SR Gen10, P204i-c SR Gen10, and P416ie-m SR Gen10

Firmware Version: 1.34

FIPS 140-2 Non-Proprietary Security Policy

FIPS Security Level: 1

Document Version: 0.6

Prepared for:



**Hewlett Packard
Enterprise**

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

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

Prepared by:



Corsec Security, Inc.

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

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

Table of Contents

- 1. Introduction4**
 - 1.1 Purpose4
 - 1.2 References.....4
 - 1.3 Document Organization4
- 2. Smart Array Gen10 RAID Controllers5**
 - 2.1 Overview5
 - 2.2 Module Specification.....9
 - 2.3 Module Interfaces 12
 - 2.4 Roles, Services, and Authentication..... 13
 - 2.5 Physical Security 16
 - 2.6 Operational Environment..... 16
 - 2.7 Cryptographic Key Management 16
 - 2.8 EMI / EMC..... 20
 - 2.9 Self-Tests 20
 - 2.9.1 Power-Up Self-Tests 20
 - 2.9.2 Conditional Self-Tests..... 20
 - 2.9.3 Critical Functions Self-Tests 20
 - 2.10 Mitigation of Other Attacks..... 21
- 3. Secure Operation22**
 - 3.1 Installation and Setup 22
 - 3.1.1 Initial Setup 22
 - 3.2 Crypto Officer Guidance..... 24
 - 3.2.1 Management 24
 - 3.2.2 Monitoring Status..... 24
 - 3.2.3 Zeroization..... 24
 - 3.3 User Guidance 25
 - 3.4 Additional Usage Policies 25
 - 3.5 Non-FIPS-Approved Mode 25
- 4. Acronyms26**

List of Tables

- Table 1 – Security Level per FIPS 140-2 Section8
- Table 2 – Controller Form Factor/Processor Configurations..... 10
- Table 3 – FIPS-Approved Algorithm Implementations 11
- Table 4 – FIPS 140-2 Logical Interface Mappings 12
- Table 5 – Mapping of Operator Services to Inputs, Outputs, CSPs, and Type of Access 14
- Table 6 – Unallocated Services 15
- Table 7 – Authentication Mechanism 16

Table 8 – List of Cryptographic Keys, Cryptographic Key Components, and CSPs 18
 Table 9 – Acronyms 26

List of Figures

Figure 1 – P408i-p SR Gen10 Controller5
 Figure 2 – P408e-p SR Gen10 Controller6
 Figure 3 – P408i-a SR Gen10 Controller6
 Figure 4 – P816i-a SR Gen10 Controller6
 Figure 5 – P204i-b SR Gen10 Controller7
 Figure 6 – P408e-m SR Gen10 Controller7
 Figure 7 – P204i-c SR Gen10 Controller.....7
 Figure 8 – P416ie-m SR Gen10 Controller8
 Figure 9 – Smart Array Gen10 RAID Controllers Block Diagram 10

1. Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the HPE Smart Array Gen10 P-Class RAID Controllers (Hardware Models: P408i-p SR Gen10, P408e-p SR Gen10, P408i-a SR Gen10, P816i-a SR Gen10, P204i-b SR Gen10, P408e-m SR Gen10, P204i-c SR Gen10, and P416ie-m SR Gen10; Firmware Version: 1.34) by Hewlett Packard Enterprise Development LP. This Security Policy describes how the HPE Smart Array Gen10 P-Class 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 HPE Smart Array Gen10 P-Class RAID Controllers are referred to in this document as “Smart Array Gen10 RAID 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.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 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 Gen10 RAID Controllers

2.1 Overview

The Smart Array Gen10 RAID Controllers make up a family of serial-attached SCSI¹ host bus adapters that provide intelligent control for storage arrays. These 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, for the controlled storage arrays. Additional drives can be easily added to increase throughput. The purpose of the Smart Array Gen10 RAID Controllers is to transform an application's high-level 'read' or 'write' disk operations into the individual instructions required for a RAID² array using an embedded RAID-on-Chip (ROC) processor. Disk operations are protected in transit via the Smart Array Gen10 RAID 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 Smart Array Gen10 RAID 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. The 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.

The Smart Array Gen10 RAID Controllers can be delivered in a variety of form factors for use with the HPE ProLiant Gen10 server platform (see Figure 1 through Figure 8 below). Each controller contains a PCIe³ connector, multiple serial attached SCSI (SAS) ports, and a cryptographic state LED⁴. HPE ProLiant servers provides a Smart Storage Administrator GUI and CLI that are used to manage the Smart Array Gen10 RAID Controllers. For a list of servers compatible with the HPE Smart Array Gen10 P-Class RAID Controllers, refer to the [HPE Smart Array Controllers – Supported Gen10 Servers](#) webpage.



Figure 1 – P408i-p SR Gen10 Controller

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 2 – P408e-p SR Gen10 Controller



Figure 3 – P408i-a SR Gen10 Controller



Figure 4 – P816i-a SR Gen10 Controller



Figure 5 – P204i-b SR Gen10 Controller



Figure 6 – P408e-m SR Gen10 Controller



Figure 7 – P204i-c SR Gen10 Controller



Figure 8 – P416ie-m SR Gen10 Controller

The Smart Array Gen10 RAID Controllers provide encryption for data at rest. Each controller includes an ASIC⁵ from Microsemi Corporation 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. Disk encryption keys are encrypted with a second key encryption 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 Gen10 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	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

⁵ ASIC – Application-Specific Integrated Circuit

⁶ EMI/EMC – Electromagnetic Interference / Electromagnetic Compatibility

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 (version 1.34) and Express Logic's ThreadX RTOS⁷ v6.2.

The modules are primarily composed of the following components:

- Microsemi PM82xx ROC processor
- 16MB⁸ NAND Flash memory
- 256Kb⁹ Encryption NVRAM¹⁰
- Double data rate (DDR) memory
- 12G SAS ports
- SAS Support Logic module
- PCIe connector
- Serial port
- A multistate LED

A block diagram of the Smart Array Gen10 RAID Controllers, including major physical components and logical interfaces, is provided as Figure 9. Note that there are Bootstrap NVRAM and SAS Mfg ID NVRAM components that do not process any cryptographic information.

⁷ RTOS – Real-Time Operating System

⁸ MB – Megabytes

⁹ Kb – Kilobits

¹⁰ NVRAM – Non-Volatile Random Access Memory

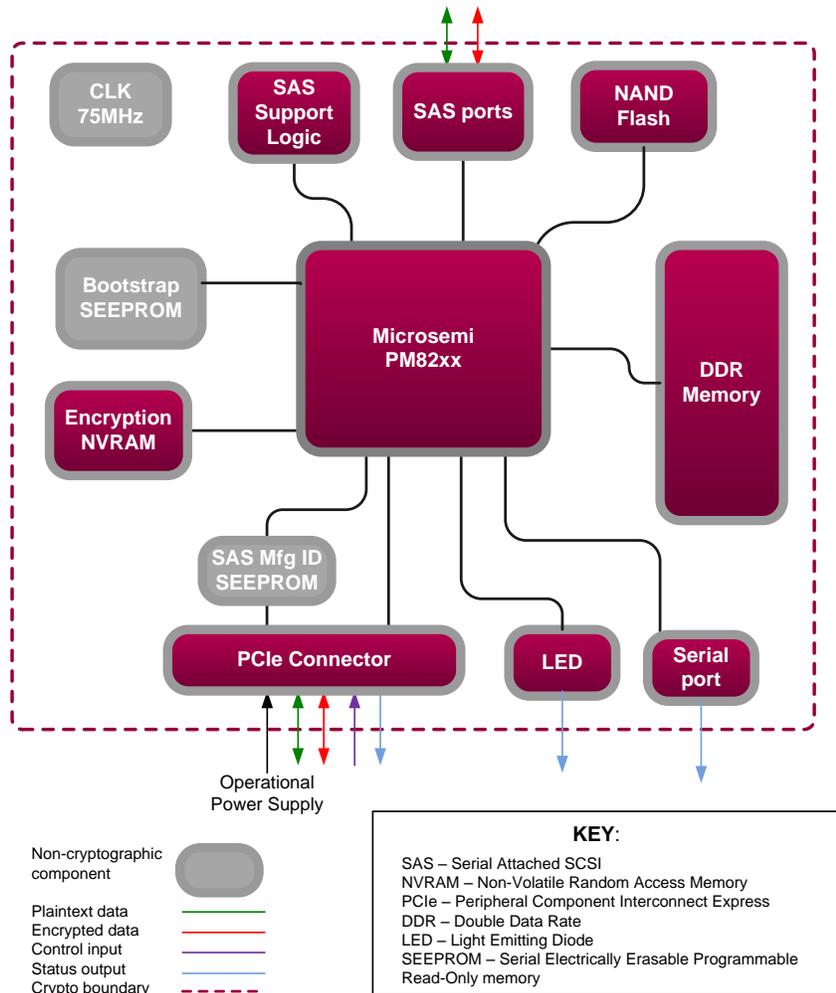


Figure 9 – Smart Array Gen10 RAID Controllers Block Diagram

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
P408i-p SR Gen10	Standard PCIe plugin controller	PM8205
P408e-p SR Gen10	Standard PCIe plugin controller	PM8205
P408i-a SR Gen10	Modular controller	PM8205
P816i-a SR Gen10	Modular controller	PM8237
P204i-b SR Gen10	Modular controller	PM8221

HPE Smart Array Gen10 P-Class RAID Controllers

©2019 Hewlett Packard Enterprise Development LP

This document may be freely reproduced and distributed whole and intact including this copyright notice.

Controller Model	Form Factor	Embedded ROC
P408e-m SR Gen10	Mezzanine controller	PM8205
P204i-c SR Gen10	Modular controller	PM8221
P416ie-m SR Gen10	Mezzanine controller	PM8237

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

Table 3 – FIPS-Approved Algorithm Implementations

CAVP Certificate			Algorithm	Standard	Mode/Method	Key Lengths, Curves or Moduli	Use
PM8205	PM8221	PM8237					
#5232	#5234	#5233	AES	FIPS PUB 197	ECB ¹¹	256	data encryption/decryption
				FIPS PUB 197 NIST SP ¹² 800-38E	XTS ^{13,14,15}	256	data encryption/decryption
Vendor Affirmed	Vendor Affirmed	Vendor Affirmed	CKG ¹⁶	NIST SP 800-133	-	-	cryptographic key generation
#1998	#2000	#1999	DRBG	NIST SP 800-90Arev1	CTR_based	-	deterministic random bit generation
#3464	#3466	#3465	HMAC ¹⁷	FIPS PUB 198-1	SHA-256	-	message authentication
Vendor Affirmed	Vendor Affirmed	Vendor Affirmed	PBKDF2 ¹⁸	NIST SP 800-132	Option 2	-	password-based key derivation
#4212	#4214	#4213	SHS ¹⁹	FIPS PUB 180-4	SHA-256	-	message digest

Note: AES XTS is only approved for storage applications.

The vendor affirms the following cryptographic security methods:

- As per *NIST SP 800-132*, the modules use PBKDF2 option 2 to derive the Local Master Key. This function takes an input salt that is 128 bits in length with a password containing at least eight characters and produces a random value of 256 bits. In addition, the function has an iteration count of 10,000. The underlying pseudorandom function used in this derivation is HMAC SHA-256.

¹¹ ECB – Electronic Codebook

¹² SP – Special Publication

¹³ XTS – XEX-Based Tweaked-Codebook Mode with Ciphertext Stealing

¹⁴ XEX – XOR-Encrypt-XOR

¹⁵ XOR – Exclusive Or

¹⁶ CKG – Cryptographic Key Generation

¹⁷ HMAC – Hash Message Authentication Code

¹⁸ PBKDF2 – Password-Based Key Derivation Function 2

¹⁹ SHS – Secure Hash Standard

- As per *NIST SP 800-133*, the modules use the FIPS-Approved counter-based DRBG specified in *NIST SP 800-90A Revision 1* to generate cryptographic keys. The resulting symmetric key or generated seed is an unmodified output from the DRBG.

The controllers also employ the following non-Approved algorithm:

- Non-Deterministic Random Number Generator (NDRNG), which uses eight free-running oscillators to generate entropy for the counter-based DRBG.

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

Table 4 lists the modules’ physical interfaces and maps them to the FIPS-required logical interfaces.

Table 4 – FIPS 140-2 Logical Interface Mappings

Device	Physical Port/Interface	Quantity	FIPS 140-2 Logical Interface
P408i-p SR Gen10	PCIe Connector	1	Data Input, Data Output, Control Input, Status Output
	SAS port(s)	2 x 4 internal	Data Input, Data Output
	Multistate LED	1	Status Output
	Serial port	1	Status Output
P408e-p SR Gen10	PCIe Connector	1	Data Input, Data Output, Control Input, Status Output
	SAS port(s)	2 x 4 external	Data Input, Data Output
	Multistate LED	1	Status Output
	Serial port	1	Status Output
P408i-a SR Gen10	PCIe Connector	1	Data Input, Data Output, Control Input, Status Output
	SAS port(s)	2 x 4 internal	Data Input, Data Output
	Multistate LED	1	Status Output
	Serial port	1	Status Output
P816i-a SR Gen10	PCIe Connector	1	Data Input, Data Output, Control Input, Status Output
	SAS port(s)	4 x 4 internal	Data Input, Data Output
	Multistate LED	1	Status Output
	Serial port	1	Status Output
P204i-b SR Gen10	PCIe Connector	1	Data Input, Data Output, Control Input, Status Output
	SAS port(s)	1 x 4 internal	Data Input, Data Output
	Multistate LED	1	Status Output
	Serial port	1	Status Output

Device	Physical Port/Interface	Quantity	FIPS 140-2 Logical Interface
P408e-m SR Gen10	PCIe Connector	1	Data Input, Data Output, Control Input, Status Output
	SAS port(s)	2 x 4 external	Data Input, Data Output
	Multistate LED	1	Status Output
	Serial port	1	Status Output
P204i-c SR Gen10	PCIe Connector	1	Data Input, Data Output, Control Input, Status Output
	SAS port(s)	1 x 4 internal	Data Input, Data Output
	Multistate LED	1	Status Output
	Serial port	1	Status Output
P416ie-m SR Gen10	PCIe Connector	1	Data Input, Data Output, Control Input, Status Output
	SAS port(s)	2 x 4 internal 2 x 4 external	Data Input, Data Output
	Multistate LED	1	Status Output
	Serial port	1	Status Output

2.4 Roles, Services, and Authentication

The following sections detail the roles, services, and authentication mechanisms provided by the module.

2.4.1 Roles

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.

2.4.2 Services

Descriptions of the services available to module operators are detailed in Table 5 below. 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.

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

Service ²⁰	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 – W, 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 Local Master Key Name – R, X 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 ²¹ – R, X 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
Set 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 volume key	x		Rekey DEK	Command and parameters	Command response	CTR_DRBG Seed – R, W, X CTR_DRBG Entropy Input – R, W, X CTR_DRBG ‘V’ Value – R, W, X CTR_DRBG ‘Key’ Value – R, W, X DEK – 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 – W User Password – W
Disallow plaintext logical drive creation	x		Inhibit the creation of plaintext logical drives	Command	Command response and status output	CO Password – X
Set volatile encryption key storage mode	x		Set the encryption key for the specified logical drive to be volatile or stored on disk	Command	Command response and status output	None

²⁰ While the “Perform data transformations”, “Show status” and “Perform self-test” services are allocated to the Crypto Officer and User roles, 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).

²¹ DEK – Data Encryption Key (also referred to as the “Volume Encryption Key” in HPE documentation)

Service ²⁰	Operator		Description	Input	Output	CSP and Type of Access
	CO	User				
Perform data transformations	x	x	Modify the distribution or contents of one or more logical drives, including: <ul style="list-style-type: none"> • adding/removing physical drives • deleting logical drives • adding encrypted logical drives • moving logical drives 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	DEK – R, X
Reset CO password	x		Allow CO to reset password by answering a preset security question	Command	Command response and status output	CO pPssword – R, W
Clear encryption	x	x	Zeroize all CSPs	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 modules also offer 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 modules, nor do they modify, disclose, or substitute any keys or CSPs.

Table 6 – Unallocated Services

Service	Description	Input	Output
Check encryption status	Indicate the module’s encryption status	Command	Status output
Reboot the controller	Reboot the controller	Reboot controller	Status output

2.4.3 Authentication Mechanisms

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

Table 7 – Authentication Mechanism

Authentication Type	Strength
Username/Password	<p>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.</p> <p>The chance of a random attempt falsely succeeding is = 1 : (10*26*26*32*94⁴), or 1 : 16,889,161,502,720; which is less than 1:1,000,000 as required by FIPS 140-2.</p> <p>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 10¹¹ which is less than 1:100,000 as required by FIPS 140-2.</p>

2.5 Physical Security

The Smart Array Gen10 RAID 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: 1.34) is executed by the module’s Microsemi processor. The modules do not provide a general-purpose operating system to module operators.

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 3.1 below for the required configuration steps.

The module's entropy source has a min-entropy of 5.77881 per 8 bits. Thus, when providing 384 bits of seed material to the DRBG, the entropy source generates 277 bits of entropy for key generation.

Table 8 below describes the keys and CSPs supported by the modules.

Table 8 – 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 DDR module	Reboot Logical drive deleted	Used for encryption and decryption of logical drives
HMAC Key	128-bit HMAC key	Generated internally	Never exits the module	Plaintext in volatile memory	Reboot Logical drive deleted	Used with the PRF for the PBKDF function
Crypto Officer Password	8 – 16 character password	Entered electronically	Never exits the module	Stored in encrypted form in NVRAM Stored in plaintext in volatile DDRIMM module	Return to factory reset Reboot	Used for authenticating Crypto Officer role operators
User Password	8 – 16 character password	Entered electronically	Never exits the module	Stored in encrypted form in NVRAM Stored in plaintext in volatile DDR 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 DDR 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 DDR module in plaintext	Automatically upon completion of CTR_DRBG seed operation	Used in the process of generating a random number
CTR_DRBG 'V' Value	Internal state value	Internally generated	Never	Plaintext in volatile memory	Return to factory reset Reboot	Used in the process of generating a random number
CTR_DRBG 'Key' Value	Internal state value (256-bit AES-ECB key)	Internally generated	Never	Plaintext in volatile memory	Return to factory reset Reboot	Used in the process of generating a random number

CSP	CSP Type	Generation / Input	Output	Storage	Zeroization	Use
Local Master Key*	256-bit AES-XTS 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 DEKs
Local Master Key Name	10 – 64 character string	Generated externally and entered electronically	Never exits the module	Stored in plaintext in NVRAM	Return to factory reset	Used as input to PBKDF for generating the Local Master Key

**Keys derived from the PBKDF2 function shall only be used for storage applications.*

2.8 EMI / EMC

The Smart Array Gen10 RAID 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 modules 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 modules perform the following conditional self-tests:

- Continuous RNG Test for NDRNG
- Continuous RNG Test 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 Revision 1, are performed by the modules at start-up and at any time the DRBG is instantiated. A failure of any of these tests will result in a critical error for the DRBG, requiring that the affected module be replaced. When the DRBG is in error, no new keys can be generated.

The modules also conditionally perform a duplicate key test to ensure that its parsed AES-XTS keys are distinct. Failure of this test will result in a transition to a transitory, recoverable error state. In this state, no cryptographic processing can take place and data output is prohibited. Clearing this error state consists of the controllers generating a new XTS key for comparison. When the new key is generated, the modules will re-run the duplicate key test using the new key until successful.

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 Gen10 RAID 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 Installation and Setup

The Smart Array Gen10 RAID Controllers can be ordered pre-installed in a target server or as standalone units for customer installation. The [HPE Smart Array Controllers for HPE ProLiant Servers User Guide](#) include the steps to install P-Class controllers in a supported server.

In all cases, the modules are delivered in a non-operational factory state (security during delivery is guaranteed by trusted carriers such as FedEx, DHL, and UPS). 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 initialize the modules for their Approved mode of operation, the CO must:

1. Set the CO password, key management mode, encryption mode, and disallow plaintext volumes²²
2. Enable volatile data encryption keys
3. Enable the User role
4. Verify and lock the firmware

Additional guidance for performing these tasks (including the plaintext-to-encrypted volume conversion) using the SSA GUI can be found in the [HPE Smart Array SR Secure Encryption Installation and User Guide](#).

3.1.1 Initial Setup

To initialize each module, start the HPE 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, and encryption mode, and disallow plaintext volumes
 1. Select the controller to be configured and click **Configure**.
 2. Under **Tools**, click **Encryption Manager**.
 3. Select "Perform Initial Setup". This will display the **Perform Initial Setup** screen.

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.

4. Under **Create Crypto Officer Password**, click **Show**.
5. Enter (then re-enter) the desired password in the **New Password** fields. The CO password is required to be at least 8 characters.
6. Under **Encryption Mode**, select "Enable and Disallow Future Plaintext Volumes".
7. Under **Master Key**, enter the Master Key name in the field provided.
8. Under **Key Management Mode**, select "Local Key Management Mode".
9. Click **OK**.

When configured for local key management mode, the 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. Select the controller to be configured and click **Configure**.
2. Under **Tools**, click **Encryption Manager**.
3. Select "Set/Change User Password". This will display the **Set/Change User Password** screen.
4. Under **New Password**, click **Show**.
5. Enter (then re-enter) the desired password in the **New Password** fields. User password is required to be at least 8 characters.
6. 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 GUI's **More Info** page.

If the version is not 1.34, the firmware must be updated to the 1.34 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 1.34, 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.

When all of the above steps are successfully completed, the modules will be configured in their Approved mode of operation.

3.2 Crypto Officer Guidance

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. Detailed instructions to manage and troubleshoot the modules are provided in the [HPE Smart Array SR Secure Encryption Installation and User Guide](#).

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 that 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. The CO shall ensure that only encrypted drives are attached.

Detailed instructions to monitor and troubleshoot the systems are provided in the [HPE Smart Array SR 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. To zeroize the module, the module operator must start the HPE SSA utility and select the controller to be cleared. Then, the operator shall follow the steps below to complete the zeroization process:

7. Under **Actions**, click **Clear Configuration**.
8. A new window appears, confirming the request to clear the controller's configuration. To continue, click **Clear**.
9. A new window appears, displaying controller settings and configuration. To continue, click **Finish**.
10. Click **Configure**.
11. Under **Tools**, click **Encryption Manager**.
12. Log into the **Encryption Manager**.
13. Under **Utilities**, click **Clear Encryption Configuration**.

Clearing all encryption settings will clear all secrets, keys, CSPs, and passwords from the controller. The controller 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 Additional Usage Policies

This section notes additional policies below that must be followed by module operators:

- HPE SSA exists in three interface formats: the HPE SSA GUI, the HPE SSA CLI²³, and the HPE SSA Scripting Interface. The Crypto Officer shall configure, monitor, and manage the modules through the SSA GUI only.
- The SSA CLI and the SSA Scripting Interface shall not be used in an Approved mode of operation. Any operation of the module using these interfaces is outside the scope of this Security Policy.
- The Crypto Officer shall not set the controller password or disable encryption.
- The Crypto Officer shall not disable volatile data encryption keys.
- The CO password shall be at least 8 characters in length.
- Plaintext volumes shall not be allowed and shall not be moved to the controller.
- Only local key management mode shall be used.

3.5 Non-FIPS-Approved Mode

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

²³ CLI – Command Line Interface

4. Acronyms

Table 9 provides definitions for the acronyms used in this document.

Table 9 – Acronyms

Acronym	Definition
AES	Advanced Encryption System
CKG	Cryptographic Key Generation
CLI	Command Line Interface
CMVP	Cryptographic Module Validation Program
CO	Crypto Officer
CSE	Communications Security Establishment
CSP	Critical Security Parameter
DDR	Double Data Rate
DEK	Data Encryption Key
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
NAND	Not And
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 2
PCI	Peripheral Component Interconnect
PCIe	PCI Express

Acronym	Definition
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
SEEPROM	Serial Electrically Erasable Programmable Read-Only Memory
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
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/>

