HPE XP8 Encrypt Backend 4pk NVMe I/O Mod (eDKBN)

FIPS 140-2
Non-Proprietary Cryptographic Module Security Policy

Version: 4.0

Date: February 01, 2021

Prepared by: Hewlett Packard Enterprise Company

Table of Contents

List of Tables

List of Figures

1 Introduction

This document defines the Security Policy for the HPE XP8 Encrypt Backend 4pk NVMe I/O Mod (eDKBN) , hereafter denoted the module. The module is 32 Gb/s PCIe I/O module with Encryption. The module provides high speed data at rest encryption for HPE storage. In other words, the module encrypts data onto SSDs and decrypts data read from SSDs using XTS-AES. The XTS-AES mode was approved by CMVP for protecting the confidentiality of data on storage devices. The module meets FIPS 140-2 overall Level 2 requirements.

Table 1 – Cryptographic Module Configurations

	Module	HW P/N and Version	FW Version
1	HPE XP8 Encrypt Backend 4pk NVMe I/O Mod (eDKBN)	P/N: 3292549-A Version: A	90-00-01

The module is intended for use by US Federal agencies and other markets that require FIPS 140-2 validated PCIe I/O module used for HPE storage system with data at rest encryption feature. The module is a hardware cryptographic module with multi-chip embedded embodiment.

The FIPS 140-2 security levels for the module are as follows:

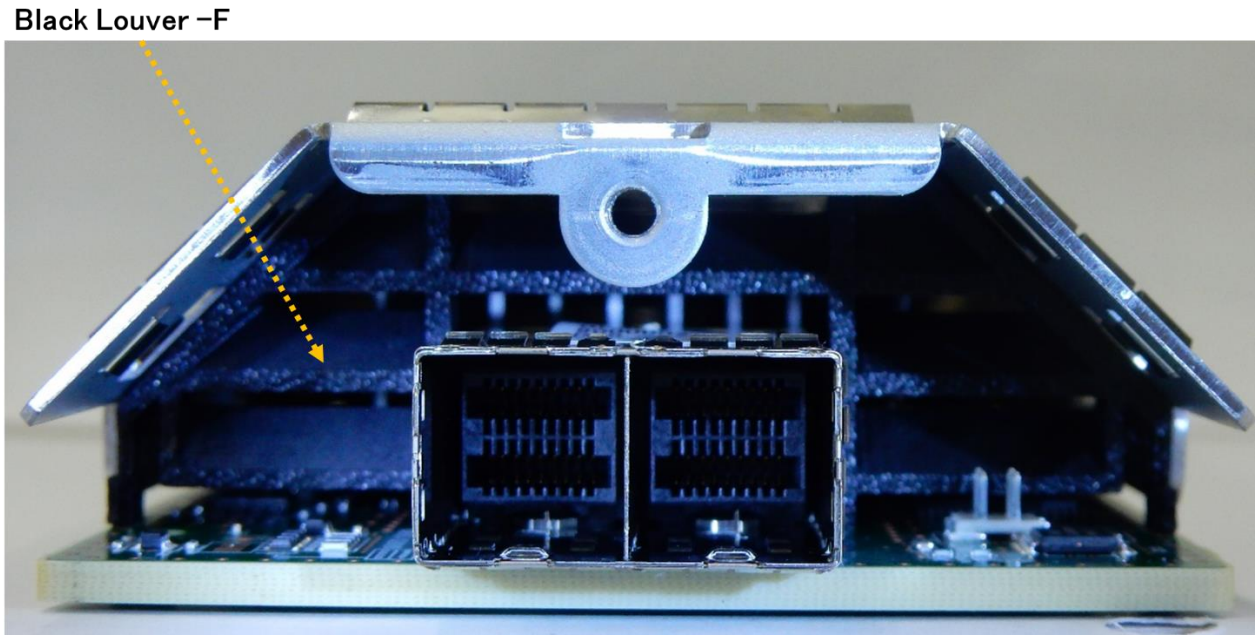
Table 2 – Security Level of Security Requirements

Security Requirement	Security Level
Cryptographic Module Specification	2
Cryptographic Module Ports and Interfaces	2
Roles, Services, and Authentication	2
Finite State Model	2
Physical Security	2
Operational Environment	N/A
Cryptographic Key Management	2
EMI/EMC	2
Self-Tests	2
Design Assurance	2
Mitigation of Other Attacks	N/A
Overall	2

1.1 Hardware and Physical Cryptographic Boundary

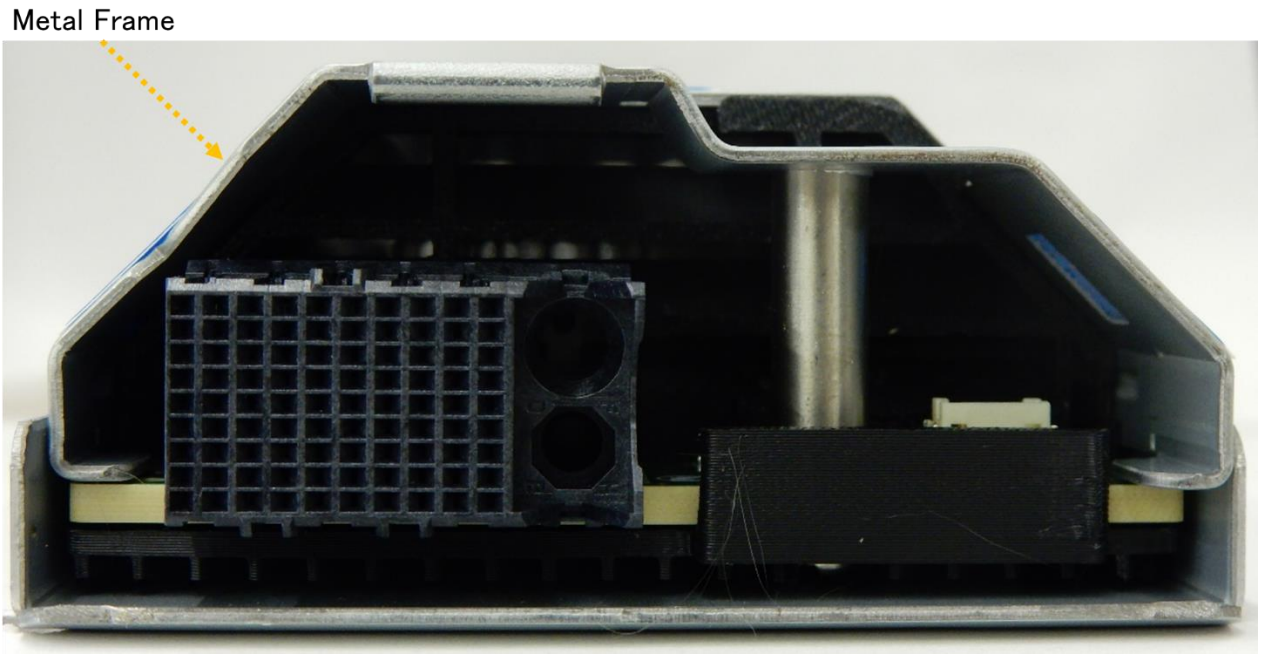
The physical form of the module is depicted in Figure 1 to 4; the physical boundary of the cryptographic module is the enclosure of metal frame shown in the Figures. Major components of the module are module board, FPGA, SDRAM, PCIe-Switch, SPI ROM and interfaces. The module board is covered with the metal frame and the tamper seal is on the screw. In addition, the black louvers are implemented to the circuit board to disturb the access from an opening of the front and back side of the module as shown figure-1(b), 2(b). The black louver and the metal frame are opaque within the visible spectrum. The module relies on HPE storage as input/output devices.

(a)

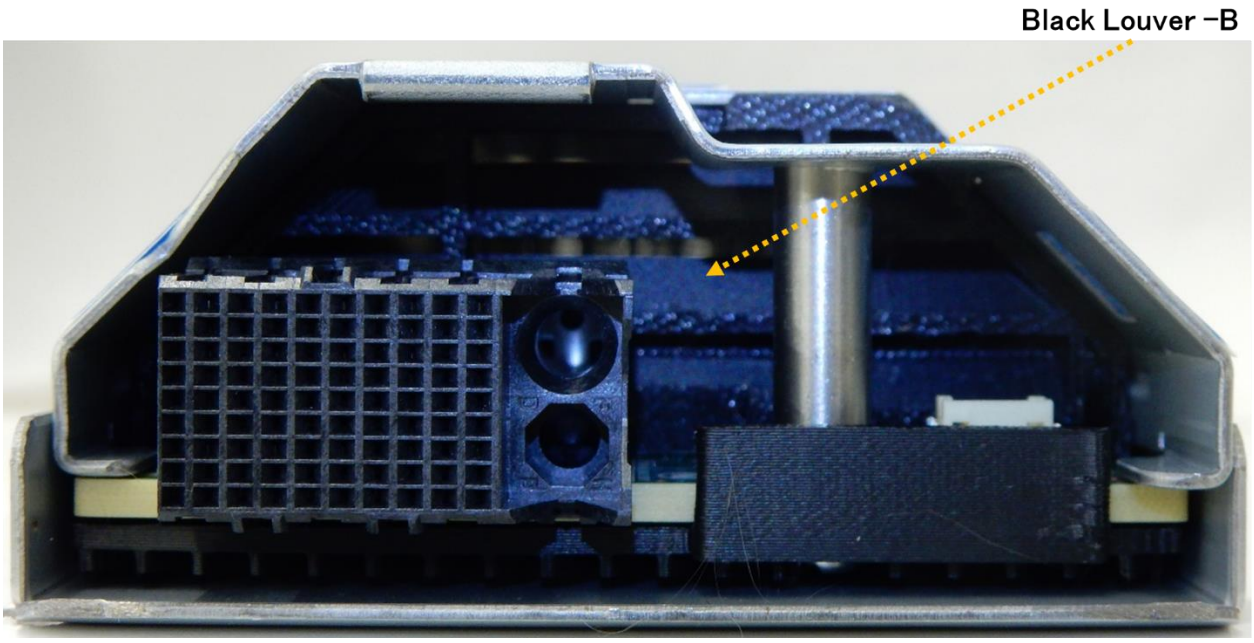


(b)

Figure 1 – (a) Front Side of the Module (b) Front Side of the Module with light



(a)



(b)

Figure 2 – (a) Back Side of the Module (b) Back Side of the Module with light

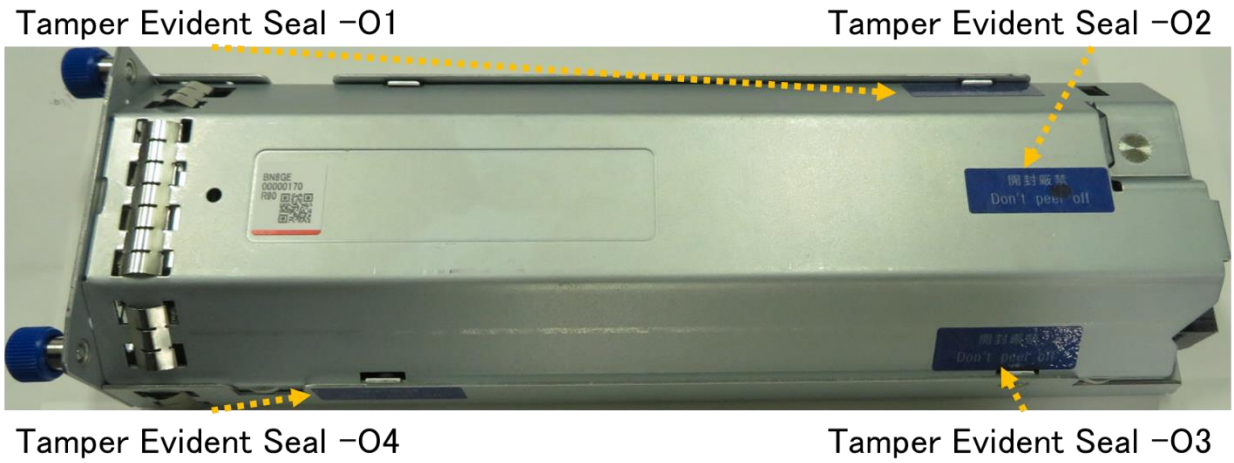


Figure 3 – Up Side of the Module

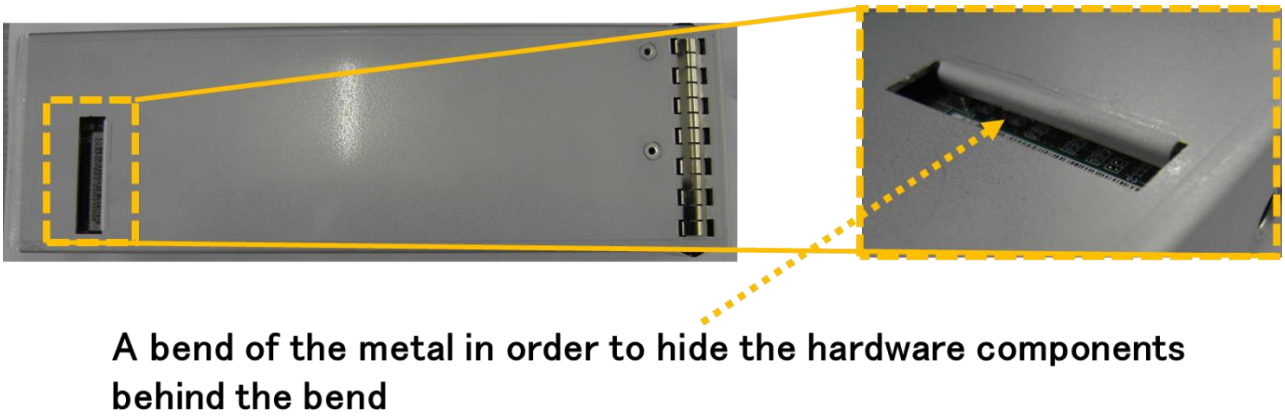


Figure 4 – Bottom Side of the Module

1.2 Firmware and Logical Cryptographic Boundary

Black bold line shows the cryptographic boundary. The FPGA is responsible for processing IOs to SSDs as well as encrypting/decrypting IOs where applicable. The PCIe-Switch is connected to FPGA, miniSAS-HD and CPU with PCI-Express interface, therefore IOs in the module can access to SSDs high speed transmission. Firmware images are stored in the SPI ROM of FPGA and PCIe-Switch. They are loaded to each FPGA and PCIe-Switch when the module power up. All functions and system initialization are performed by the FPGA, which is contained within the cryptographic boundary of the module. CSPs are stored in SPI ROM.

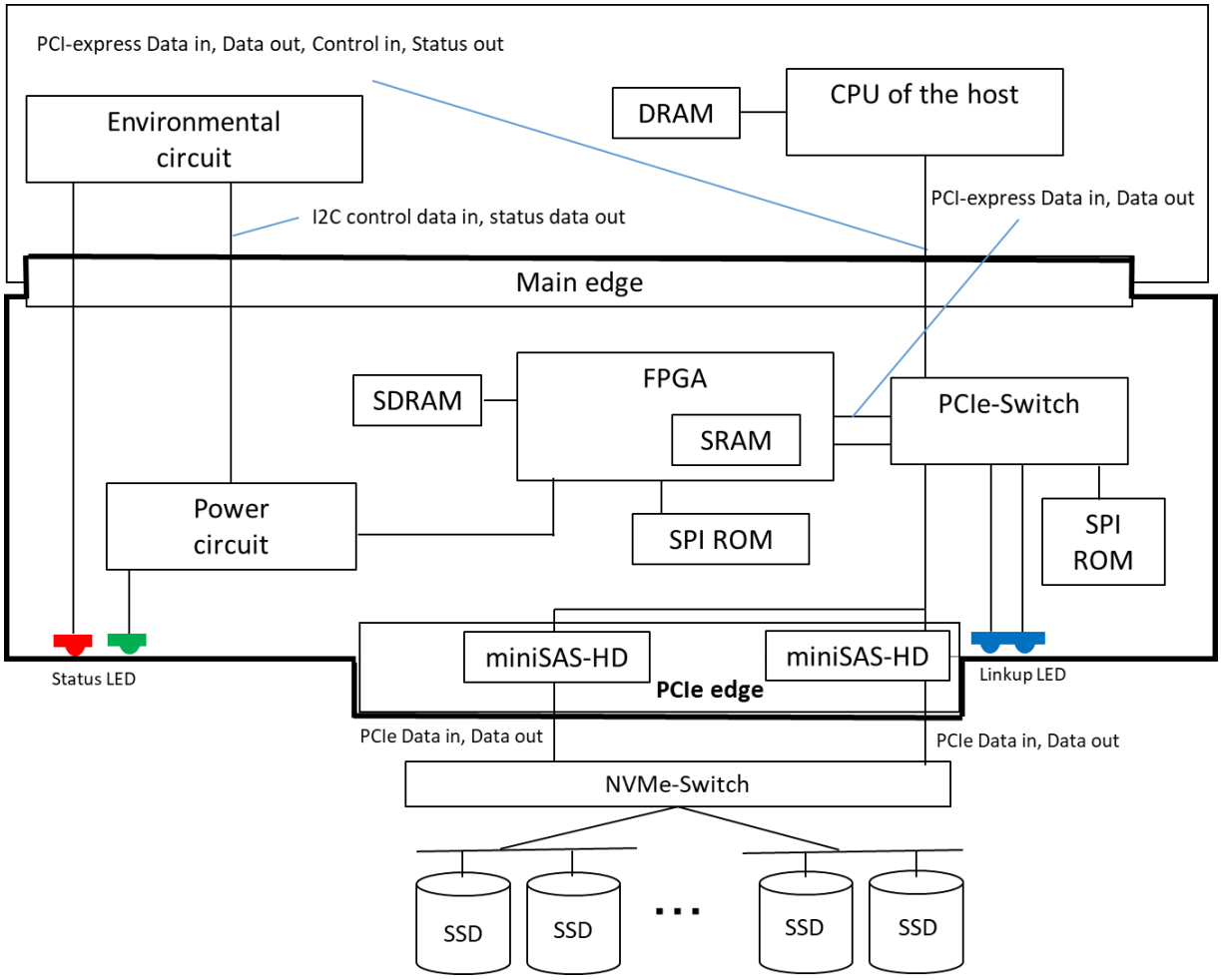


Figure 5 – Module Block Diagram

Table 3 – Ports and Interfaces

Port	Description	Logical Interface Type
Main edge	- PCI-express: plaintext input/output, module control data input, module status data output - I2C: module control data input, module status data output - Power: 12V power input	- Power - Data in - Data out - Control in - Status out
PCIe edge	- PCIe: cipher text input/output	- Data in - Data out
LED	- LED: module status output	- Status out

1.3 Mode of Operation

The module only supports FIPS-approved mode of operation, and therefore, only supports FIPS-approved security functions. No other modes of operation and no other security functions are implemented.

2 Cryptographic Functionality

The module implements the FIPS Approved cryptographic functions listed in the tables below.

The module implements no vendor affirmed security function.

Table 4 – Approved and CAVP Validated Cryptographic Functions

Algorithm	Description	Cert #
AES-ECB	[FIPS 197] [SP 800-38A] Functions: Encryption, Decryption Key sizes: 256 bits	C1594
XTS-AES mode	[FIPS 197] [NIST SP 800-38E] Functions: Encryption, Decryption Key sizes: 256 bits	C1594
AES Key Unwrap(KTS)	[FIPS 197] [NIST SP 800-38F] Functions: Key unwrapping; key establishment methodology provides 256 bits of encryption strength Key sizes: 256 bits	C1594
SHS	[FIPS 180-4] Functions: Calculation of HMAC, Message digesting of authentication data SHA sizes: SHA-256	C1594
HMAC	[FIPS 198-1] Functions: MAC generation SHA sizes: SHA-256	C1594

AES-OFB is implemented in the cryptographic algorithm implementation in the module and it is validated under C1594. However, since the module does not use AES-OFB, no command using AES-OFB is available for the module. Therefore, AES-OFB is not listed in Table 4.

2.1 Critical Security Parameters

All CSPs used by the module are described in this section. All usage of these CSPs by the module (including all CSP lifecycle states) is described in the services detailed in Section 3.

Table 5 – Critical Security Parameters (CSPs)

CSP	Description / Usage
KEKini	256-bit factory-set key used to unwrap KEK using AES Key Unwrap. KEK wrapped with KEKini using AES Key Wrap is entered to the module. KEK Management service zeroizes KEKini by overwriting with 0xFF. KEKini is generated outside the module and input to the module when the module is manufactured. KEKini is stored in the SPI ROM in the module.
Authentication data	256-bit string used to authenticate the operator. This bit string is set initial values as factory-set. Different values are set for each Role, such as User or Crypto Officer. Services other than Operator management cannot be used until initial Authentication Data is updated. The module holds the message digest of Authentication data to verify whether a digest of inputted Authentication data matches with it or not. SHA-256 is used for digesting the Authentication data. Although the message digest of Authentication data is not considered as a CSP, it can be zeroized by the Operator Management service (overwriting with 0xFF). Authentication data is stored in the SPI ROM in the module. The initial Authentication data set at factory is distributed to a user of the module.
KEK	256-bit key used to unwrap DEKs and HMAC Keys using AES Key Unwrap. DEKs and HMAC Keys wrapped with KEK using AES Key Wrap are entered to the module . KEK Management service zeroizes KEK by overwriting with 0xFF. KEK is generated outside the module, wrapped by KEKini or previous KEK, input to the module, and decrypted by KEKini or previous KEK. KEK is stored in the SPI ROM in the module.
DEK	Two 256-bit keys used for XTS-AES encryption/decryption. DEK Management service zeroizes DEK by overwriting with 0x00. DEK is generated outside the module, wrapped by KEK, input to the module, and decrypted by KEK. DEK is stored in the SRAM inside FPGA in the module.
HMAC Key	256-bit key used for authenticating firmware loaded from host . HMAC Key Management service zeroizes HMAC Key by overwriting with 0xFF. HMAC Key is generated outside the module, wrapped by KEK, input to the module, and decrypted by KEK. HMAC Key is stored in the SPI ROM in the module.

Table 6 – Public Security Parameter (PSP)

PSP	Description / Usage
Index counter of sampling test	The index counter used for the Deterministic Sampling Method shown in IG 9.12. This counter is used in the Sampling test service, and is written on the SRAM in the FPGA.

3 Roles, Authentication and Services

3.1 Assumption of Roles

The module supports two distinct operator roles, User and Cryptographic Officer (CO). The cryptographic module enforces the separation of roles, since concurrent operators are not supported. Re-authentication is enforced when changing roles. The operator must be assigned to a single role. An operator must log out before another operator can log in.

Table 6 lists all operator roles supported by the module. The module does not support a maintenance role and bypass capability. After the module powers off or execute Sampling test, all the data stored in SDRAM, including previously authenticated operators, are cleared. All CSPs are protected through APIs and logic developed for the sole purpose of integration into specific HPE host platforms. Only HPE-authored drivers can access cryptographic APIs. Further, the module functionally does not allow keys and authentication data to be disclosed, modified, or substituted in FIPS mode of operation, and does not provide an operator with any feedback that weaken the strength of the authentication mechanism during an attempted authentication.

Table 7 – Roles Description

Role ID	Role Description	Authentication Type	Authentication Data
CO	Cryptographic Officer – The role which used to FPGA assumed to perform cryptographic initialization or management functions.	Role-based	256-bit string
User	User – The role assumed to perform general security services, including cryptographic operations and other approved security functions.	Role-based	256-bit string

3.2 Authentication Methods

The module enforces role separation by requiring 256-bit authentication data for the two roles: User and Cryptographic Officer. The Authentication data for each role is inputted in plaintext to authenticate the operator when it logs in as the role. The module can login from Cryptographic Officer (User) to User (Cryptographic Officer), and check Authentication data.

The module holds the Authentication data digested by SHA-256 to verify whether a digest of inputted Authentication data matches with it or not.

Authentication process requires more than 300ms (actual measured value).

Table 8 – Authentication Description Strengths

Authentication Method	Probability of a Single Successful Random Attempt	Probability of a Successful Attempt within a Minute
Credential (authentication data)	1/2^256 The probability that a random attempt will succeed or a false acceptance will occur depends on 256-bit Authentication data. Therefore, the probability is 1/2^256, which is less than 1/1,000,000.	200/2^256 Since authentication requires more than 300ms in a worst case scenario, the module can perform at most 200 times Authentication data per minute. Therefore, the probability that multiple attacks within a given minute will be successful is 200/2^256, which is less than 1/100,000.

3.3 Services

All services implemented by the module are listed in the tables below. Each service description also describes all usage of CSPs by the service. Also, Table 9 shows the role that is able to perform the service.

Table 9 – Authenticated Services

Service	Description	CO	User
Operator Management	Adds an operator's role, and an Authentication data, updates the Authentication data and zeroizes one or all operators and Authentication data	X	X
Logout	Operator logout of the module This service can execute when operator logged in	X	X
Decrypt	Decrypts data using XTS-AES		X
Encrypt	Encrypts data using XTS-AES		X
DEK Management	Loads, updates and zeroizes DEKs	X	X
KEK Management	Loads, updates and zeroizes KEKs	X	X
HMAC Key Management	Loads, updates and zeroizes the HMAC key	X	X
Firmware Update	Updates the firmware	X	X
Abort	Abort Decrypt and Encrypt		X

Table 9 shows the services that are available without an operator authentication.

Table 10 – Unauthenticated Services

Service	Description
Module Reset (On demand power up self-tests)	Reset the module is performed power off/on
Login	Authenticates operators
Get Current Operator	Get the operator's role and an identity string of the current operator
Revert	Zeroizes CSPs, and an Authentication data returns initialization.
Show Status	Show module status with LEDs or bits in a status register Refer to backend NVMe IF specification about bits in a status register as MRPC command
Hardware Setting	Initialize hardware settings

Service	Description
Copy transmission	Copy I/O data
Sampling test (On demand firmware integrity test)	Performs the firmware integrity test using Sampling

Table 10 defines the relationship between access to CSPs and the different module services. The modes of access shown in the table are defined as:

- E = Execute: The module executes using the CSP.
- W = Write: The module writes the CSP. The write access is typically performed after a CSP is imported into the module, when the module generates a CSP, or when the module overwrites an existing CSP.
- Z = Zeroize: The module zeroizes the CSP.

Table 11 – CSP Access Rights within Services

Service	CSPs				
	KEKini	KEK	DEK	Authentication data	HMAC Key
Operator Management				W/Z	
Decrypt			E		
Encrypt			E		
DEK Management		E	W/Z		
KEK Management	E/W/Z	E/W/Z			
HMAC Key Management		E			W/Z
Firmware Update					E
Module Reset(Self-tests)					
Sampling test					
Hardware setting					
Abort					
Login				E	
Logout					
Get Current Operator					

Service	CSPs				
	KEKini	KEK	DEK	Authentication data	HMAC Key
Show Status					
Revert		Z	Z	Z	Z
Copy transmission					

4 Self-tests

4.1 Power up self-tests

Each time the module is powered up it tests that the cryptographic algorithms still operate correctly and that sensitive data have not been damaged. Power up self-tests are available on demand by power cycling or resetting the module.

On power up or reset, the module performs the self-tests described in Table 12 below. Each Firmware Integrity tests and all Cryptographic Algorithm Known Answer tests (hereafter KATs) must be completed successfully prior to any other use of cryptography by the module. If Firmware Integrity test or one of the KATs fails, the module enters the fatal error state. If Firmware Integrity test or one of the KATs fails, signal path(connected CPU to the module) doesn't link up and the module shows the result of self-tests with bits in an IO status are set as "11XXb".

Self-tests do not require any intervention or input from the operator. Power up self-tests are automatically executed when the module is powered up.

Table 12 – Power Up Self-tests

Test Target	Description
Firmware Integrity	16 or 32 bit CRC performed over all code in Flash memory.
XTS-AES mode	KATs: Encryption, Decryption Key sizes: 256 bits
AES Key Unwrap	KATs: Unwrap Key sizes: 256 bits
HMAC	KATs: Verification SHA sizes: SHA-256

Note1: The SHA-256 algorithm doesn't perform independently for self-test, but is performed the self-tests using HMAC ; thus, the SHA-256 doesn't describe Table 11.

Note2: The AES ECB (256bit) algorithm doesn't perform independently for self-test, but is performed the self-tests using XTS-AES ; thus, the AES ECB doesn't describe Table 11.

Note3: Perform 16bit CRC for PCIe-Switch bootloader Firmware and FPGA main Firmware

Perform 32bit CRC for PCIe-Switch main Firmware and Configuration data, FPGA bootloader Firmware and Configuration data

4.2 Sampling test

Since this type of module is required not to stop when it is in operation, the function to reset the PCIe-Switch component only is implemented. The “Sampling test” service described in Table 9 of the security policy is the function. The “Sampling test” service is neither power up self-tests nor on demand power up self-tests. The function of the PCIe-Switch component in this module is a data path control, and therefore, the function to reset the PCIe-Switch component is used for an error such as the case that a PCIe error is detected in a register.

A processing time requirement for resetting the PCIe-Switch only is highly demanded, that is, it is required to complete the reset in a very short time, comparing with the time for the power up self-tests. In order to address this problem, the concept of the sampling test shown in IG 9.12 is employed.

For the sampling test, the PCIe-Switch firmware component is divided into 17 portions. The number of the portions is less than 20 that is the maximum number of portions defined in IG 9.12. In the single sampling test, the integrity of 2,008,000 bits of firmware data is checked. The data size is more than 1,000,000 bits required by IG 9.12.

In addition to the integrity test, the sampling test runs the cryptographic algorithm known answer tests for all cryptographic algorithms implemented in the module.

In the sampling test, the portion of the PCIe-Switch bootloader Firmware is deterministically selected. That is, when the PCIe-Switch is reset 17 times (it means that the sampling test is called 17 times), the integrity of the whole PCIe-Switch firmware is checked.

4.3 Firmware load test

As the firmware is being externally sent to the module, the firmware images are authenticated using the HMAC authentication technique. Both a loaded firmware image and the HMAC key stored in the module are fed into the SHA engine, together with the proper SHA-256 algorithm, the calculated HMAC digest is compared with the one embedded in the firmware image. If they don't equal, the firmware authentication fails and the module indicate the state. If “Firmware Update” results in failure, the admin status field code of 11XXb is sent from the FPGA as the response. In addition, the reason of the failure is included in the admin status field code as 0x00001000 that means “Firmware image HMAC authentication failure”.

The firmware load test is automatically performed when the Firmware Update service is invoked.

Table 13 – Conditional Self-tests

Test Target	Description
Firmware Load	HMAC authentication performed when firmware is loaded.

5 Physical Security Policy

The module is a multi-chip embedded cryptographic module and conforms to Level 2 requirements for physical security. The cryptographic module consists of production-grade components. four tamper evident seals are pre-installed (at factory) as shown on the Figure 1-4 with dashed arrows. These tamper evident seals are very fragile and cannot be removed without clear signs of damage to the labels. The module is implemented with the black louver that is opaque within the visible spectrum. Also, from the

bottom side of the module, the SDRAM is hidden by bending structure to the metal frame and adding blind parts front of the module.

Table 14 – Physical Security Inspection Guidelines

Physical Security Mechanism	Inspection/Test Guidance Details
Tamper Evident Seals	Shown on the Figure 1-4 with dashed arrows. Upon receipt of the new module from HPE or whenever the existing module in the storage system is removed and re-installed, the CO should visually inspect the module and the tamper evident seals found on the module. It is recommended that the CO inspects the tamper evident seals, each time the module can be disconnected from the storage system (when the storage system is powered off, in the case of the system maintenance, etc.). If an evidence of tampering (including scratches or scrapes, signs of peeling off, tearing or damage) is detected, the CO shall immediately refuse the module installation and notify the management. CO shall also request a new replacement module with tamper evident seals by contacting HPE Customer Support.
louver	Black louver shown on the Figure 1 and 2
Metal frame	Metal frame shown on the Figure 2

6 Operational Environment

The module is designated as a limited operational environment under the FIPS 140-2 definitions. The module includes a firmware load service to support necessary updates. New firmware versions within the scope of this validation must be validated through the FIPS 140-2 CMVP. Any other firmware loaded into this module is out of the scope of this validation and require a separate FIPS 140-2 validation.

7 Mitigation of Other Attacks Policy

The module does not mitigate other attacks.

8 Security Rules and Guidance

The module design corresponds to the module security rules. This section documents the security rules enforced by the cryptographic module to implement the security requirements of this FIPS 140-2 Level 2 module.

1. The module shall provide two distinct operator roles: User and Cryptographic Officer.
2. The module shall provide role-based authentication.
3. The module shall clear previous authentications on power cycle.
4. When the module has not been placed in a valid role, the operator shall not have access to any cryptographic services shown in Table 8.
5. The operator shall be capable of commanding the module to perform the power up self-tests by cycling power or resetting the module.
6. Power up self-tests do not require any operator action.
7. Data output shall be inhibited during self-tests, zeroization, and error states.
8. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
9. There are no restrictions on which keys or CSPs are zeroized by the zeroization service.
10. The module does not support concurrent operators .
11. The module does not support a maintenance interface or role.
12. The module does not support manual key entry.
13. The module does not have any external input/output devices used for entry/output of data.
14. The module does not output plaintext CSPs.
15. The module does not support the update of the logical serial number or vendor ID.

8.1 Crypto Officer Guidance

The Crypto Officer must configure and enforce the following initialization procedures in order to operate in FIPS approved mode of operation:

1. Verify that the name and part number of module is 3292549-A (CTLSE) and version is A. The 3292549-A(CTLSE) is the part number of the board that includes the module.
2. Verify that the firmware version of module is 90-00-01.
3. Embed the module to the host storage system.
4. Supply power into the module through the host storage system.
5. Update and set the authentication data by the following personalization procedures when the module is accessed for the first time.
    a. Log in as the CO role with the factory setting CO authentication data. Use the Login service.
    b. Change the CO and User authentication data. Use the Operator Management service.
    c. Close the Login session. Use the Logout service.

8.2 User Guidance

The User must configure and enforce the following initialization procedures in order to operate in FIPS approved mode of operation

1. Enable data encryption on the parity group.
2. Format the Volumes at the parity-group level.

The initialization procedures performs automatically as inserting the module into main controller.

8.3 Physical Security Inspection

The Crypto Officer and Users shall inspect the module enclosure for evidence of tampering periodically.

9 Design Assurance Policy

9.1 Configuration Management Overview

Programs and documents are managed using proprietary web-based configuration management system (Electric Stock System). Documents for validation and hardware components are managed by revision management by proprietary ledger.

9.2 Installation, Initialization, and Start-up Overview

The procedure is described in section 8.1.

9.3 Secure Delivery and Operation Overview

The module shipped to customers from the factory or the distribution centers. The module is delivered by the contracted carrier and unpacked by the contacted service personnel on site, and its contents are confirmed by the personnel.

10 References and Definitions

The following standards are referred to in this Security Policy.

Table 15 – References

Abbreviation	Full Specification Name
[FIPS140-2]	*Security Requirements for Cryptographic Modules*, May 25, 2001
[NIST SP 800-131A]	*Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*, January 2011
[NIST SP 800-38A]	*Recommendation for Block Cipher Modes of Operation Methods and Techniques,* 2001 Edition
[FIPS 198-1]	*The Keyed-Hash Message Authentication Code(HMAC)*, July 2008
[NIST SP 800-38E]	*Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices*, January 2010
[NIST SP 800-38F]	*Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping*, December 2012

Table 16 – Acronyms and Definitions

Acronym	Definition
AES	Advanced Encryption Standard
CRC	Cyclic Redundancy Check
CSP	Critical Security Parameter
DEK	Data Encryption Key
FIPS	Federal Information Processing Standard
HMAC	Hash-based Message Authentication Code
KAT	Known Answer Test
KEK	Key Encryption Key
NIST	National Institute of Standards and Technology