Pure Storage, Inc.

FlashBlade Data Encryption Module

Hardware Version: PM8607B1-F3EI; Firmware Version: 2.10

Non-Proprietary FIPS 140-3 Security Policy

Document Version: 1.2

Date: April 2nd, 2025

Pure Storage, Inc.

2555 Augustine Dr.

Santa Clara, CA 95054

800-379-7873

Table of Contents

List of Tables

List of Figures

1 General

This document defines the Security Policy for the FlashBlade Data Encryption Module, hereafter denoted as the Module.

The Module is validated to FIPS 140-3 overall Level 1 requirements with security levels as follows:

Table 1 – Security Level of Security Requirements

Section	FIPS 140-3 Section Title	Security Level
1	General	1
2	Cryptographic Module Specification	1
3	Cryptographic Module Interfaces	1
4	Roles, Services, and Authentication	1
5	Software/Firmware security	1
6	Operational Environment	1
7	Physical Security	1
8	Non-invasive Security	N/A
9	Sensitive Security Parameter Management	1
10	Self-Tests	1
11	Life-cycle Assurance	1
12	Mitigation of Other Attacks	N/A

2 Cryptographic module specification

The Module is a Hardware cryptographic module, as defined by [ISO19790]. The module consists of the Belmar ASIC for performing AES-256 XTS mode encryption and decryption for User data, and a firmware component to provide self-test functionality. For XTS mode, encrypt and decrypt operations are symmetric, thus the module is one logical block. Furthermore, the AES-256 XTS mode encryption and decryption can only be used for storage of User data.

The Module is intended for use by US Federal agencies or other markets that require FIPS 140-3 validated Data Storage.

The physical form of the Module is depicted in Figure 2. The cryptographic boundary is the single-chip Flash Controller, including an XTS-AES-256 hardware block in the Direct Memory Access engine, as well as a firmware component running on the ASIC. This component is responsible for loading the AES key into the cryptographic hardware and running the Self-Tests. Data is encrypted while being transported by the DMA engine into the drive and decrypted by the engine on the way out. The diagram below shows the flow of data through the module.

Figure 1 – Cryptographic Boundary

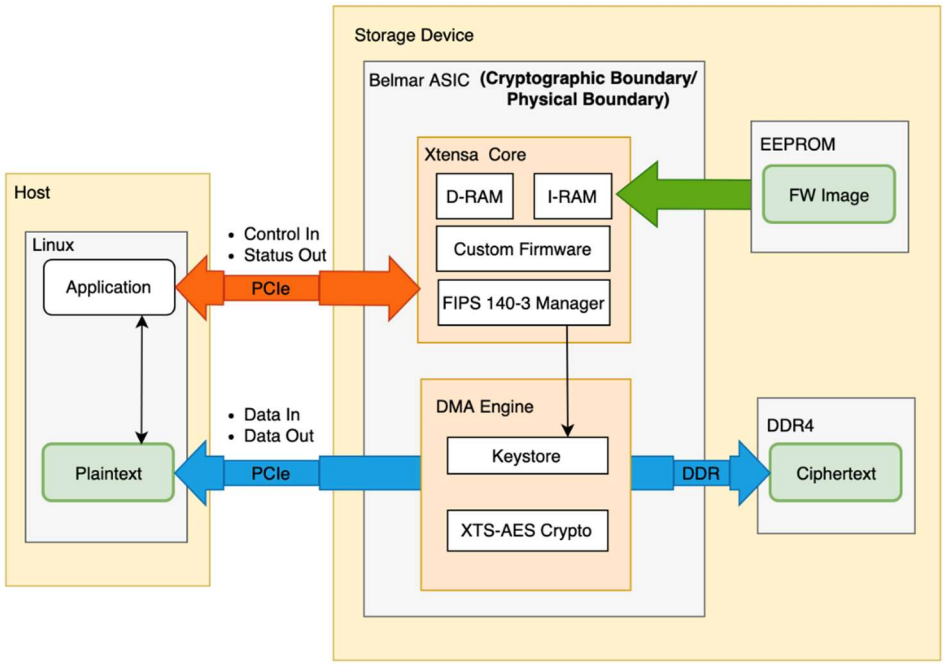

Figure 2 – Physical Perimeter

The Module was validated with the specific configuration listed below:

Table 2 – Cryptographic Module Tested Configuration

Model	Hardware [Part Number and Version]	Firmware Version	Distinguishing Features
PMC Flashtec NVMe 2016 Controller Chip	PM8607B1-F3EI	2.10	N/A

The Module implements the Approved functions listed in the table below.

Table 3 – Approved Algorithms

CAVP Cert	Algorithm and Standard	Mode/Method	Description / Key Size(s) / Key Strength(s)	Use / Function
#A906	AES [FIPS 197]	XTS [800-38E]	Key Sizes: 512 (Two 256 keys)	Encrypt/Decrypt

The module does not implement any non-Approved algorithms or services. AES is the only cryptographic algorithm available to operators.

2.1 Mode of Operation

The Module only supports an Approved mode of operation. To verify that a module is in the Approved mode of operation and that the FIPS validated version is being used, the operator must check the version output using the “Show Status” service and compare it against the FIPS certificate.

3 Cryptographic Module Interfaces

The data enters and exits the module via the memory subsystem. There are two ports to the memory subsystem, one from the PCIe interface, and one from the DDR interface, which are connected to the DMA hardware engine.

For the firmware portion of the module, the logical interfaces are the application program interfaces (APIs) through which commands are issued to the flash controller firmware. The flash controller itself communicates using the NVMe over PCIe protocol. The five interfaces which are used in the cryptographic module are specified in Table 3 below.

Table 4 – Ports and Interfaces

Physical Port	Logical Interface[1]	Data that passes over port/interface
PCIe Bus, DDR in	Data Input	Input buffer, resident in host memory or device DDR memory
PCIe Bus, DDR out	Data Output	Output buffer, resident in host memory or device DDR memory
PCIe Bus	Control Input	Arguments from NVMe over PCIe command, contain parameters such as buffer location, length, and configuration information
PCIe Bus	Status Output	API return code from NVMe over PCIe command
PCIe Bus	Power Input	None

4 Role, services, and authentication

The Module supports two distinct operator roles, Cryptographic Officer (CO) and User. The cryptographic module uses implicit mapping between services and roles to enforce the separation of roles.

The Module does not implement authentication. The Module does not support a maintenance role. The Module does not support concurrent operators.

Table 5 – Roles, Service Commands, Input and Output

Role	Service	Input	Output
CO	Key Initialization	AES Key	None
User	Encrypt	Key, plaintext	Ciphertext
User	Decrypt	Key, ciphertext	Plaintext
CO	Reset Module	API call	None
CO	Show Status	API call	Status
CO	Run self-tests	API call	Pass/Fail Status

[1] The Control Output logical interface is omitted from this table, as it is not implemented by the module.

CO	Power Off/Zeroization	None	None
CO	Power On	None	None
CO	Upgrade	FW Image	Pass/Fail Status

Table 6 – Approved Services

Service	Description	Approved Security Functions	Keys/SSPs	Roles	Access rights to Keys and/or SSPs	Indicator
Key Initialization	Set the AES Key to be used for encryption/ decryption.	-	AES Key	CO	W	Field in 'Show Status'
Encrypt/ Decrypt	Perform AES 256 Bit XTS mode encryption or decryption.	XTS-AES	AES Key	U	E	Status code
Reset Module	Resets the module and zeroizes the SSPs.	-	AES Key	CO	Z	Field in 'Show Status'
Show Status	Key Loaded (Drive Locked): (True/False) KAT Test Passed: (TEST_PASSED/ TEST_FAILED) Integrity Test Passed: TEST_PASSED/TEST_FAILED Key Init Indicator: (0 or 1) Zeroize Indicator: (0 or 1) Show State Indicator: (0 or 1) Encryption Version: (0 or 1) Approved Mode of Operation: (True/False) Version: Firmware Version from Table 2	-	-	CO	-	Field in 'Show Status'
Run self-tests	Run pre-operational self-tests on demand	-	-	CO	-	Field in 'Show Status'
Upgrade	Load Firmware to External Flash	-	-	CO	-	None

Key: G = Generate, R = Read, W = Write, E = Execute, Z = Zeroize

5 Software/Firmware security

The Module uses CRC16 to implement the integrity test. This integrity test can be run on demand using the "Run self-test" service API provided by the Module, or by power cycling the Module. The integrity test

is run automatically on power up and before the module is operational, and if the test fails then the Module will not enter an operational state.

The firmware itself is executed as a BIN executable. The Belmar ASIC has 16 separate cores, each which runs a respective binary. The binary is constructed from an ELF executable, and similarly consists of sections which are given a loading address and section size. Each section is loaded into memory in the Secondary Boot Loader during the boot process.

6 Operational Environment

The Module has a non-modifiable operational environment under the FIPS 140-3 definitions. Firmware versions validated through the FIPS 140-3 CMVP will be explicitly identified on a validation certificate, along with the Belmar ASIC model number. Any firmware or hardware not identified in this Security Policy does not constitute the Module defined by this Security Policy or covered by this validation.

7 Physical Security Policy

The Module, which has a single-chip embodiment, meets the FIPS 140-3 requirements for production grade components and standard passivation. The PMC Flashtec NVMe 2016 Controller Chip (referred to as the Belmar ASIC) the module consists of is produced for high performance enterprise workloads.

8 Non-invasive security

Not Applicable. The module does not support non-invasive attack security.

9 Sensitive Security Parameter Management

All SSPs used by the Module are described in this section. All usage of these SSPs by the Module are described in the services detailed in Section 4. The SSPs are kept in volatile write-only registers in the Module, and all intermediate values used for loading SSPs are zeroized immediately after use.

Table 7 – Sensitive Security Parameters (SSPs)

SSP Name	Strength	Security Function and Cert. Number	Generation	Import/ Export	Establishment	Storage	Zeroization	Use & Related keys
AES Key	256 bits	AES #A906	None	Electronically Input	None	Temporary Memory	Reset/ Power cycle	Encrypt/ Decrypt

9.1 Zeroization

All SSPs managed by the module are stored in volatile memory. The Crypto-office can zeroize all SSPs by:

- removing power from the module, or
- invoking the 'reset module' service.

10 Self-tests

Each time the Module is powered on it will perform self-tests to ensure its proper operation. Per FIPS 140-3 these are categorized as either pre-operational self-tests or conditional self-tests. Pre-operational self–tests are available on demand by power cycling the module, or through an API call. Conditional self-tests are available through an API call. All cryptographic algorithm self-tests (CASTs) must complete successfully prior to any other use of cryptography by the Module.

The Module performs the following pre-operational self-tests.

- Firmware Integrity: CRC16 EDC of the firmware component, performed within the cryptographic boundary over the whole binary

The Module performs the following conditional cryptographic algorithm self-tests:

- AES-XTS-256 Encrypt/Decrypt KAT

The Module performs the following conditional critical function self-tests:

- XTS Duplicate key test - during key initialization the module checks that XTS key1 does not equal key2 and fails to load the key if this condition is not satisfied (IG C.I XTS-AES).

All pre-operational self-tests must be completed successfully prior to any other use of cryptography by the Module. The only pre-operational test for the Module is the integrity test. If the integrity test fails, then the firmware will fail to start the Belmar ASIC, prohibiting any read or write operations. The drive will return a CRC_CHECK_FAILED code and control input will not be allowed.

To become operational, the AES KAT test must be run. This will be run automatically during the “key initialization service” or can be run manually through the “run self-test” service. If the AES KAT test fails, the Module enters the KAT_ERROR error state, and the output of the “Show Status” service will be kat_test_passed=TEST_FAILED.

Upon power-up, a user can read the self-test status through the "Show Status” service to determine the status of the self-tests.

If the module is in the error state, then all cryptographic functions will be disabled, and a power cycle is required to get out of the error state.

Below are the possible ways to enter the error state, and the accompanying status indicators:

- Integrity Test Failed
  - integrity_test_status=TEST_FAILED
- AES KAT Test Failed
  - kat_test_status=TEST_FAILED
- Key Initialization Failed
  - key_init_status=TEST_FAILED

11 Life-cycle Assurance

11.1 General requirements

The FlashBlade Data Encryption Module is integrated into Pure Storage Inc. storage products and is not delivered on its own as a standalone product. Pure Storage Inc.'s internal development process guarantees that the correct version of module goes with its intended products.

11.2 Crypto Officer Guidance

The module is configured to be operational by default. If the Flash Controller Chip starts up successfully and has successfully passed the Self-tests detailed in Section 10, it is operating correctly and can begin servicing requests.

All the functions, ports and logical interfaces described in this document are implicitly available to the Crypto Officer and User roles. The module only provides approved functions, and as such there are no special procedures to configure or administer the approved mode of operation. There are no requirements for non-administrator operators.
The operator can verify that the module is in the Approved mode of operation and that the FIPS validated version is being used, by checking the version output using the "Show Status" service. This is performed by invoking the *'wssdtool dump'* command. The output will include the following:

```
Chip version: NVMe2016.B1
Firmware Version: 2.10.27
```

11.3 End of Life

When decommissioning the Flash Controller Chip a reset of the power will sanitize all SSPs in the module (the AES-XTS keys).

12 Mitigation of Other Attacks Policy

Not Applicable. The module does not support mitigation of other attacks.

13 References and Definitions

The following standards are referred to in this Security Policy.

Table 8 – References

Abbreviation	Full Specification Name
[FIPS140-3]	*Security Requirements for Cryptographic Modules*, May 25, 2001
[IG]	*Implementation Guidance for FIPS PUB 140-3 and the Cryptographic Module Validation Program*
[197]	*National Institute of Standards and Technology, Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, November 26, 2001*
[38E]	*Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices*, January 2010

Table 9 – Acronyms and Definitions

Acronym	Definition
AES	Advanced Encryption Standard
ACVP	Automated Cryptographic Validation Program
CMVP	Cryptographic Module Validation Program
CO	Cryptographic Officer
SSP	Sensitive Security Parameter
XTS	**X**EX (XOR Encrypt XOR) **T**weakable block cipher with ciphertext **S**tealing
EPROM	A programmable NOR flash memory
FIPS	Federal Information Processing Standard
KAT	Known Answer Test
NVMe	Non-Volatile Memory Express
DMA	Direct Memory Access
SDMA	Sector DMA, moves memory in Sector chunks