

**Pure Storage, Inc.**

**Purity Encryption Module**

**FIPS 140-2 Cryptographic Module Non-Proprietary  
Security Policy**

**Version: 1.1**

**Date: 11/08/2022**

Pure Storage, Inc.

650 Castro Street, Suite #260

Mountain View, CA 94041

800-379-7873

## Table of Contents

- [1 Introduction](#)**
  - [1.1 Cryptographic Boundary](#)
  - [1.2 Mode of Operation](#)
- [2 Cryptographic Functionality](#)**
  - [2.1 Critical Security Parameters](#)
- [3 Roles, Authentication and Services](#)**
  - [3.1 Assumption of Roles](#)
  - [3.2 Services](#)
- [4 Self-tests](#)**
- [5 Physical Security Policy](#)**
- [6 Operational Environment](#)**
- [7 Mitigation of Other Attacks Policy](#)**
- [8 Security Rules and Guidance](#)**
- [9 References and Definitions](#)**

## List of Tables

- [Table 1 – Cryptographic Module Configurations](#)
- [Table 2 – Security Level of Security Requirements](#)
- [Table 3 – Ports and Interfaces](#)
- [Table 4 – Approved and CAVP Validated Cryptographic Functions](#)
- [Table 5 – Non-Approved but Allowed Cryptographic Functions](#)
- [Table 6 – Critical Security Parameters \(CSPs\)](#)
- [Table 7 – Roles Description](#)
- [Table 8 – Services](#)
- [Table 9 – CSP Access Rights within Services](#)
- [Table 10 – Power Up Self-tests](#)
- [Table 11 – Conditional Self-tests](#)
- [Table 12 – Critical Function Test](#)
- [Table 13 – References](#)
- [Table 14 – Acronyms and Definitions](#)

## List of Figures

- [Figure 1 – Module Diagram](#)

## 1 Introduction

This document defines the Security Policy for the Pure Storage Inc. Purity Encryption Module, hereafter denoted the Module. The Module is a multi-chip standalone software-hybrid module (within the FlashArray product) and is run on a General-Purpose Computer (GPC) with a modifiable operational environment. The Module meets FIPS 140-2 overall Level 1 requirements.

**Table 1 – Cryptographic Module Configurations**

Module	SW Version	Operational Environment
Purity Encryption Module	1.3	Operating System: Purity OS 5.3 Hardware Platform: M70R2 CPU: Intel Xeon E5-2698 v4 with AES-NI
Purity Encryption Module	1.3	Operating System: Purity OS 5.3 Hardware Platform: X70R3 CPU: Intel Xeon 6230 with AES-NI
Purity Encryption Module	1.3	Operating System: Purity OS 5.3 Hardware Platform: C60 CPU: Intel Xeon 6130 with AES-NI
Purity Encryption Module	1.3	Operating System: Purity OS 6.1 Hardware Platform: X20R2 CPU: Intel Xeon 4114 with AES-NI
Purity Encryption Module	1.3	Operating System: Purity OS 6.1 Hardware Platform: X70R3 CPU: Intel Xeon 6230 with AES-NI
Purity Encryption Module	1.3	Operating System: Purity OS 6.1 Hardware Platform: C60 CPU: Intel Xeon 6130 with AES-NI
Purity Encryption Module	1.3	Operating System: Purity OS 6.2 Hardware Platform: XL170 CPU: Intel Xeon 8368 with AES-NI

The Module is intended for use by US Federal agencies and other markets that require FIPS 140-2 validated Data Storage. The Module is a multi-chip standalone, software-hybrid embodiment; the cryptographic boundary is the dynamically linked library libcrypto.so, and the configuration file libcrypto.hash, and the Intel Xeon CPU.

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

**Table 2 – Security Level of Security Requirements**

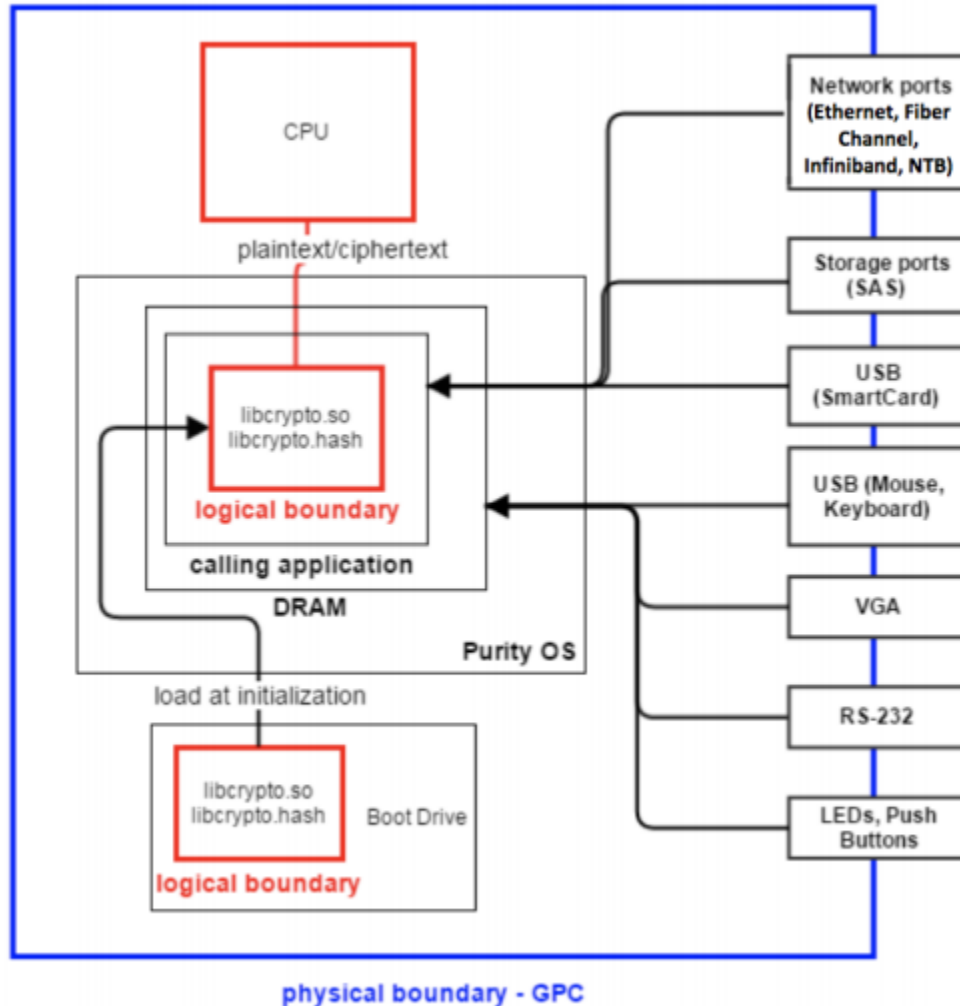
Security Requirement	Security Level
Cryptographic Module Specification	1
Cryptographic Module Ports and Interfaces	1
Roles, Services, and Authentication	1
Finite State Model	1
Physical Security	1
Operational Environment	1
Cryptographic Key Management	1
EMI/EMC	1
Self-Tests	1
Design Assurance	2
Mitigation of Other Attacks	1
<b>Overall Level</b>	<b>1</b>

## 1.1 Cryptographic Boundary

The cryptographic boundaries of the Module are depicted in Figure 1; the blue outline depicts the physical cryptographic boundary, and the red outline depicts the logical cryptographic boundary. The module is implemented on a General-Purpose PC with the following standard components:

1. Processors: Intel Xeon CPU with AES-NI and RDSEED
2. Read-only memory (ROM) integrated circuits for program executable code and data consistent with a GPC platform
3. Random access memory (RAM) integrated circuits for temporary data storage consistent with a GPC platform
4. Other active electronic circuit elements consistent with a GPC platform
5. Power supply components consistent with a GPC platform
6. Circuit boards or other component mounting surfaces consistent with a GPC platform
7. Enclosures, including any removable access doors or covers consistent with a GPC platform
8. Physical connectors for devices outside of the module consistent with a GPC platform
9. Software/firmware modules that are unlikely to be modified consistent with a GPC platform

Pure Storage bundles both the hardware and software together for customers, and also includes several additional network and storage interfaces that are documented in the figure below:



**Figure 1 – Module Diagram**

The table below contains the physical ports on the GPC, and a mapping to the FIPS logical interface types. The module itself does not rely on any physical PC interfaces, and instead only provides a logical API interface to the calling application. The module’s logical API interfaces, and their FIPS logical interface types, are listed in User Guidance.

**Table 3 – Ports and Interfaces**

Port	Description	FIPS Logical Interface Type
Ethernet Ports	Gigabit Ethernet interfaces for replication, management, and iSCSI. The calling application will pass data coming from replication and iSCSI protocols to the module.	Data in   Data out   Control in   Status out

Port	Description	FIPS Logical Interface Type
Infiniband / NTB (Non-Transparent Bridge)	Communication between two PCs (primary/secondary) for High Availability purposes.	Control in   Status out
Fiber Channel	Hosts storage services for other Fiber channel devices on the SAN. The calling application will pass data coming from/destined to SAN devices to/from the module.	Control in   Data in   Data out   Status out
VGA	Connects video for local administration of the PC.	Control in   Status out
RS-232	Offers local administration of the PC.	Control in   Status out
USB (mice and keyboard devices)	Connects mice and keyboard devices for local administration of the PC.	Power   Control in
USB (smart card devices)	Connects Spyrus Rosetta Series II Smart Card to the calling application.	Power   Control in   Data in   Data out   Status out
Power Supply	2x 110V	Power
SAS	(Serial Attached SCSI) Communication between PC and storage shelves.	Control in   Data in   Data out   Status out
LEDs	Status indicators including: Pure Storage Logo LED, power LED, boot drive LED	Status out
Push Button	Power on push button	Control In

## 1.2 Mode of Operation

The module contains a single FIPS approved mode of operation. To verify that a module is in the approved mode of operation, the user can verify the cryptographic module version matches the validated version in the Security Policy through the “pureversion -c” command offered by the operational environment which accesses the Show Version service of the module.

## 2 Cryptographic Functionality

The Module implements the FIPS Approved and Non-Approved but Allowed cryptographic functions listed in the table(s) below,

**Table 4 – Approved and CAVP Validated Cryptographic Functions**

Algorithm	Description	Cert #
AES	[FIPS 197, SP 800-38A] Functions: Encryption, Decryption Modes: ECB, CTR Key sizes: 128, 256 bits	A727
AES Key Wrapping	[SP 800-38F] Functions: Encryption, Decryption (Wrap, Unwrap) Modes: KW Key sizes: 128, 256 bits	A727
CKG	[SP 800-133r2] Section 4 Section 6.1 Direct symmetric key generation using unmodified DRBG output	Vendor Affirmed
DRBG	[SP 800-90A] Functions: CTR DRBG Security Strengths: 256 bits	A727
HMAC-SHA-256	[FIPS 198-1] Functions: Verification	A727
SHA-256	[FIPS 180-4] Functions: Used within HMAC Verification	A727

**Table 5 – Non-Approved but Allowed Cryptographic Functions**

Algorithm	Description
NDRNG	[Annex C] Hardware Non-Deterministic RNG. The NDRNG output (256-bit) is used to seed the FIPS Approved DRBG. The implementation uses the Intel Xeon CPU instruction RDSEED, along with post-processing.

The module does not implement any non-FIPS-allowed algorithms.



## 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 4.

**Table 6 – Critical Security Parameters (CSPs)**

CSP	Description / Usage
Data Encryption Key (DEK)	<p>Purpose: Used to encrypt and decrypt storage data destined for SAS drives or SAN protocols.</p> <p>Algorithm: AES</p> <p>Size: 128 or 256 bits</p> <p>Mode: CTR</p> <p>Generation / Entry:</p> <ol style="list-style-type: none"> <li>1. Generated internally by DRBG on product initialization</li> <li>2. Imported as wrapped by DEKEK on product startup</li> </ol> <p>Output: Output in encrypted form (with DEKEK)</p>
Data Encryption Key (DEK) AES Counter	<p>Purpose: Used in AES counter-mode while providing encryption/decryption services for storage data.</p> <p>Algorithm: AES</p> <p>Size: 32 bits</p> <p>Mode: CTR</p> <p>Generation / Entry: Imported as plaintext over electronic API</p> <p>Output: N/A</p>
Data Encryption Key Encryption Key (DEKEK)	<p>Purpose: Used to wrap the DEK.</p> <p>Algorithm: AES</p> <p>Size: 128 or 256 bits</p> <p>Mode: ECB</p> <p>Generation / Entry:</p> <ol style="list-style-type: none"> <li>1. Generated internally by DRBG on product initialization and/or customer rekey request</li> <li>2. Imported as split-knowledge for key recovery</li> <li>3. Imported as plaintext on product startup over electronic API</li> </ol> <p>Output:</p> <ol style="list-style-type: none"> <li>1. As split-knowledge</li> <li>2. As plaintext over the API (for RDL function)</li> </ol>

CSP	Description / Usage
DRBG entropy input	Purpose: Internally used to provide entropy for DEK and DEKEK generation. Algorithm: SP 800-90A Size: 256 bits Mode: CTR Generation / Entry: Generated internally via RDRSEED calls Output: N/A
DRBG personalization string	Purpose: Internally used to provide entropy for DEK and DEKEK generation. Algorithm: SP 800-90A Size: Max 1024 bits Mode: CTR Generation / Entry: Generated internally based on versioning information. Output: N/A
DRBG Counter value	Purpose: Internally used as a state value for the SP 800-90A CTR DRBG. Size: 128 bits Mode: CTR Generation / Entry: Generated internally Output: N/A

### 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 using implicit mapping between services and roles.

The Module does not support a maintenance role and/or bypass capability. The Module does not support concurrent operators. On each power cycle, all state is cleared. The module is a Level 1 software-hybrid module and does not support authentication.

**Table 7 – Roles Description**

Role ID	Role Description
CO	Cryptographic Officer – The calling process which powers on/off the module.
User	User – The calling process which accesses any API functionality.

#### 3.2 Services

All services implemented by the Module are listed in the table(s) below. Each service description also describes all usage of CSPs by the service. In addition, each service is mapped to a specific role, shown by the “X” in the appropriate column.

**Table 8 –Services**

Service	Description	CO	U
Data Storage Encrypt/Decrypt	Provides data encryption / decryption for calling application.		X
DEKEK Import/Export in plaintext	The DEKEK is exported by the module, transformed by the calling application, and re-imported.		X
DEK Import/Export in encrypted form	When the configuration is changed, the DEK is wrapped by the DEKEK and exported. The wrapped DEK is imported (by the calling application) on module's powerup.		X
DEKEK Import/Export as split-knowledge	After a new DEKEK is generated, the keys are exported in split-knowledge form. They are stored by the calling application. On demand, the DEKEK is imported in split knowledge form, (provided by the calling application).		X
SP 800-90A DRBG	Provides random numbers to the calling application, also serves to generate keys such as DEKEK and DEK and export them immediately.		X
Module Power-on (Run self-tests)	The module runs all self-tests implicitly at power-up.		X

Service	Description	CO	U
Show Status	The module automatically calls the FOEd logging service as events, such as power-up, occur.		X
Show Version	Display the version of the module.		X
Zeroize	Destroys all CSPs by powering down the physical GPC.	X	

Table 9 defines the relationship between access to CSPs and the different module services. The modes of access shown in the table are defined as:

- G = Generate: The module generates the CSP.
- R = Read: The module reads the CSP. The read access is typically performed before the module uses the CSP.
- 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 9 – CSP Access Rights within Services**

Service	CSPs						
	DEK	DEKEK	DEK Counter	DEK Nonce	DRBG Pers. String	DRBG Entropy	DRBG Counter
Data Storage Encrypt/ Decrypt	R		RW	RW			
DEKEK Import/Export in plaintext		RW					
DEK Import/Export in encrypted form	RW						
DEKEK Import/Export as split-knowledge		RW					
SP 800-90A DRBG	G	G			GR	GR	GW
Module Power-on (Run self-tests)							
Show Status							
Show Version							
Zeroize	Z	Z	Z	Z	Z	Z	Z

## 4 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 the module.

On power up or reset, the Module performs the self-tests described in Table 10 below. All KATs must be completed successfully prior to any other use of cryptography by the Module. If one of the KATs fails, the Module enters the FIPS error state. Recovery from the FIPS error state is accomplished by re-invoking the module, which creates a new instance. Successful completion of self-tests is indicated by a status message and returning control to the calling application from the Default Entry Point successfully.

**Table 10 – Power Up Self-tests**

Test Target	Description
Software Integrity	HMAC-SHA-256 of the executable code.
AES	KATs: Encryption, Decryption Modes: ECB, CTR, KW Key sizes: 128 bits, 256 bits
DRBG	KATs: CTR DRBG per SP800-90A Section 11.3 Requirements Security Strength: 256 bits
SHA	KATs: Hash SHA size: SHA-256

**Table 11 – Conditional Self-tests**

Test Target	Description
NDRNG	NDRNG Continuous Test performed when a random value is requested from the NDRNG.
DRBG	DRBG Continuous Test performed when a random value is requested from the DRBG.

**Table 12 – Critical Functions Test**

Test Target	Description
Reed-Solomon	Performs a secret-splitting and joining and verifies the result of each step.

## 5 Physical Security Policy

The module is a multi-chip standalone, software hybrid embodiment module with a specific CPU family (Intel Xeon CPU with AES-NI and RDSEED - E5 Family or Scalable Processor Family) installed within a GPC. The module utilizes a production grade hardware component with standard passivation applied to it.

## 6 Operational Environment

The Module is designated as a modifiable operational environment under the FIPS 140-2 definitions. The operational environment is the Purity Operating System (OS) version 5.3. 6.1 or 6.2, which is based off of Ubuntu Linux 16. The operational environment implicitly enforces single mode of operation by managing process memory of the module and ensuring each calling process is logically separated and protected.

The module was tested on the following platforms:

- Purity OS 5.3 running on M70R2 with Intel Xeon E5-2698 v4 with AES-NI;
- Purity OS 5.3 running on X70R3 with Intel Xeon 6230 with AES-NI; and
- Purity OS 5.3 running on C60 with Intel Xeon 6130 with AES-NI
- Purity OS 6.1 running on X20R2 with Intel Xeon 4114 with AES-NI;
- Purity OS 6.1 running on X70R3 with Intel Xeon 6230 with AES-NI;
- Purity OS 6.1 running on C60 with Intel Xeon 6130 with AES-NI; and
- Purity OS 6.2 running on XL170 with Intel Xeon 8368 with AES-NI

The module also operates on the following platforms running on Intel Xeon with AES-NI and remains compliant with FIPS 140-2 validation because it is possible to operate without any source code change:

- //M models
  - Purity OS 6.2 running on M10R2 (vendor affirmed)
  - Purity OS 6.2 running on M20R2 (vendor affirmed)
  - Purity OS 6.2 running on M50R2 (vendor affirmed)
  - Purity OS 6.2 running on M70R2 (vendor affirmed)
- //X models
  - Purity OS 6.2 running on X70 (vendor affirmed)
  - Purity OS 6.2 running on X10R2 (vendor affirmed)
  - Purity OS 6.2 running on X20R2 (vendor affirmed)
  - Purity OS 6.2 running on X50R2 (vendor affirmed)
  - Purity OS 6.2 running on X70R2 (vendor affirmed)
  - Purity OS 6.2 running on X90R2 (vendor affirmed)
  - Purity OS 6.2 running on X10R3 (vendor affirmed)
  - Purity OS 6.2 running on X20R3 (vendor affirmed)
  - Purity OS 6.2 running on X50R3 (vendor affirmed)
  - Purity OS 6.2 running on X90R3 (vendor affirmed)
- //XL models
  - Purity OS 6.2 running on XL130 (vendor affirmed)
- //C models
  - Purity OS 6.2 running on C40 (vendor affirmed)
  - Purity OS 6.2 running on C60 (vendor affirmed)
- Cloud Block Store models
  - Cloud Block Store V10 Purity OS 6.2 running on Amazon Web Services (vendor affirmed)
  - Cloud Block Store V20 Purity OS 6.2 running on Amazon Web Services (vendor affirmed)
  - Cloud Block Store V10 Purity OS 6.2 running on Microsoft Azure (vendor affirmed)
  - Cloud Block Store V20 Purity OS 6.2 running on Microsoft Azure (vendor affirmed)

○ Note: The CMVP makes no claim as to the correct operation of the module on these operational environments.

## 7 Mitigation of Other Attacks Policy

The module implements Reed-Solomon splitting to export the DEKEK in a manner that requires  $n/2 + 2$  parts in order to recover the DEKEK for all  $n$  parts. Each part is stored on an externally connected SAS by the calling application. Therefore, the DEKEK is recoverable only when sufficient parts of the DEKEK are supplied.

The reference for the original article describing this method is: "How to share a secret", Communications of the ACM 22 (11): 612–613, [doi:10.1145/359168.359176](https://doi.org/10.1145/359168.359176)



## 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 1 module.

1. The module shall provide two distinct operator roles: User and Cryptographic Officer.
2. The module does not provide authentication, and implicitly maps the services offered to the respective role.
3. The operator shall be capable of commanding the module to perform the power up self-tests by cycling power or resetting the module.
4. Power up self-tests do not require any operator action.
5. Data output shall be inhibited during key generation, self-tests, zeroization, and error states.
6. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
7. There are no restrictions on which keys or CSPs are zeroized by the zeroization service.
8. The module does not support concurrent operators.
9. The module does not support a maintenance interface or role.
10. The module does not support manual key entry.
11. The module does not have any external input/output devices used for entry/output of data.
12. The module does not enter or output plaintext CSPs from the physical boundary.
13. The module does not output intermediate key values.

## 9 References and Definitions

The following standards are referred to in this Security Policy.

**Table 13 – References**

Abbreviation	Full Specification Name
[FIPS140-2]	Security Requirements for Cryptographic Modules, May 25, 2001
[SP 800-131A rev2]	Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths, March 2019
[SP 800-90A rev1]	Recommendation for Random Number Generation Using Deterministic Random Bit Generators, June 2015
[SP 800-38A]	Recommendation for Block Cipher Modes of Operation, Methods and Techniques, 2001 Edition

**Table 14 – Acronyms and Definitions**

Acronym	Definition
AES	Advanced Encryption Standard
AES-NI	Advanced Encryption Standard (Intel x86 Instruction)
API	Application Programming Interface
CAVP	Cryptographic Algorithm Validation Program
CMVP	Cryptographic Module Validation Program
CO	Cryptographic Officer
CPU	Central Processing Unit
CSP	Critical Security Parameter
CTR	Counter Mode
DEK	Data Encryption Key
DEKEK	Data Encryption Key Encryption Key
DRBG	Deterministic Random Number Generator
ECB	Electronic Code Book
EMI / EMC	Electromagnetic Interference / Electromagnetic Compatibility
FIPS	Federal Information Processing Standard
GPC	General Purpose Computer
HMAC	Hashed Message Authentication Code
iSCSI	SCSI protocol over TCP/IP (IETF draft standard)

Acronym	Definition
KAT	Known Answer Test
KEK	Key Encryption Key
LED	Light Emitting Diode
NDRNG	Non-Deterministic Random Number Generator
NTB	Non-Transparent Bridge
OS	Operating system
PC	Personal Computer
RAM	Random Access Memory
RDSEED	Deterministic Random Number Generator (Intel x86 Instruction)
ROM	Read Only Memory
RS-232	Recommended Standard 232 (computer serial interface, IEEE)
SAN	Storage Area Network
SAS	Serial-Attached SCSI (Small Computer System Interface)
SHA	Secure Hash Algorithm
USB	Universal Serial Bus
VGA	Video Graphics Adapter