Pure Storage, Inc.

Purity Encryption Module

Version: FA-2.0

FIPS 140-3 Non-Proprietary Security Policy

Prepared for:

Pure Storage, Inc.
2555 Augustine Drive
Santa Clara,
California 95054, USA

Prepared by:

TERON LABS

www.teronlabs.com

Table of Contents

List of Tables

List of Figures

1 General

1.1 Overview

This document defines the non-proprietary Security Policy for the Purity Encryption Module version FA-2.0, hereafter denoted the module. The module is a multi-chip standalone software module (within the FlashArray product) and is run on a host device within a modifiable operational environment. The module meets FIPS 140-3 overall Level 1 requirements.

1.2 Security Levels

The Overall Security rating of the module is Level 1. The table below contains the security levels for all FIPS 140-3 sections.

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	N/A
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
	Overall Level	1

Table 1: Security Levels

2 Cryptographic Module Specification

2.1 Description

Purpose and Use:

Purity Encryption Module is a standalone cryptographic module for the Purity Operating Environment for FlashArray (Purity/FA). Purity/FA powers Pure Storage's Flash Array family of products which provide economical all-flash storage. Purity Encryption Module enables Flash Array to support always-on, inline encryption of data with an internal key management scheme that requires no user intervention.

Module Type: Software

Module Embodiment: Multi-Chip Standalone

Cryptographic Boundary:

The cryptographic boundary of the cryptographic module encompasses:

- libps_fips.so – the single, dynamically-linked software library,
- libps_fips.hash - the configuration file containing the module integrity code.

The Tested Operational Environment's Physical Perimeter (TOEPP) of the cryptographic module is defined by the physical host device on which the module is installed. The module supports Process Algorithm Acceleration (PAA) from the host device. Therefore, PAA is a component within the cryptographic module boundary. The block diagram below (Figure 1) depicts these physical and cryptographic boundaries in relation to the module and physical components.

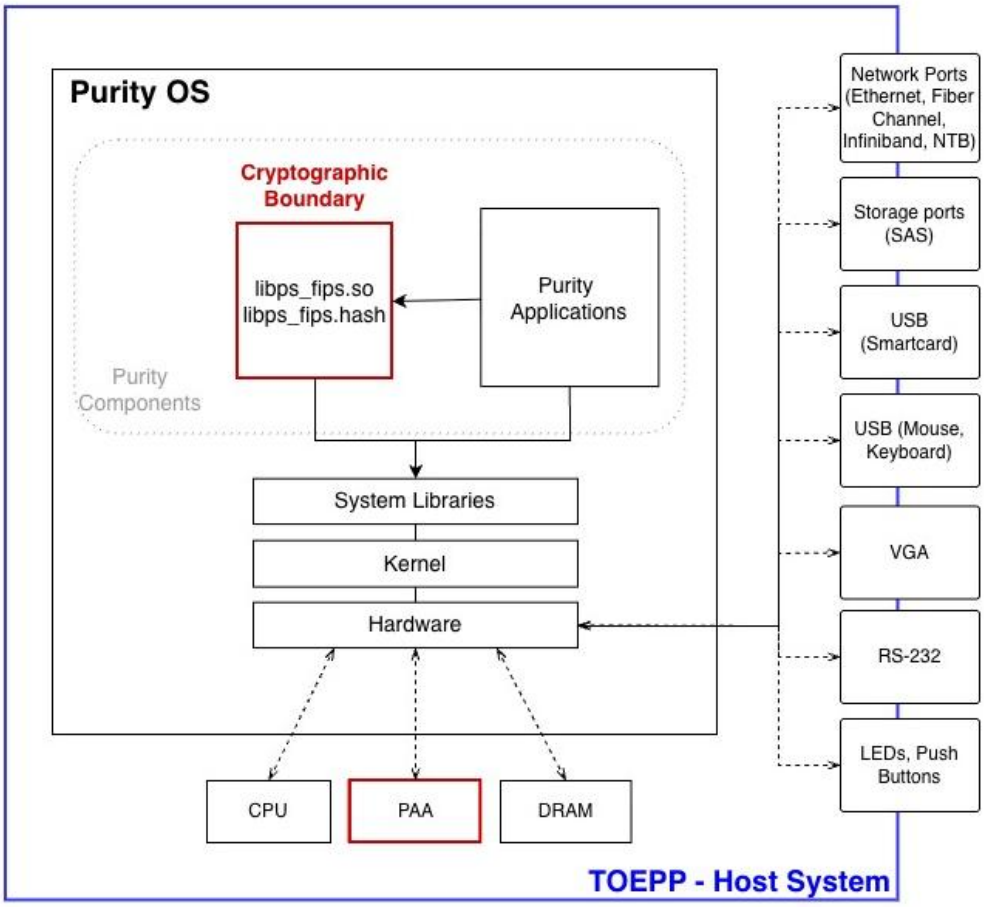

Figure 1: Block Diagram

2.2 Tested and Vendor Affirmed Module Version and Identification

Tested Module Identification – Software, Firmware, Hybrid (Executable Code Sets):

The cryptographic module is defined as a software module. The validated module name is "Purity Encryption Module", and the current version is output by the module as "FA-2.0".

Package or File Name	Software/ Firmware Version	Features	Integrity Test
libps_fips.so, libps_fips.hash	FA-2.0		Yes

Table 2: Tested Module Identification – Software, Firmware, Hybrid (Executable Code Sets)

Tested Operational Environments - Software, Firmware, Hybrid:

The table lists the operational environments the module was tested on.

Operating System	Hardware Platform	Processors	PAA/PAI	Hypervisor or Host OS	Version(s)
Purity OS 6.10	FlashArray X90R3	Intel Xeon Gold 6252	Yes		FA-2.0
Purity OS 6.10	FlashArray X90R3	Intel Xeon Gold 6252	No		FA-2.0
Purity OS 6.10	FlashArray XL170R5	Intel Xeon PLATINUM 8568Y+	Yes		FA-2.0
Purity OS 6.10	FlashArray XL170R5	Intel Xeon PLATINUM 8568Y+	No		FA-2.0

Table 3: Tested Operational Environments - Software, Firmware, Hybrid

Vendor-Affirmed Operational Environments - Software, Firmware, Hybrid:

The table lists the operational environments that the vendor affirms can be used by the module.

Operating System	Hardware Platform
Purity OS 6.9	FlashArray X20 R4 with Intel® Xeon® Silver 4410Y
Purity OS 6.9	FlashArray X50 R4 with Intel® Xeon® Silver 4410Y
Purity OS 6.9	FlashArray X70 R4 with Intel® Xeon® Gold 5416S
Purity OS 6.9	FlashArray X90 R4 with Intel® Xeon® Gold 5418N
Purity OS 6.9	FlashArray C20 R4 with Intel® Xeon® Silver 4410Y
Purity OS 6.9	FlashArray C50 R4 with Intel® Xeon® Silver 4410Y
Purity OS 6.9	FlashArray C70 R4 with Intel® Xeon® Gold 5416S
Purity OS 6.9	FlashArray C90 R4 with Intel® Xeon® Gold 5418N
Purity OS 6.9	FlashArray C10 R3 with Intel® Xeon® Silver 4208
Purity OS 6.9	FlashArray X20 R3 with Intel® Xeon® Silver 4210R
Purity OS 6.9	FlashArray X50 R3 with Intel® Xeon® Silver 4214Y
Purity OS 6.9	FlashArray X70 R3 with Intel® Xeon® Silver 6230
Purity OS 6.9	FlashArray X90 R3 with Intel® Xeon® Silver 6252
Purity OS 6.9	FlashArray C60 R3 with Intel® Xeon® Gold 6230
Purity OS 6.9	FlashArray C40 R3 with Intel® Xeon® Silver 4210R
Purity OS 6.9	FlashArray XL130 with Intel® Xeon® Gold 6338
Purity OS 6.9	FlashArray XL170 with Intel® Xeon® Platinum 8368
Purity OS 6.9	FlashArray XL130 R5 with Intel® Xeon® Gold 6554S
Purity OS 6.9	FlashArray XL170 R5 with Intel® Xeon® Platinum 8568Y+

Operating System	Hardware Platform
Purity OS 6.9	FlashArray X20 R5 with Intel® Xeon® Silver 4514Y
Purity OS 6.9	FlashArray X50 R5 with Intel® Xeon® Silver 4514Y
Purity OS 6.9	FlashArray X70 R5 with Intel® Xeon® Silver 4516Y+
Purity OS 6.9	FlashArray X90 R5 with Intel® Xeon® Gold 5520+
Purity OS 6.9	FlashArray C50 R5 with Intel® Xeon® Silver 4514Y
Purity OS 6.9	FlashArray C70 R5 with Intel® Xeon® Silver 4516Y
Purity OS 6.9	FlashArray C90 R5 with Intel® Xeon® Gold 5520+
Purity OS 6.10	FlashArray X20 R4 with Intel® Xeon® Silver 4410Y
Purity OS 6.10	FlashArray X50 R4 with Intel® Xeon® Silver 4410Y
Purity OS 6.10	FlashArray X70 R4 with Intel® Xeon® Gold 5416S
Purity OS 6.10	FlashArray X90 R4 with Intel® Xeon® Gold 5418N
Purity OS 6.10	FlashArray C20 R4 with Intel® Xeon® Silver 4410Y
Purity OS 6.10	FlashArray C50 R4 with Intel® Xeon® Silver 4410Y
Purity OS 6.10	FlashArray C70 R4 with Intel® Xeon® Gold 5416S
Purity OS 6.10	FlashArray C90 R4 with Intel® Xeon® Gold 5418N
Purity OS 6.10	FlashArray C10 R3 with Intel® Xeon® Silver 4208
Purity OS 6.10	FlashArray X20 R3 with Intel® Xeon® Silver 4210R
Purity OS 6.10	FlashArray X50 R3 with Intel® Xeon® Silver 4214Y
Purity OS 6.10	FlashArray X70 R3 with Intel® Xeon® Silver 6230
Purity OS 6.10	FlashArray X90 R3 with Intel® Xeon® Silver 6252
Purity OS 6.10	FlashArray C60 R3 with Intel® Xeon® Gold 6230
Purity OS 6.10	FlashArray C40 R3 with Intel® Xeon® Silver 4210R
Purity OS 6.10	FlashArray XL130 with Intel® Xeon® Gold 6338
Purity OS 6.10	FlashArray XL170 with Intel® Xeon® Platinum 8368
Purity OS 6.10	FlashArray XL130 R5 with Intel® Xeon® Gold 6554S
Purity OS 6.10	FlashArray XL170 R5 with Intel® Xeon® Platinum 8568Y+
Purity OS 6.10	FlashArray X20 R5 with Intel® Xeon® Silver 4514Y
Purity OS 6.10	FlashArray X50 R5 with Intel® Xeon® Silver 4514Y
Purity OS 6.10	FlashArray X70 R5 with Intel® Xeon® Silver 4516Y+
Purity OS 6.10	FlashArray X90 R5 with Intel® Xeon® Gold 5520+
Purity OS 6.10	FlashArray C50 R5 with Intel® Xeon® Silver 4514Y
Purity OS 6.10	FlashArray C70 R5 with Intel® Xeon® Silver 4516Y
Purity OS 6.10	FlashArray C90 R5 with Intel® Xeon® Gold 5520+

Table 4: Vendor-Affirmed Operational Environments - Software, Firmware, Hybrid

CMVP makes no statement as to the correct operation of the module or the security strengths of the generated keys when so ported if the specific operational environment is not listed on the validation certificate.

2.3 Excluded Components

The module does not contain any excluded components.

2.4 Modes of Operation

Mode Name	Description	Type	Status Indicator
Approved Mode	The Approved mode is enabled upon successful start-up of the module.	Approved	Module is operational

Table 5: Modes List and Description

The module does not support a non-approved mode of operation, nor a degraded mode of operation.

There are no specific initialization steps required for start-up of the module beyond powering on the Flash Array product.

2.5 Algorithms

Approved Algorithms:

Algorithm	CAVP Cert	Properties	Reference
AES-CTR	A7671	Direction - Decrypt, Encrypt Key Length - 128, 256	SP 800-38A
AES-KW	A7671	Direction - Decrypt, Encrypt Key Length - 128, 256	SP 800-38F
Counter DRBG	A7671	Prediction Resistance - Yes Mode - AES-256 Derivation Function Enabled - Yes	SP 800-90A Rev. 1
HMAC-SHA2-256	A7671	Key Length - Key Length: 512-2048 Increment 512	FIPS 198-1
SHA2-256	A7671	Message Length - Message Length: 0-51200 Increment 8	FIPS 180-4

Table 6: Approved Algorithms

Vendor-Affirmed Algorithms:

N/A for this module.

Non-Approved, Allowed Algorithms:

N/A for this module.

Non-Approved, Allowed Algorithms with No Security Claimed:

The table contains the non-approved algorithms allowed in approved mode of operation with no security claimed.

N/A for this module.

Non-Approved, Not Allowed Algorithms:

The module does not support any non-approved, not allowed algorithms.

N/A for this module.

2.6 Security Function Implementations

Name	Type	Description	Properties	Algorithms
AES for Symmetric Encryption	BC-UnAuthEncrypt	The AES key is used for the symmetric encryption of data	Standard:SP 800-38A	AES-CTR: (A7671)
AES for Symmetric Decryption	BC-UnAuthDecrypt	The AES key is used for the symmetric decryption of data	Standard:SP 800-38A	AES-CTR: (A7671)
AES for Key Wrapping	BC-AuthEncrypt	The AES key is used for Key Wrapping	Standard:SP 800-38F	AES-CTR: (A7671) AES-KW: (A7671)
AES for Key Unwrapping	BC-AuthDecrypt	The AES key is used for Key Unwrapping	Standard:SP 800-38F	AES-CTR: (A7671) AES-KW: (A7671)
DRBG	DRBG	Random Number Generation	Standard:SP 800-90A Rev1	Counter DRBG: (A7671)
Keyed Hash Verification	MAC	Keyed Hash Verification	Standard:FIPS 198-1	HMAC-SHA2-256: (A7671)
Message Digest	SHA	Message Digest	Standard:FIPS 180-4	SHA2-256: (A7671)

Table 7: Security Function Implementations

2.7 Algorithm Specific Information

The module does not establish SSPs using an approved key transport scheme (KTS). However, it does offer approved authenticated algorithms that can be used by an external operator/application as part of an approved KTS.

2.8 RBG and Entropy

The module implements an Approved DRBG algorithm for the purpose of supplying random bytes to the calling application via the module's random byte generation service. This DRBG is used for this service only and is not used by the module for any other purpose. The module implements CTR-DRBG with security strength of 256 bits.

The DRBG receives entropy input passively from an entropy source configured by the calling application via a callback function. The calling application and its entropy sources are external to the module's cryptographic boundary. The DRBG loads 256-bits of entropy input (plus 128-bits of nonce) from the configured entropy source during DRBG instantiation. It is a requirement of the FlashArray product that the entropy source configured for the module provides full entropy.

The module claims the entropy caveat "*No assurance of the minimum strength of generated SSPs (e.g., keys)*."

2.9 Key Generation

The module does not generate SSPs.

2.10 Key Establishment

The module does not establish SSPs.

2.11 Industry Protocols

The module does not implement any industry protocols.

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

As a software-only module, the module does not have physical ports. For the FIPS 140-3 validation, the physical ports are interpreted to be the physical ports of the hardware platform on which it runs.

The module supports four logical interfaces: Data Input, Data Output, Control Input and Status Output. It does not support a Control Output interface. The table below defines the logical interfaces.

Physical Port	Logical Interface(s)	Data That Passes
N/A	Data Input	The data read from memory area(s) provided to the invoked API functions via input parameters that point to the memory area(s), including plaintext, ciphertext, key data, checksums.
N/A	Data Output	The data written to memory area(s) provided to the invoked API functions via output parameters that point to the memory area(s), including plaintext, ciphertext, checksums.
N/A	Control Input	The API function invoked, and API function parameters designated as control inputs.
N/A	Control Output	N/A
N/A	Status Output	The return value of the invoked API functions; Console log messages.

Table 8: Ports and Interfaces

4 Roles, Services, and Authentication

4.1 Authentication Methods

Authentication mechanisms are not applicable for this module.

4.2 Roles

Name	Type	Operator Type	Authentication Methods
Cryptographic Officer	Role	CO	None

Table 9: Roles

The module supports the Crypto Officer role, which is assumed implicitly by the operator of the module (the calling application) for all module services. No authentication mechanisms are provided to assume the role of Crypto Officer. The module does not support concurrent operators and does not authenticate the Crypto Officer role. Furthermore, it does not support a maintenance role and/or bypass capability.

4.3 Approved Services

The table below lists the services that can be used in the approved mode of operation with corresponding input and output. The abbreviations of the access rights to keys and SSPs have the following interpretation.

G = Generate: The module generates or derives the SSP.
R = Read: The SSP is read from the module (e.g., the SSP is output).
W = Write: The SSP is updated, imported, or written to the module.
E = Execute: The module uses the SSP in performing a cryptographic operation.
Z = Zeroize: The module zeroizes the SSP.
N/A= The service does not access any SSP during its operation

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
AES Encrypt	Perform AES encryption	Success/Failure	Key, IV, Plaintext, optional checksum	Ciphertext, optional checksum, optional RAID-6 parity shards	AES for Symmetric Encryption	Cryptographic Officer - AES Key: W,E
AES decrypt	Perform AES decryption	Success/Failure	Key, IV, Ciphertext, optional checksum	Plaintext, optional checksum	AES for Symmetric Decryption	Cryptographic Officer - AES Key: W,E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
AES key wrap	Perform AES key wrap	Success/Failure	Wrapping key, plaintext key	Wrapped key	AES for Key Wrapping	Cryptographic Officer - AES Key Wrapping Key: W,E - AES Key: W,E
AES key unwrap	Perform AES key unwrap	Success/Failure	Wrapping key, wrapped key	Plaintext key	AES for Key Unwrapping	Cryptographic Officer - AES Key Wrapping Key: W,E - AES Key: W,E
Random Byte Generation	Generate random bytes from the module DRBG	Success/Failure	Entropy source callback, DRBG input parameters	Random bytes	DRBG	Cryptographic Officer - DRBG Entropy Input: G,E,Z - DRBG Seed: G,E,Z - DRBG 'V' value: G,E,Z - DRBG 'Key' value: G,E,Z
Perform self-tests	On-demand self tests via power-cycling the host device.	N/A	Manual power cycle	Pass/fail	Keyed Hash Verification Message Digest	Cryptographic Officer
Zeroization	Zeroize/ destroy all CSPs via power off/cycle the host device.	N/A	Manual power cycle	None (completion indicator is implicitly provided by the module rebooting)	None	Cryptographic Officer - AES Key: Z - AES Key Wrapping Key: Z - DRBG Entropy Input: Z - DRBG Seed: Z - DRBG 'V' value: Z - DRBG 'Key' value: Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Show status	Return code for each API call	N/A	None	Return code	None	Cryptographic Officer
Show version	Display the version of the module	N/A	None	Name and version information	None	Cryptographic Officer

Table 10: Approved Services

4.4 Non-Approved Services

Non-approved services are not supported by this module.

4.5 External Software/Firmware Loaded

Software loading is not supported by this module.

5 Software/Firmware Security

5.1 Integrity Techniques

The module is a single, shared object, binary component that is in an Executable and Linkable Format (ELF). A software integrity test is performed on this component using HMAC-SHA2-256. This algorithm is implemented in the module. If the integrity test fails, the module enters an error state and the module becomes inoperable.

5.2 Initiate on Demand

Integrity tests are performed as part of the Pre-Operational Self-Tests, which are executed on load of the module shared library. Pre-operational self-tests can be initiated on demand by powering-off and reloading the module.

6 Operational Environment

6.1 Operational Environment Type and Requirements

Type of Operational Environment: Modifiable

The module is designated as a Modifiable operational environment under the FIPS 140-3 definitions. The operational environment is the Purity OS 6.10 for FlashArray. The operational environment implicitly enforces a single mode of operation by managing process memory of the module and ensuring each calling process is logically separated and protected.

No rules, settings or restrictions to the operational environment apply for operation of the module.

7 Physical Security

As a software module, the FIPS 140-3 physical security requirements do not apply to the Purity Encryption Module.

8 Non-Invasive Security

There are currently no non-invasive security requirements that apply to FIPS 140-3 modules.

9 Sensitive Security Parameters Management

9.1 Storage Areas

Storage Area Name	Description	Persistence Type
RAM	Random Access Memory	Dynamic

Table 11: Storage Areas

The CPU interacts with dynamic RAM where the executable code, API input and output parameters are maintained (see Figure 1).

9.2 SSP Input-Output Methods

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
API input parameters	Calling application (External)	RAM	Plaintext	Manual	Electronic	
API output parameters	RAM	Calling application (External)	Encrypted	Manual	Direct	AES-KW (A7671)

Table 12: SSP Input-Output Methods

9.3 SSP Zeroization Methods

Zeroization Method	Description	Rationale	Operator Initiation
Power off/cycle	Zeroization of SSPs in RAM via invocation of manual power off/cycle	RAM is volatile and all data is lost when power is taken off. Zeroization is practically instantaneous.	Via invocation of manual power off/cycle

Table 13: SSP Zeroization Methods

9.4 SSPs

The Sensitive Security Parameters (SSPs) that are used by cryptographic services implemented in the module are:

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
AES Key	Symmetric Encryption and Decryption	128 and 256 bits - 128 and 256 bits	Symmetric Key - CSP			AES for Symmetric Encryption AES for Symmetric Decryption
AES Key Wrapping Key	Key Transport	128 and 256 bits - 128 and 256 bits	Symmetric Key - CSP			AES for Key Wrapping AES for Key Unwrapping
DRBG Entropy Input	DRBG entropy material	256 - 256	Entropy source output - CSP			DRBG
DRBG Seed	DRBG state value	256 - 256	DRBG internal state - CSP	DRBG		DRBG
DRBG 'V' value	DRBG state value	256 - 256	DRBG internal state - CSP	DRBG		DRBG
DRBG 'Key' value	DRBG state value	256 - 256	DRBG internal state - CSP	DRBG		DRBG

Table 14: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
AES Key	API input parameters API output parameters	RAM:Plaintext	Until power off/cycle	Power off/cycle	
AES Key Wrapping Key	API input parameters	RAM:Plaintext	Until power off/cycle	Power off/cycle	
DRBG Entropy Input	API input parameters	RAM:Plaintext	Until power off/cycle	Power off/cycle	
DRBG Seed		RAM:Plaintext	Until power off/cycle	Power off/cycle	
DRBG 'V' value		RAM:Plaintext	Until power off/cycle	Power off/cycle	
DRBG 'Key' value		RAM:Plaintext	Until power off/cycle	Power off/cycle	

Table 15: SSP Table 2

10 Self-Tests

All self-tests are executed automatically when the module is loaded into memory before the module transitions to the operational state. The services of the module are not available prior to the completion of the self-tests. If any tests fail, the module reports an error message indicating the failure and enters the Error State. Successful completion of self-tests is indicated by a status message and passing control to the calling application.

The module permits operators to initiate all self-tests on demand by power-cycling the system.

10.1 Pre-Operational Self-Tests

The module performs pre-operational self-tests as specified in the table below.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
HMAC-SHA2-256 (A7671)	HMAC-SHA2-256	KAT	SW/FW Integrity	PASS/FAIL console output	

Table 16: Pre-Operational Self-Tests

10.2 Conditional Self-Tests

The module performs conditional self-tests as specified in the table below.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-CTR Encrypt	Key Sizes: 128, 256	KAT	CAST	PASS/FAIL console output	Encrypt	On power-up
AES-CTR Decrypt	Key Sizes: 128, 256	KAT	CAST	PASS/FAIL console output	Decrypt	On power-up
AES-KW Wrap	Key Sizes: 128, 256	KAT	CAST	PASS/FAIL console output	Encrypt	On power-up
AES-KW Unwrap	Key Sizes: 128, 256	KAT	CAST	PASS/FAIL console output	Decrypt	On power-up
Counter DRBG	256 bits	KAT	CAST	PASS/FAIL console output	Instantiate, Reseed, Generate	On power-up
HMAC-SHA2-256	Key size: 256 bits, = 256	KAT	CAST	PASS/FAIL console output	Verify	On power-up
SHA2-256	n/a	KAT	CAST	PASS/FAIL console output	Hash	On power-up

Table 17: Conditional Self-Tests

10.3 Periodic Self-Test Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
HMAC-SHA2-256 (A7671)	KAT	SW/FW Integrity	On demand	Manually

Table 18: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-CTR Encrypt	KAT	CAST	On demand	Manually
AES-CTR Decrypt	KAT	CAST	On demand	Manually
AES-KW Wrap	KAT	CAST	On demand	Manually
AES-KW Unwrap	KAT	CAST	On demand	Manually
Counter DRBG	KAT	CAST	On demand	Manually
HMAC-SHA2-256	KAT	CAST	On demand	Manually
SHA2-256	KAT	CAST	On demand	Manually

Table 19: Conditional Periodic Information

10.4 Error States

The module has a single Error State, as described in the table below.

Name	Description	Conditions	Recovery Method	Indicator
Error State	The module reports an error message indicating the failure and enters the Error State. No services are available in this state.	On any pre-operational or conditional self-test failure	Power cycle	Error log message

Table 20: Error States

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

The module is built into Purity OS, which comes pre-installed on target FlashArray products. There is no standalone delivery of the module as a software library.

The vendor's internal development process guarantees that the correct version of module is distributed with the intended device.

No specific initialization steps are required for start-up of the module beyond powering on the FlashArray product.

The module does not have any specific maintenance requirements.

11.2 Administrator Guidance

There is only one Approved mode of operation. Crypto Officer role guidance is provided by the API documentation provided by the module's header files.

Zeroization (via power-cycling the host system) must be performed under the control of the operator.

11.3 Non-Administrator Guidance

As the module does not support non-administrator users, non-administrator guidance is not applicable.

12 Mitigation of Other Attacks

The module does not claim mitigation of other attacks.