Phison Electronics Corp

Phison TCG OPAL SSC SSD Series
FIPS 140-2 Non-Proprietary
SECURITY POLICY

Document Revision: V1.01

REVISION HISTORY

Author(s)	Version	Updates
Rice Fan	V1.00	Initial Release
Rice Fan	V1.01	Add Firmware ECPM13.1 Add CAVP certificate for PBKDF Update Exhibit 22

PHISON Knows What You Need

Table of Contents

1 INTRODUCTION 3

2 CRYPTOGRAPHIC BOUNDARY 8

3 ACRONYMS 8

4 SECURITY LEVEL SPECIFICATION 9

5 PHYSICAL PORTS AND LOGICAL INTERFACES 10

6 SECURITY RULES 10

6.1 NON-APPROVED MODE OF OPERATION 10

6.2 SECURITY INITIALIZATION 12

6.3 FIPS-APPROVED MODE OF OPERATION 14

6.4 CRYPTOGRAPHIC OFFICER GUIDANCE 15

6.5 USER GUIDANCE 15

6.6 SELF TESTS 15

6.6.1 POWER UP SELF TESTS 16

6.6.2 CONDITIONAL SELF TESTS 18

7 CRITICAL SECURITY PARAMETERS, PUBLIC KEYS, AND PRIVATE KEYS 19

8 IDENTIFICATION AND AUTHENTICATION POLICY 22

9 ACCESS CONTROL POLICY 25

9.1 AUTHENTICATED SERVICES 25

9.2 UNAUTHENTICATED SERVICE 27

10 APPROVED ALGORITHMS 29

11 PHYSICAL SECURITY POLICY 34

12 MITIGATION OF OTHER ATTACKS POLICY 34

1 INTRODUCTION

Phison TCG OPAL SSC SSD series, hereafter referred to as “Phison SSDs” or the “cryptographic modules” are multi-chip embedded cryptographic modules designed to fulfill FIPS 140-2 level 2 requirements and offer on-the-fly AES encryption and decryption of user data stored on the NAND Flash. Phison SSDs offer both NVMe PCIe as well as SATA III interfaces and are fully compliant with industry standard TCG OPAL SSC protocol.

MODULE	CAPACITY	HW P/N AND VERSION	FW VERSION
PS3112-S12 2.5-INCH SATA NAND FLASH SSD	128GB	PSS12F-2.5-128G-V01	SCPM13.0
	256GB	PSS12F-2.5-256G-V01	SCPM13.0
	512GB	PSS12F-2.5-512G-V01	SCPM13.0
	1024GB	PSS12F-2.5-1024G-V01	SCPM13.0
	2048GB	PSS12F-2.5-2048G-V01	SCPM13.0
PS3112-S12 M.2 2280 SATA NAND FLASH SSD (D3)	128GB	PSS12F-M.2280D3-128G-V01	SCPM13.0
	256GB	PSS12F-M.2280D3-256G-V01	SCPM13.0
	512GB	PSS12F-M.2280D3-512G-V01	SCPM13.0
	1024GB	PSS12F-M.2280D3-1024G-V01	SCPM13.0
	2048GB	PSS12F-M.2280D3-2048G-V01	SCPM13.0
PS3112-S12 M.2 2280 SATA NAND FLASH SSD (S3)	128GB	PSS12F-M.2280S3-128G-V01	SCPM13.0
	256GB	PSS12F-M.2280S3-256G-V01	SCPM13.0
	512GB	PSS12F-M.2280S3-512G-V01	SCPM13.0
PS3112-S12 M.2 2242 SATA NAND FLASH SSD	128GB	PSS12F-M.2242-128G-V01	SCQM12.0
	256GB	PSS12F-M.2242-256G-V01	SCQM12.0
PS5012-E12 M.2 2280 NVME NAND FLASH SSD	256GB	PSE12F-M2280-256G-V01	ECPM13.0 ECPM13.1
	512GB	PSE12F-M2280-512G-V01	ECPM13.0 ECPM13.1
	1024GB	PSE12F-M2280-1024G-V01	ECPM13.0 ECPM13.1
	2048GB	PSE12F-M2280-2048G-V01	ECPM13.0 ECPM13.1

Exhibit 1– *Cryptographic Module Configurations*

Exhibit 2- *Specification of the PS3112-S12 2.5-INCH SATA NAND FLASH SSD Series Cryptographic Boundary (From left to right: top side, bottom side).*

Exhibit 3 - *Specification of the PS3112-S12 M.2 2280 SATA NAND FLASH SSD (D3) Series Cryptographic Boundary (From top to bottom: top side, bottom side).*

Exhibit 4 - *Specification of the PS3112-S12 M.2 2280 SATA NAND FLASH SSD (S3) Series Cryptographic Boundary (From top to bottom: top side, bottom side).*

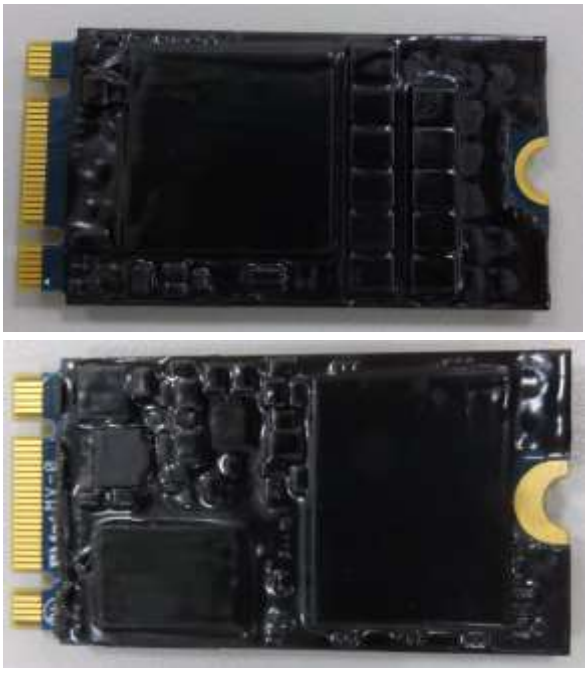

Exhibit 5 - *Specification of the PS3112-S12 M.2 2242 SATA NAND FLASH SSD Series Cryptographic Boundary (From top to bottom: top side, bottom side).*

Exhibit 6 - *Specification of the PS5012-E12 M.2 2280 NVMe NAND FLASH SSD Series Cryptographic Boundary (From top to bottom: top side, bottom side).*

2 CRYPTOGRAPHIC BOUNDARY

The cryptographic boundary of the modules is the physical perimeter of the PCB including the physical connector (SATA/NVMe). The following diagram defines the cryptographic boundary as Exhibit 7.

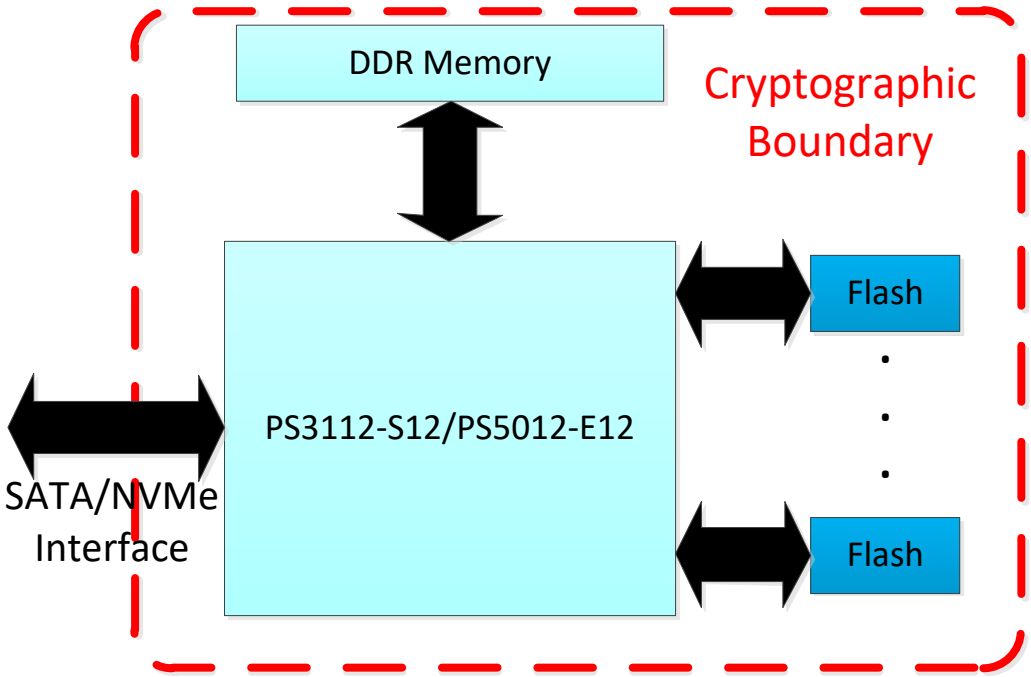

Exhibit 7- *Specification of Cryptographic Boundary*

3 ACRONYMS

TERM	DESCRIPTION
AES	Advanced Encryption Standard
CBC	Cipher Block Chaining
CMVP	Cryptographic Module Validation Program
CO	Cryptographic Officer
CSP	Critical Security Parameter
DRBG	Deterministic Random Bit Generator
EMI/EMC	Electromagnetic Interference / Electromagnetic Compatibility
HMAC	(Keyed-) Hash Message Authentication Code
KAT	Known Answer Test

TERM	DESCRIPTION
KEK	Key Encryption Key
NDRNG	Non-Deterministic Random Number Generator
MEK	Media Encryption Key
RSA	Rivest, Shamir, and Adleman
SHA	Secure Hash Algorithm

Exhibit 8 – *Specification of Acronyms and their Descriptions*

4 SECURITY LEVEL SPECIFICATION

This document was prepared as part of the Level 2 FIPS 140-2 validation of the module. The following table lists the module's FIPS 140-2 security level for each section as Exhibit 9.

SECURITY REQUIREMENTS AREA	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	3
Self-tests	2
Design Assurance	2
Mitigation of Other Attacks	N/A

Exhibit 9 – *Security Level Table.*

5 PHYSICAL PORTS AND LOGICAL INTERFACES

The ports and interfaces of the cryptographic module are as follows:

- SATA/NVMe Connector

The following ports are disabled during the manufacturing process and physically protected by the module's physical security mechanisms. Therefore, they are considered latent-functionality and not available when operating in FIPS mode or non-FIPS mode:

- JTAG
- UART

Exhibit 10 shows how the module's physical interfaces map to the logical interfaces defined in FIPS 140-2.

PHYSICAL PORT	LOGICAL INTERFACE
SATA/NVMe Connector	Data Input
SATA/NVMe Connector	Control Input
SATA/NVMe Connector	Data Output
SATA/NVMe Connector	Status Output
SATA/NVMe Connector	Power

Exhibit 10 - *Specification of Cryptographic Module Physical Ports and Logical Interfaces*

6 SECURITY RULES

6.1 NON-APPROVED MODE OF OPERATION

The moment the module is shipped from the factory, in this fresh out-of-box state the module is in a non-approved mode of operation. The Cryptographic Officer shall follow the requirements defined in the Security Policy including following the initialization procedures in section 6.2 to initialize the module into a FIPS Approved mode of operation

In the non-approved mode of operation, the module supports the following services and algorithms:

ROLE	SERVICE	ALGORITHMS
Unauthenticated Role	Power Cycle	N/A
Unauthenticated Role	Generate Random Number	DRBG (non-compliant)
Unauthenticated Role	Show Status	N/A
Anybody	TCG Get MBR	N/A
Unauthenticated Role	Reset	N/A
Unauthenticated Role	Return to uninitialized state(PSID)	DRBG (non-compliant) AES-XTS (non-compliant) AES-KW (non-compliant)
Unauthenticated Role	Show FIPS approve mode state	N/A
Anybody	TCG Get MSID	N/A
Anybody	TCG Session Control	HMAC (non-compliant) SHA (non-compliant) PBKDF (non-compliant)
Unauthenticated Role	SATA Standard	N/A
Unauthenticated Role	NVMe Standard	N/A
Unauthenticated Role	User Data Read/Write	AES-XTS (non-compliant)
Unauthenticated Role	TCG Session Control	N/A
Unauthenticated Role	Non User Data Output	N/A
Unauthenticated Role	Non User Data Input	N/A
Unauthenticated Role	Configuration	N/A
Unauthenticated Role	Self-Test	N/A
Unauthenticated Role	Show Status(DAS)	N/A
Cryptographic Officer (Drive Owner)	TCG Activate	AES-KW (non-compliant)
Cryptographic Officer, User	TCG Set PIN	SHA (non-compliant)
Cryptographic Officer, User	TCG Gen Key	DRBG (non-compliant)
Cryptographic Officer	TCG Enable/Disable Authority	N/A
Cryptographic Officer	TCG Set/Get LBA Range	N/A
Cryptographic Officer, User	TCG Lock / Unlock LBA Range	AES-XTS (non-compliant) AES-KW (non-compliant)

ROLE	SERVICE	ALGORITHMS
Cryptographic Officer	Return to uninitialized state	DRBG (non-compliant) AES-XTS (non-compliant) AES-KW (non-compliant)
Cryptographic Officer	TCG Set MBR	N/A
Cryptographic Officer	TCG SET/GET DataStore	N/A
Cryptographic Officer	TCG SET ACE	N/A
Cryptographic Officer	TCG Enable/Disable MBR Mode	N/A

Exhibit 11 – *Non-Approved Mode Services*

NOTE:
Unauthenticated Role is a role who is eligible for making use of non-TCG OPAL commands.
Anybody is a role who is able to use the TCG OPAL command based services (as listed in Exhibit 11) without password.

6.2 SECURITY INITIALIZATION

Cryptographic Officer (Drive Owner) needs to follow these steps to initialize the cryptographic module into FIPS approved mode after having received the Phison SSD drive.

1. Examine the tamper evidence and check the module has not been tampered.
2. StartSession SID of AdminSP with MSID password, and then set new password for SID password. The new password shall be at least 20 bytes.
3. Disable AdminSP “Makers” Authority.
4. Execute TCG activate command to have the module enter TCG active mode.
5. StartSession Admin1 of LockingSP with new password of SID in Step2, and then set new password for Admin1-4 passwords and User1-9 passwords of LockingSP. The new passwords shall be at least 20 bytes.
6. Configure all LockingRanges of LockinSP by setting ReadLockEnabled and WriteLockEnabled columns to TRUE.
7. Power cycle the module.

8. Check if the module is in the FIPS approved mode by using the Identify command response data byte 506 bit1 (SATA) or the Identify controller command response data byte 4093 bit1 (NVMe). The bit1 shall be set to 1.
9. Check the module's firmware version using the Identify command response data dword 23-26 (SATA) or the Identify controller command response data byte 64-71 (NVME). The firmware version shall be an approved version as per Exhibit 1 above.

   NOTE: 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 that is not reflected in Exhibit 1 above is out of the scope of this validation and requires a separate FIPS 140-2 validation.

After following these steps the drive is in the FIPS approved mode of operation.

6.3 FIPS-APPROVED MODE OF OPERATION

Once the Cryptographic Officer has followed the initialization procedures in section 6.2, the module is in a FIPS-approved mode of operation. Any violation of section 6.2 or other requirements specified in the Security Policy will place this module in a non-approved mode of operation.

In the FIPS-approved mode of operation the module shall adhere to the following rules:

1. Operators shall not use passwords less than 20 bytes.
2. The module generates at a minimum 256 bits of entropy for use in key generation.
3. The cryptographic module satisfies the requirements of FIPS 140-2 IG A.9 (ex:. key_1 ≠ key_2).
4. The cryptographic module shall not output CSPs in any form.
5. The cryptographic module enters the FIPS Error State upon failure of self-tests and the module ceases to provide cryptographic services and inhibits all data outputs.
6. The approved DRBG shall be used for generating cryptographic keys.
7. The cryptographic module shall enforce role-based authentication for security relevant services.
8. The cryptographic module shall enforce a limited operational environment by the secure firmware load test using RSA-2048 with SHA-256.
9. An operator can invoke on demand power-on self tests by power cycling the module.
10. Data output interface is inhibited when module is performing self-test and when the module is in an Error State.
11. Data output interface is logically disconnected when module is performing key generation or zeroization processes.
12. Caveat: The module generates cryptographic keys whose strengths are modified by available entropy

6.4 CRYPTOGRAPHIC OFFICER GUIDANCE

1. Periodically examine tamper evidence, if evidence of tamper has been detected then the device must be put out of service and the Cryptographic Officer (Drive Owner) shall be notified.
2. When first executing StartSession with the password provided by Cryptographic Officer (Drive Owner), the Cryptographic Officer (CO) needs to change to a new password for the CO himself and the password must contain at least 20 bytes.

6.5 USER GUIDANCE

1. When first executing StartSession with the password which was provided by CO, user needs to change to a new user password and the password must contain at least 20 bytes.

6.6 SELF TESTS

When self tests fail, module either enters the Boot Code Fail Loop State or the FIPS error state in which it ceases to provide any services to the host and where the error can only be cleared by power-cycling of the module.

FIPS Error State: When module enters FIPS Error State, the module can't service any host commands and the DAS signal pin will toggle at a 1Hz frequency. (The DAS signal default is high.)

Boot Code Fail Loop State: When module enters Boot Code Fail Loop State, the module is not accessible by the host. This is an implicit status as no service nor command input will be processed and the data output and status output interfaces are inhibited.

Note: For different form factor, the assigned DAS PIN number is:
PS3112-S12 2.5-Inch SATA NAND Flash SSD (PIN#18)
PS3112-S12 M.2 2280 SATA NAND Flash SSD (D3) (PIN#10)
PS3112-S12 M.2 2280 SATA NAND Flash SSD (S3) (PIN#10)
PS3112-S12 M.2 2242 SATA NAND Flash SSD (PIN#10)
PS5012-E12 M.2 2280 NVMe NAND Flash SSD (PIN#10)

6.6.1 POWER UP SELF TESTS

Function	Description	Failure Handle
Rom Code SHA 256 bit	KAT Mode : SHA-256	Boot Code Fail Loop State
Rom Code RSA 2048 bit	KAT Mode : RSA 2048 SHA-256 PSS Signature Verification	Boot Code Fail Loop State
Boot Loader Integrity	Firmware Integrity Test Mode : RSA 2048 SHA-256 PSS Signature Verification	Boot Code Fail Loop State
Firmware Integrity	Firmware Integrity Test Mode : RSA 2048 SHA-256 PSS Signature Verification	FIPS Error State
Firmware AES XTS 256 bit Encrypt	KAT Mode : AES-XTS-256	FIPS Error State
Firmware AES XTS 256 bit Decrypt	KAT Mode : AES-XTS-256	FIPS Error State
Firmware SHA 256 bit	KAT Mode : SHA-256	FIPS Error State
Firmware SHA 512 bit	KAT Mode : SHA-512	FIPS Error State
Firmware HMAC SHA 256 bit	KAT Mode : HMAC SHA-256	FIPS Error State

Function	Description	Failure Handle
Firmware AES Key Wrap	KAT Mode : AES-KW-256	FIPS Error State
Firmware AES Key Unwrap	KAT Mode : AES-KW-256	FIPS Error State
Firmware DRBG	KAT Mode : HMAC-SHA-256-DRBG	FIPS Error State
Firmware DRBG Health Tests	SP 800-90A Section 11.3 Health Tests Mode : HMAC-SHA-256-DRBG	FIPS Error State
Firmware AES CBC 256 bit Encrypt	KAT Mode : AES-CBC-256	FIPS Error State
Firmware AES CBC 256 bit Decrypt	KAT Mode : AES-CBC-256	FIPS Error State
Firmware SP 800-132 PBKDF	KAT Mode : HMAC-SHA-256	FIPS Error State

Exhibit 12 - *Power Up Self Tests*

6.6.2 CONDITIONAL SELF TESTS

Function	Description	Failure Handle
DRBG	Conditional: Continuous RNG test for DRBG	FIPS Error State
NDRNG	Conditional: Continuous RNG test for NDRNG	FIPS Error State
Firmware Download Check	Conditional: RSA 2048 SHA-256 PSS Signature Verification	Abort the Microcode Download command and discard the new image. FW will perform an additional RSA 2048 SHA-256 PSS KAT to attempt error recovery. If the KAT fails, module immediately enters the FIPS error state. If the KAT succeeds module is operational.

Exhibit 13 – *Conditional Self Tests*

7 CRITICAL SECURITY PARAMETERS, PUBLIC KEYS, AND PRIVATE KEYS

The module supports the following CSPs and Public Keys as defined in Exhibit 14 below.

CSP or Public Key	Type	Generation	Storage	Zeroization
Data Encryption Key (DEK)	AES-XTS-256	SP800-90A HMAC-SHA-256-DRBG	Encrypted by Key Encryption Key and stored in NAND Plaintext in DRAM and registers	Actively overwritten in all storage locations via "Return to uninitialized state" and "TCG Gen Key" services
User Key Encryption Key (UKEK)	AES-KW-256	SP800-90A HMAC-SHA256-DRBG	Encrypted by PBKDF Master Key with AES-KW-256 and stored in NAND Plaintext in DRAM and registers	Actively overwritten in all storage locations via "Return to uninitialized state" service
PBKDF Master Key	Keying Material for AES-KW-256	SP800-132 PBKDF	Plaintext in DRAM and registers	Actively overwritten in DRAM and registers after each use and by "Return to uninitialized state" service

CSP or Public Key	Type	Generation	Storage	Zeroization
Operator Password (Crypto Officer password/user password)	20 - 32 byte Password	N/A – Generated outside of the module	SHA-512 stored in NAND Plaintext in DRAM and registers	Plaintext values are actively overwritten when executing “TCG Session Control” service with End of Session command and “Return to uninitialized state” (CO)
PBKDF Internal State	SP800-132 PBKDF with HMAC-SHA-256	SP800-132 PBKDF with HMAC-SHA-256	Plaintext in DRAM and registers	Actively overwritten in DRAM and registers after each use and by “Return to uninitialized state” service
Seed Material of SP800-90A	Entropy Input and Nonce for SP800-90A HMAC-SHA-256-DRBG	NDRNG	Plaintext in DRAM and registers	Actively overwritten in DRAM and registers after each use and by “Return to uninitialized state” service

CSP or Public Key	Type	Generation	Storage	Zeroization
Internal State of SP800-90A	V and Key for SP800-90A HMAC-SHA-256-DRBG	SP800-90A HMAC-SHA-256-DRBG	Plaintext in DRAM and registers	Actively overwritten in DRAM and registers after each use and by "Return to uninitialized state" service
RSA Code Sign Public Key	RSA-2048	N/A – Generated outside of the module	Plaintext in DRAM and registers SHA-256 message digest value is stored in OTP-ROM	N/A

Exhibit 14- List of CSPs

Note: In accordance with FIPS 140-2 IG D.12, the cryptographic module performs Cryptographic Key Generation (CKG) as per SP 800-133 (Vendor Affirmed). The resulting generated symmetric keys are the unmodified output from SP 800-90A DRBG.

8 IDENTIFICATION AND AUTHENTICATION POLICY

ROLE	AUTHENTICATION TYPE	AUTHENTICATION DATA
Cryptographic Officer (Drive Owner)	Role Base	Password
Cryptographic Officer	Role Base	Password
User	Role Base	Password
Firmware Download Role	Identity Base	RSA-PSS-2048 with SHA-256
Unauthenticated Role	N/A	N/A
Anybody	N/A	N/A

Exhibit 15 – *Identification and Authentication Policy*

Note: To assume the “Anybody” role the operator needs to execute “TCG Session Control” service with a TCG StartSession command, supplying the Anybody UID and does not need a password. “Anybody” is a TCG authority who can only perform TCG methods which are unauthenticated services but still need to use the TCG StartSession command. Hence, this role is also considered as an unauthenticated role.

For reference here is a mapping between the applicable FIPS 140-2 Roles and the corresponding TCG Authorities:

ROLE	TCG Authority
Cryptographic Officer (Drive Owner)	SID
Cryptographic Officer	Admin1~Admin4
User	User1~User9
Anybody	Anybody

Exhibit 16 – *TCG Authority and Role Mapping*

Minimum password length for Cryptographic Officers and Users shall be 20 bytes with maximum password length supported being 32 bytes. Using the minimum password length, the probability of a single random attempt to succeed is $1/(2^{160})$ which is much less than FIPS 140-2 requirement of 1/1,000,000.

Each authentication attempt takes about 2ms to complete, so within one minute ((60*1000)/2) = 30,000 attempts can be conducted. The probability of multiple random attempts to succeed is $30,000/(2^{160})$ which is much less than FIPS 140-2 requirement of 1/100,000. Both single as well as multiple random attempt probabilities meet FIPS 140-2 requirement.

The authentication mechanism for Firmware Download Role is RSA-PSS-2048 with SHA-256 digital signature verification, which means a single random attempt, can succeed with the probability of $1/2^{112}$.

Each RSA signature verification attempt takes at least 50ms. So within one minute ((60*1000)/50) = 1200 attempts can be conducted. Therefore, the probability of multiple random attempts to succeed in one minute is $1200/2^{112}$, which is much less than the FIPS 140-2 requirement 1/100,000.

AUTHENTICATION MECHANISM	STRENGTH OF MECHANISM
Password (Min : 20 bytes, Max: 32 Bytes)	The probability of successful single random attempt is $1/(2^{160})$ The probability of successful multiple random attempts is $30,000/(2^{160})$ in one minute
RSA-PSS-2048 with SHA-256 digital signature verification	The probability of successful single random attempt is $1/2^{112}$ The probability of successful multiple random attempts is $1200/2^{112}$ in one minute

Exhibit 17 - *Strengths of Authentication Mechanisms*

9 ACCESS CONTROL POLICY

9.1 AUTHENTICATED SERVICES

Type(s) of access
R – read access
W – write access
E – execute access
Z – zeroize

ROLE	SERVICE	CSPS AND PUBLIC KEYS	SECURITY FUNCTIONS	TYPE(S) OF ACCESS
Cryptographic Officer (Drive Owner)	TCG Activate	UKEK PBKDF Master Key PBKDF Internal State Operator Password	KTS (AES-KW) SHS (SHA-512) PBDKF	E
Cryptographic Officer User	TCG Set PIN	UKEK PBKDF Master Key PBKDF Internal State Operator Password	KTS (AES-KW) SHS (SHA-512) PBKDF	W
Cryptographic Officer User	TCG Gen Key	Seed Material of SP800-90A Internal State of SP800-90A UKEK PBKDF Master Key PBKDF Internal State DEK	KTS (AES-KW) SHS (SHA-512) DRBG(HMAC_DRBG) PBDKF	E
		DEK	DRBG(HMAC_DRBG)	Z

ROLE	SERVICE	CSPS AND PUBLIC KEYS	SECURITY FUNCTIONS	TYPE(S) OF ACCESS
Cryptographic Officer	TCG Enable/Disable Authority	N/A	N/A	N/A
Cryptographic Officer	TCG Set/Get LBA Range	N/A	N/A	N/A
Cryptographic Officer User	TCG Lock / Unlock LBA Range	UKEK PBKDF Master Key PBKDF Internal DEK	KTS (AES-KW) PBKDF	E
Cryptographic Officer	Return to uninitialized state	DEK UKEK PBKDF Master Key PBKDF Internal State Seed Material of SP800-90A Internal State of SP800-90A Operator Password	KTS (AES-KW) SHS (SHA-512) DRBG(HMAC_DRBG) PBKDF	E Z
Cryptographic Officer	TCG Set MBR	N/A	N/A	N/A
Cryptographic Officer	TCG SET/GET DataStore	N/A	N/A	N/A
Cryptographic Officer	TCG SET ACE	N/A	N/A	N/A
Cryptographic Officer	TCG Enable/Disable MBR Mode	N/A	N/A	N/A
Cryptographic Officer User	Authenticated User Data Read/Write	DEK	AES (XTS)	R W E
Firmware Download Role	Update Firmware	RSA Code Sign Public Key	RSA(RSA-2048-PSS) SHS (SHA-256)	E

Exhibit 18 – *Authenticated Services Table*

9.2 UNAUTHENTICATED SERVICE

The following services are available to unauthenticated roles. They are also available to authenticated roles upon successful authentication.

ROLE	SERVICE	CSPS AND PUBLIC KEYS	TYPE(S) OF ACCESS
Unauthenticated Role	Power Cycle	N/A	N/A
Unauthenticated Role	Generate Random Number	Seed Material of SP800-90A Internal State of SP800-90A	E
Unauthenticated Role	Show Status	N/A	N/A
Anybody	TCG Get MBR	N/A	N/A
Unauthenticated Role	Reset	N/A	N/A
Unauthenticated Role	Return to uninitialized state(PSID)	DEK UKEK PBKDF Master Key PBKDF Internal State Seed Material of SP800-90A Internal State of SP800-90A	Z
Unauthenticated Role	Show FIPS approve mode state	N/A	N/A
Anybody	TCG Get MSID	N/A	N/A

ROLE	SERVICE	CSPS AND PUBLIC KEYS	TYPE(S) OF ACCESS
Anybody Unauthenticated Role	TCG Session Control	Operator Password[1]	E Z
Unauthenticated Role	SATA Standard	N/A	N/A
Unauthenticated Role	NVMe Standard	N/A	N/A
Unauthenticated Role	Non User Data Read/Write	N/A	N/A
Unauthenticated Role	Non User Data Output	N/A	N/A
Unauthenticated Role	Non User Data Input	N/A	N/A
Unauthenticated Role	Configuration	N/A	N/A
Unauthenticated Role	Self-Test	N/A	N/A
Unauthenticated Role	Show Status(DAS)	N/A	N/A

Exhibit 19 – *Unauthenticated Services Table*

[1] In order to perform TCG Session Control with Start Session command, the Operator Password must be entered into the module to successfully authenticate into the proper Role. The service is unauthenticated until such a time that a successful authentication occurs. When, TCG Session Control with End Session command is issued, the plaintext Operator Password is zeroized.

10 APPROVED ALGORITHMS

CAVP CERT	ALGORITHM	STANDARD	MODE/METHOD	KEY LENGTH	USE
C1356	AES	FIPS 197 SP 800-38A	CBC[2]	256	Prerequisite
C1356	AES	FIPS 197 SP800-38E	XTS	256	User Data Encrypt/ Decrypt
Vendor Affirmed	CKG	SP800-133	unmodified output from SP 800-90A DRBG		Cryptographic Key Generation
C1356	DRBG	SP800-90A	HMAC_DRBG (SHA-256)		Deterministic Random Bit Generation
C1356	HMAC	FIPS 198-1	HMAC-SHA256[3]	256	Prerequisite
C1356	KTS	SP800-38F	AES-KW	256	Key Wrapping
A1726	PBKDF	SP800-132 (option 2a)	HMAC-SHA256	160	Deriving Keys for Storage Application
C1355 C1356	RSA	FIPS 186-4	RSA-2048-PSS With SHA-256	2048	Digital Signature Verification
C1355 C1356	SHS	FIPS 180-4	SHA 256[4]	N/A	Prerequisite

[2] AES-CBC is only used as a pre-requisite; AES-CBC standalone is not utilized in the FIPS Approved Mode.

[3] HMAC-SHA-256 is only used as a pre-requisite; HMAC-SHA-256 standalone is not utilized in the FIPS Approved Mode.

[4] SHA-256 is only used as a pre-requisite; SHA-256 standalone is not utilized in the FIPS Approved Mode.

CAVP CERT	ALGORITHM	STANDARD	MODE/METHOD	KEY LENGTH	USE
C1356	SHS	FIPS 180-4	SHA-512	N/A	Password Protection

Exhibit 20 – *Table of Approved Algorithms for the PS3112-S12 SATA family*

CAVP CERT	ALGORITHM	STANDARD	MODE/METHOD	KEY LENGTH	USE
C1358	AES	FIPS 197 SP 800-38A	CBC[5]	256	Prerequisite
C1358	AES	FIPS 197 SP800-38E	XTS	256	User Data Encrypt/ Decrypt
Vendor Affirmed	CKG	SP800-133	unmodified output from SP 800-90A DRBG		Cryptographic Key Generation
C1358	DRBG	SP800-90A	HMAC_DRBG (SHA-256)		Deterministic Random Bit Generation
C1358	HMAC	FIPS 198-1	HMAC-SHA256[6]	256	Prerequisite
C1358	KTS	SP800-38F	AES-KW	256	Key Wrapping
A1725	PBKDF	SP800-132 (option 2a)	HMAC-SHA256	160	Deriving Keys for Storage Application
C1357 C1358	RSA	FIPS 186-4	RSA-2048-PSS With SHA-256	2048	Digital Signature Verification

5 AES-CBC is only used as a pre-requisite; AES-CBC standalone is not utilized in the FIPS Approved Mode.

6 HMAC-SHA-256 is only used as a pre-requisite; HMAC-SHA-256 standalone is not utilized in the FIPS Approved Mode.

CAVP CERT	ALGORITHM	STANDARD	MODE/METHOD	KEY LENGTH	USE
C1357 C1358	SHS	FIPS 180-4	SHA-256[7]	N/A	Prerequisite
C1358	SHS	FIPS 180-4	SHA-512	N/A	Password Protection

Exhibit 21 – *Table of Approved Algorithms for the PS5012-E12 NVMe PCIe family*

[7] SHA-256 is only used as a pre-requisite; SHA-256 standalone is not utilized in the FIPS Approved Mode.

The following are Non-Approved but allowed Algorithms:

ALGORITHM	USE
NDRNG	Seed of DRBG (256 bit)
HMAC-SHA-256[8] (non-compliant) (no security claimed)	No security claimed as per FIPS 140-2 IG 1.23 scenario number 2. The HMAC-SHA-256 algorithm is approved, however its usage is not security relevant and non-compliant as its only purpose is to support a proprietary handshake between the module and the host (outside of the security boundary) to check the correctness of the command associated with the "Configuration" service. The HMAC-SHA-256 algorithm is not used whatsoever during the “Configuration” service to meet any FIPS 140-2 requirements and its usage is strictly considered plaintext. The HMAC-SHA-256 algorithm does not access CSPs of the module and is not intended to be used as a security function, the algorithm is non-compliant because the key used is hardcoded (i.e. constant), non-zeroizable, and said key is not meant to fulfill a security purpose. The non-compliant use and purpose of the HMAC-SHA-256 algorithm is unambiguous and cannot be easily confused for a security function since in the FIPS approved mode there are no HMAC-SHA-256 services exposed to the operator and HMAC-SHA-256 is only used as an underlying prerequisite for other algorithms.

Exhibit 22 – *Table of Non-Approved but allowed Algorithms for all modules*

[8] The use of this non-compliant algorithm is only available in Firmware Version ECPM13.1

11 PHYSICAL SECURITY POLICY

Following physical security mechanisms are implemented by the module:

1. Production grade components
2. The complete module is covered with an opaque epoxy resin, leaving only the host interface connector (NVMe/SATA data and power ports) exposed.

When checking the module for tamper evidence the following actions are mandatory:

PHYSICAL SECURITY MECHANISMS	RECOMMENDED FREQUENCY OF INSEPCTION/TEST	INSPECTON/TEST GUIDANCE DETAILS
Opaque epoxy resin	As often as possible	Inspection of the epoxy resin for any evidence of scratches, gouges, cuts and other deficiencies. In any case of evidence of tampering the module shall be removed from service

Exhibit 23 - *Inspection/Testing of Physical Security Mechanisms*

12 MITIGATION OF OTHER ATTACKS POLICY

The cryptographic module has not been designed to mitigate any specific attacks beyond the scope of FIPS 140-2.

OTHER ATTACKS	MITIGATION MECHANISM	SPECIFIC LIMITATIONS
N/A	N/A	N/A

Exhibit 24 – *Table of Mitigation of Other Attacks*