MaiStorage

Maistorage Technology Sdn. Bhd.

MaiStorage TCG Opal SSC SSD Series (PS5018-E18)

MyCV Non-Proprietary Security Policy

Document Version: V1.00

H/W Version: FPD2130-512G-V01, FPD2130-1024G-V01, FPD2130-2048G-V01, FPD2130-4096G-V01, FPD2130-8192G-V01, FPD2110-1024G-V01, FPD2110-2048G-V01, FPD2110-4096G-V01, FPD2110-8192G-V01, FPD2150-1024G-V01, FPD2150-2048G-V01, FPD2150-4096G-V01, FPD2150-8192G-V01

F/W Version: EIQM50.0

Table of Contents

List of Tables

List of Figures

Version	Date	Updates	Author
V1.00	2026/2/20	First release	Hoh Chew Wen

1 General

1.1 Overview

This document is the non-proprietary MyCV Security Policy for the MaiStorage TCG Opal SSC SSD Series (PS5018-E18), hereafter referred to as “MaiStorage SSDs” or the “cryptographic modules” or simply “CM” in this document. It describes how the cryptographic module products meet MyCV for overall Security Level 2 security requirement.

1.2 Security Levels

Section	Title	Security Level
1	General	2
2	Cryptographic module specification	2
3	Cryptographic module interfaces	2
4	Roles, services, and authentication	2
5	Software/Firmware security	2
6	Operational environment	N/A
7	Physical security	2
8	Non-invasive security	N/A
9	Sensitive security parameter management	2
10	Self-tests	2
11	Life-cycle assurance	2
12	Mitigation of other attacks	N/A
	Overall Level	2

Table 1: Security Levels

2 Cryptographic Module Specification

2.1 Description

Purpose and Use:

The MaiStorage TCG Opal SSC SSD Series (PS5018-E18) consists of multi-chip embedded cryptographic modules designed to meet MyCV Level 2 requirements. These SSDs provide access control and feature built-in AES-XTS-256 encryption hardware for on-the-fly encryption of user data before it is stored on NAND Flash. MaiStorage SSDs support NVMe PCIe interfaces and they are based on the industry-standard TCG Opal SSC protocol.

Module Type: Hardware

Module Embodiment: Multi-Chip Embedded

Module Characteristics [O]:

Cryptographic Boundary:

The multi-chip embedded modules are shown below in Figure 1, Figure 2 and Figure 3 according to different form factors. M.2 2280 cryptographic boundary of the modules is defined by the physical perimeter of the PCB. U.2 and E1.S cryptographic boundary is the enclosure case. The physical interface to the cryptographic module is the PCIe connector.

Tested Operational Environment's Physical Perimeter (TOEPP) [O]:

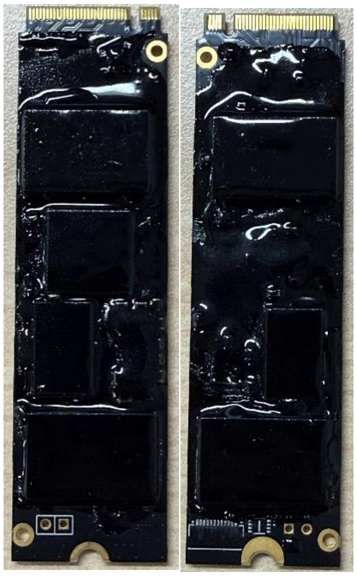

Figure 1: MaiStorage TCG Opal SSC SSD Series (PS5018-E18) with M.2 2280 form factor [Capacities: 512GB, 1TB, 2TB and 4TB]

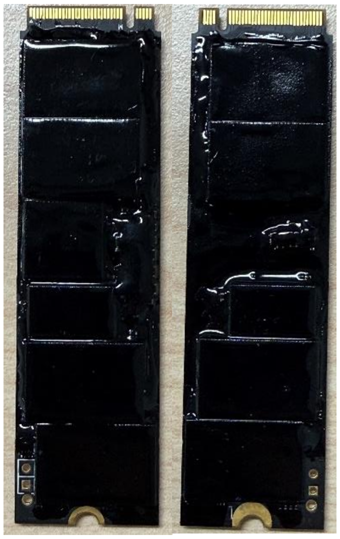

Figure 2: MaiStorage TCG Opal SSC SSD Series (PS5018-E18) with M.2 2280 form factor [Capacity: 8TB]

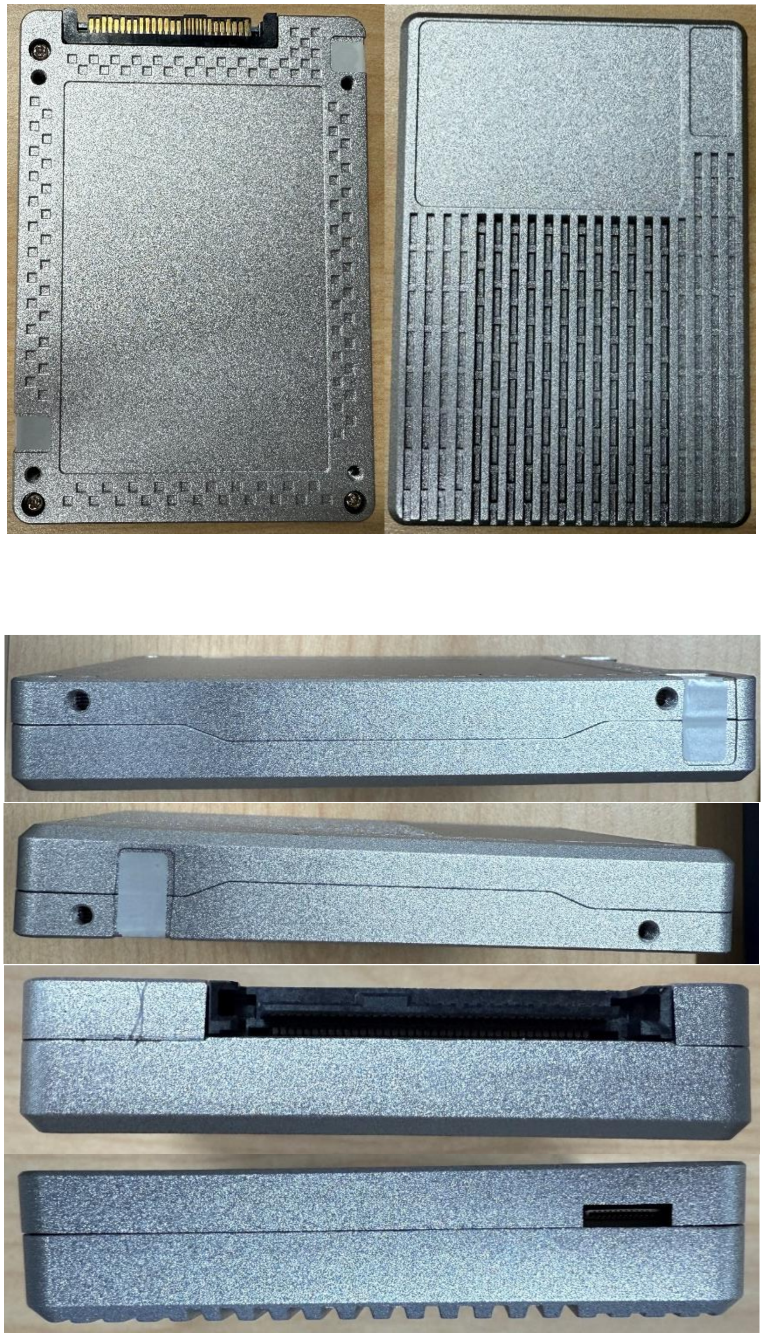

Figure 3: MaiStorage TCG Opal SSC SSD Series (PS5018-E18) with U.2 form factor

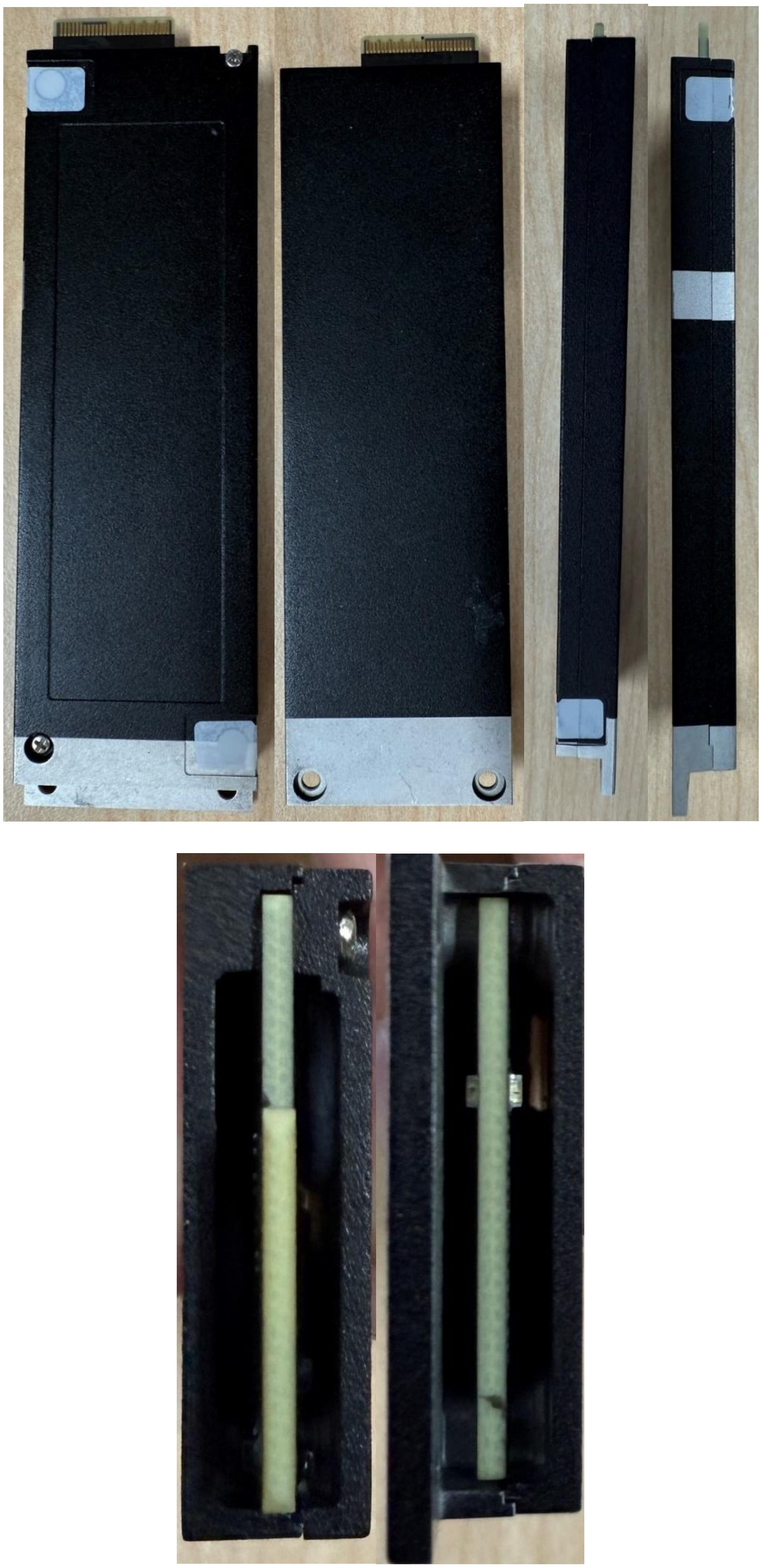

Figure 4: MaiStorage TCG Opal SSC SSD Series (PS5018-E18) with E1.S form factor

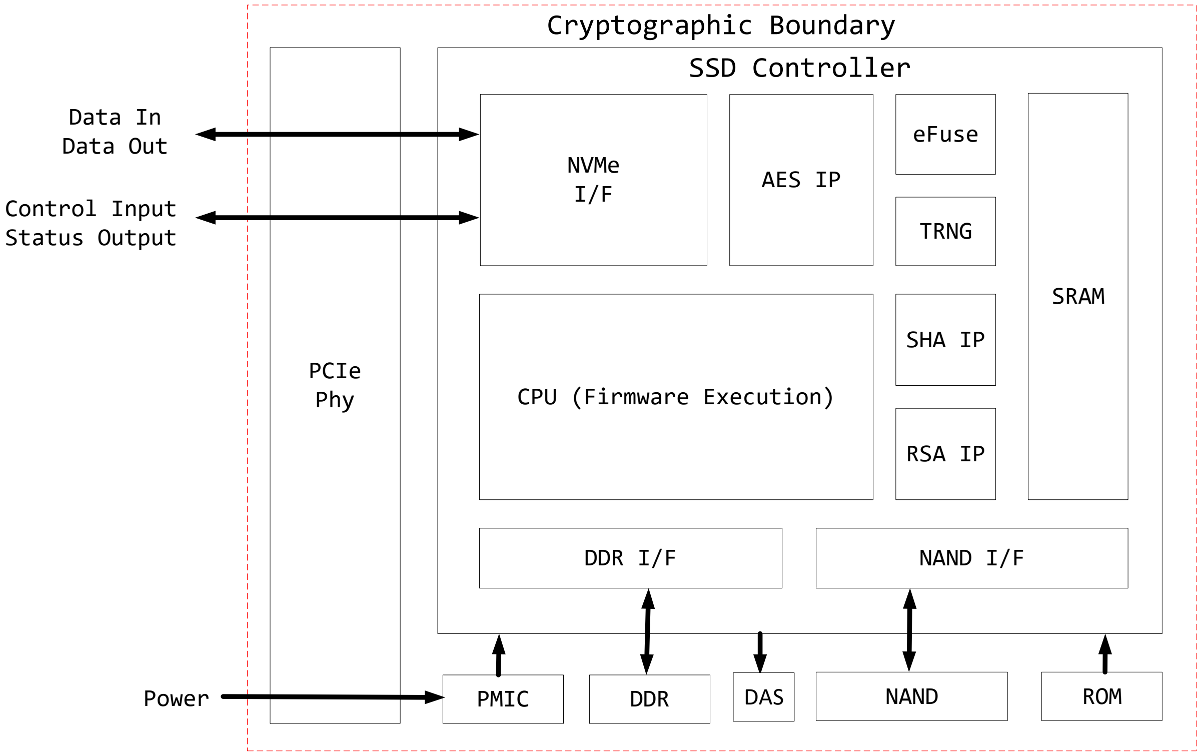

Figure 5: Module Block Diagram

2.2 Tested and Vendor Affirmed Module Version and Identification

Tested Module Identification – Hardware:

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
M.2 2280 NVMe NAND FLASH SSD 512GB	FPD2130-512G-V01	EIQM50.0	PS5018-E18	M.2 2280, 512GB
M.2 2280 NVMe NAND FLASH SSD 1TB	FPD2130-1024G-V01	EIQM50.0	PS5018-E18	M.2 2280, 1TB
M.2 2280 NVMe NAND FLASH SSD 2TB	FPD2130-2048G-V01	EIQM50.0	PS5018-E18	M.2 2280, 2TB
M.2 2280 NVMe NAND FLASH SSD 4TB	FPD2130-4096G-V01	EIQM50.0	PS5018-E18	M.2 2280, 4TB
M.2 2280 NVMe NAND FLASH SSD 8TB	FPD2130-8192G-V01	EIQM50.0	PS5018-E18	M.2 2280, 8TB
U.2 NVMe NAND FLASH SSD 1TB	FPD2110-1024G-V01	EIQM50.0	PS5018-E18	U.2, 1TB
U.2 NVMe NAND FLASH SSD 2TB	FPD2110-2048G-V01	EIQM50.0	PS5018-E18	U.2, 2TB
U.2 NVMe NAND FLASH SSD 4TB	FPD2110-4096G-V01	EIQM50.0	PS5018-E18	U.2, 4TB
U.2 NVMe NAND FLASH SSD 8TB	FPD2110-8192G-V01	EIQM50.0	PS5018-E18	U.2, 8TB

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
E1.S NVMe NAND FLASH SSD 1TB	FPD2150-1024G-V01	EIQM50.0	PS5018-E18	E1.S, 1TB
E1.S NVMe NAND FLASH SSD 2TB	FPD2150-2048G-V01	EIQM50.0	PS5018-E18	E1.S, 2TB
E1.S NVMe NAND FLASH SSD 4TB	FPD2150-4096G-V01	EIQM50.0	PS5018-E18	E1.S, 4TB
E1.S NVMe NAND FLASH SSD 8TB	FPD2150-8192G-V01	EIQM50.0	PS5018-E18	E1.S, 8TB

Table 2: Tested Module Identification – Hardware

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

N/A for this module.

Tested Module Identification – Hybrid Disjoint Hardware:

N/A for this module.

Tested Operational Environments - Software, Firmware, Hybrid:

N/A for this module.

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

N/A for this module.

2.3 Excluded Components

The MaiStorage TCG Opal SSC SSD Series (PS5018-E18) does not define any excluded components within the module's boundary.

2.4 Modes of Operation

Modes List and Description:

Mode Name	Description	Type	Status Indicator
MyCV Approved Mode	The cryptographic module is operating as a compliant MyCV module	Approved	The MyCV Approved Mode global indicator is at Level 0 Discovery response data byte 47 bit 1. When bit 1 is equal to 1, it means that the module is already in MyCV approved mode.

Table 3: Modes List and Description

When the cryptographic module is shipped from the manufacturer factory, it is an uninitialized mode of operation in its fresh out-of-the-box state with an approved firmware. The Crypto Officer must follow the requirements defined in this Security Policy, including the initialization procedures outlined in Section 11, to initialize the module into an Approved mode of operation to enable authentication function. It is possible to switch from the initialized state to an uninitialized state by performing the Return to uninitialized state service.

Mode Change Instructions and Status [O]:

Once the Crypto Officer has followed the initialization procedures in Section 11, the module is in a MyCV approved mode of operation. Any violation of Section 11 or other requirements specified in the Security Policy will place this module in a non-compliance mode of operation.

Degraded Mode Description [O]:

The cryptographic module does not claim any degraded mode.

2.5 Algorithms

Approved Algorithms:

Algorithm	CAVP Cert	Properties	Reference
AES-ECB	MyCV-CAV006	Direction: Decrypt, Encrypt Key Length: 256	ISO/IEC 18033 3:2010 Information technology — Security techniques — Encryption algorithms Part 3: Block ciphers
			FIPS 197 Advanced Encryption Standard (AES)
AES-KW	MyCV-CAV006	Direction: Decrypt, Encrypt Key Length: 256	ISO/IEC 18033 3:2010 Information technology — Security techniques — Encryption algorithms Part 3: Block ciphers
AES-XTS Testing Revision 2.0	MyCV-CAV006	Direction: Decrypt, Encrypt Key Length: 256	ISO/IEC 18033 3:2010 Information technology — Security techniques — Encryption algorithms Part 3: Block ciphers
			FIPS 197 Advanced Encryption Standard (AES)
HMAC DRBG	MyCV-CAV006	Prediction Resistance: No Mode: SHA2-256	ISO/IEC 18031:2011 Information technology – Security techniques – Random bit generation
			NIST Special Publication 800-90A Revision 1 Recommendation for Random Number Generation Using

Algorithm	CAVP Cert	Properties	Reference
			Deterministic Random Bit Generators
HMAC-SHA2-256	MyCV-CAV006	Key Length: Key Length: 64-256 Increment 8	ISO/IEC 9797-2:2021 Information technology– Security techniques — Message Authentication Codes (MACs) - Part 2: Mechanisms using a dedicated hash-function
			FIPS 198-1 The Keyed-Hash Message Authentication Code (HMAC)
PBKDF	MyCV-CAV006	Iteration Count: Iteration Count: 1-1000 Increment 1 Password Length: Password Length: 8-32 Increment 1	SP 800-132 Recommendation for Password-Based Key Derivation: Part 1: Storage Applications
RSA SigVer (FIPS186-4)	MyCV-CAV006	Signature Type: PKCSPSS Modulo: 4096	FIPS186-4 Digital Signature Standard (DSS)
SHA2-256	MyCV-CAV006	Message Length: Message Length: 0-65536 Increment 8	ISO/IEC 10118-3:2004 Information technology — Security techniques — Hash-functions Part 3: Dedicated hash-functions
			FIPS 180-4 Secure Hash Standard (SHS)
SHA2-512	MyCV-CAV006	Message Length: Message Length: 0-65536 Increment 8	ISO/IEC 10118-3:2004 Information technology — Security techniques — Hash-functions Part 3: Dedicated hash-functions
			FIPS 180-4 Secure Hash Standard (SHS)

Table 4: Approved Algorithms

Vendor-Affirmed Algorithms:

Name	Properties	Implementation	Reference
CKG	Symmetric Key: AES	PS5018-E18	SP 800-133 Rev. 2: Section 4: Using the output of a Random Bit Generator

Table 5: Vendor-Affirmed Algorithms

Non-Approved, Allowed Algorithms:

N/A for this module.

Non-Approved, Allowed Algorithms with No Security Claimed:

N/A for this module.

Non-Approved, Not Allowed Algorithms:

N/A for this module.

2.6 Security Function Implementations

Name	Type	Description	Properties	Algorithms
User Data Protection	BC-UnAuth	Encryption/Decryption of Operator Data	SP800-38E: Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices	AES-XTS Testing Revision 2.0: (MyCV-CAV006) Key size: 256 bits AES-ECB: (MyCV-CAV006) Key size: 256 bits
Password Protection	SHA	Hash authentication password	FIPS PUB 180-4: Secure Hash Standard (SHS)	SHA2-512: (MyCV-CAV006) Digest size: 512 bits
Deterministic Random Bit Generation	DRBG	Generate deterministic random bit	NIST SP 800-90A Rev. 1: Recommendation for Random Number Generation Using Deterministic Random Bit Generators	HMAC DRBG: (MyCV-CAV006) Digest size: 256 bits
Key Wrapping	KTS-Wrap	Key Wrapping, Key Unwrapping	NIST SP 800-38F: Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping	AES-KW: (MyCV-CAV006) Key size: 256 bits AES-ECB: (MyCV-CAV006) Key size: 256 bits

Name	Type	Description	Properties	Algorithms
Digital Signature Verification	DigSig-SigVer SHA	Perform RSA Signature Verification	FIPS 186-4: Digital Signature Standard (DSS) FIPS PUB 180-4: Secure Hash Standard (SHS)	RSA SigVer (FIPS186-4): (MyCV-CAV006) Key size: 4,096 bits SHA2-512: (MyCV-CAV006) Digest size : 512 bits
Password-Based Key Derivation	PBKDF	Deriving Keys for Storage Application	SP 800-132: Recommendation for Password-Based Key Derivation: Part 1: Storage Applications FIPS 198-1: The Keyed-Hash Message Authentication Code (HMAC)	PBKDF: (MyCV-CAV006) Key size: 160 bits HMAC-SHA2-256: (MyCV-CAV006) Digest size: 256 bits SHA2-256: (MyCV-CAV006) Digest size: 256 bits
HW RNG	ENT-ESV	Entropy Source		

Table 6: Security Function Implementations

2.7 Algorithm Specific Information

PBKDF

The module supports key derivation from a password using PBKDF algorithm as per SP 800-132. This algorithm's specifications include the iteration count between 1 to 1000 with the increment of 1, salt length between 128 bits to 256 bits with the increment of 8 bits and HMAC-SHA-256.

The password includes any value from a minimum 10 bytes to a maximum 32 bytes. With this range, it leads to the probability that a random attempt correctly guesses a 10-byte password is equal to 1 / (2^{80}). Also, this leads to the probability that a random attempt correctly guesses a 32-byte password is equal to 1 / (2^{256}).

The derived key is used for key-wrapping the Key Encryption Key (KEK) to protect the Data Encryption Key (DEK), which is used in data storage applications.

2.8 RBG and Entropy

Cert Number	Vendor Name
NIST CMVP Entropy Source Validation (ESV) Certificate E274	Phison Electronics Corporation

Table 7: Entropy Certificates

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
Phison NOISEGEN T12FFC TRNG	Physical	PS5018-E18	1 bit	0.8 bits	

Table 8: Entropy Sources

The PS5018-E18 ASIC hardware includes a true non-deterministic random number generator called “NOISEGEN_T12FFC”. This NOISEGEN_T12FFC is a physical entropy source that meets the requirements of SP800-90B. It is used to seed a deterministic random bit generator (DRBG) that complies with SP800-90A.

2.9 Key Generation

The cryptographic module performs Cryptographic Key Generation (CKG) as per SP 800-133 rev 2 Section 4 “Using the output of a Random Bit Generator”. The resulting generated symmetric keys are the unmodified output from HMAC DRBG as per SP 800-90A Rev. 1.

2.10 Key Establishment

The cryptographic module does not support key establishment scheme.

2.11 Industry Protocols

The cryptographic module supports the TCG Storage SSC: Opal Security Protocol.

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

Physical Port	Logical Interface(s)	Data That Passes
PCIe Connector	Data Input	NVMe interface, user data, authentication data, signed data
PCIe Connector	Data Output	NVMe interface, user data
PCIe Connector	Control Input	NVMe interface, command and signal input
PCIe Connector	Control Output	N/A
PCIe Connector	Status Output	NVMe interface, status and signal output

Physical Port	Logical Interface(s)	Data That Passes
PCIe Connector	Power	Power interface
Device Activity Signal (DAS)	Status Output	The DAS pin will toggle at different frequencies according to different types of error which are MyCV Error State or Boot Code Fail Loop State

Table 9: Ports and Interfaces

The cryptographic module uses the PCIe Connector for the interface. The debug interfaces, including JTAG and UART, are physically present but disabled during manufacturing and protected by the module's security mechanisms. Therefore, they are considered latent functionalities and are not available in either the uninitialized state or the Approved mode.

Additionally, Control Output is not applicable for this cryptographic module as it does not output any commands, signals or control data to control another module.

4 Roles, Services, and Authentication

The roles, services and authentication that are supported by this CM are included in this section.

4.1 Authentication Methods

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
Password	Role-based, Cryptographic Officer, User Min: 10 bytes Max: 32 bytes Under a power on condition, entering the password of the storage device incorrectly 5 times consecutively will result in a locked state of the device, and the password cannot be entered again. To unlock the device and input the password again, a power cycle or using PSID revert at the 5th incorrect attempt is required.	Password Protection	The probability of a successful single random attempt is 1/(2^80).	The probability of successful multiple random attempts is 30,000/(2^80) in one minute.

Table 10: Authentication Methods

4.2 Roles

Name	Type	Operator Type	Authentication Methods
SID	Role	Crypto Officer (Drive Owner)	Password
Admins(1~4)	Role	Crypto Officer	Password

Name	Type	Operator Type	Authentication Methods
Users(1~9)	Role	User	Password
PSID	Role	Crypto Officer	Password

Table 11: Roles

To assume the “Anybody” role, the operator needs to execute “TCG Session Control” service with a TCG StartSession command, provided with the Anybody UID and a password is not required. “Anybody” is a TCG authority who can only perform TCG methods under unauthenticated services but still need to use the TCG StartSession command. Hence, this role is considered an unauthenticated role.

4.3 Approved Services

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
TCG Set PIN	Change operator authentication credentials	MyCV Approved mode global indicator is true	Password	Status	Password Protection Key Wrapping Password-Based Key Derivation	SID - Operator Password: W,E - Password Hash: W - User Key Encryption Key (All Range): W Admins(1~4) - Operator Password: W,E - Password Hash: W - User Key Encryption Key (All Range): W Users(1~9) - Operator Password: W,E - Password Hash: W - User Key Encryption Key (All Range): W
TCG Activate	Activate TCG	MyCV Approved mode global	N/A	Status	Password Protection Key Wrapping	SID - Operator Password: W,E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
		indicator is true			Password-Based Key Derivation	- User Key Encryption Key (All Range): W - PBKDF Master Key: W,E - PBKDF Internal State: W,E
TCG Gen Key	Generate new keys	MyCV Approved mode global indicator is true	N/A	Status	Deterministic Random Bit Generation Key Wrapping HW RNG	Admins(1~4) - Entropy Input String: G,W,E - Seed: G,W,E - Internal State (V and Key) of SP800-90A: G,W,E - User Key Encryption Key (All Range): E - PBKDF Master Key: W,E - PBKDF Internal State: W,E - Data Encryption Key (DEK): G,E,Z
TCG Enable/ Disable Authority	Enable or disable the authority	MyCV Approved mode global indicator is true	Authority Table data	Status	None	Admins(1~4)
TCG Set/Get LBA Range	Set or Get the Locking LBA Range	MyCV Approved mode global indicator is true	Set: LBA Range Get: N/A	Set: Status Get: LBA Range	None	Admins(1~4)
TCG Lock/ Unlock	Lock or unlock the LBA Range	MyCV Approved mode global	Locking Table Data	Status	Key Wrapping Password-	Admins(1~4) - User Key Encryption Key (All

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
LBA Range		indicator is true			Based Key Derivation	Range): E - PBKDF Master Key: W,E - PBKDF Internal State: W,E - Data Encryption Key (DEK): E Users(1~9) - User Key Encryption Key (All Range): E - PBKDF Master Key: W,E - PBKDF Internal State: W,E - Data Encryption Key (DEK): E
Return to uninitialized state	Erase user data in all Range by changing the data encryption key and clearing the authentication data	MyCV Approved mode global indicator is true	PSID, Revert()	Status	Password Protection Deterministic Random Bit Generation Key Wrapping Password-Based Key Derivation HW RNG	Admins(1~4) - Operator Password: Z - User Key Encryption Key (All Range): G,W,Z - Data Encryption Key (DEK): G,W,Z - PBKDF Master Key: W,E,Z - PBKDF Internal State: W,E,Z - Entropy Input String: G,W,E,Z - Seed: G,W,E,Z - Internal State

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						(V and Key) of SP800-90A: G,W,E,Z PSID - Data Encryption Key (DEK): G,W,Z - User Key Encryption Key (All Range): G,W,Z - PBKDF Master Key: W,E,Z - PBKDF Internal State: W,E,Z - Seed: G,W,E,Z - Internal State (V and Key) of SP800-90A: G,W,E,Z - Entropy Input String: G,W,E,Z
TCG Set MBR	Set MBR Byte Table	MyCV Approved mode global indicator is true	MBR Byte Table Data	Status	None	Admins(1~4)
TCG Set/Get DataStore	Write or Read DataStore Byte Table	MyCV Approved mode global indicator is true	Set: DataStore Byte Table Get: N/A	Set: N/A Get: DataStore Byte Table	None	Admins(1~4)
TCG Set ACE	Set ACE Table	MyCV Approved mode global indicator is true	ACE Table Data	Status	None	Admins(1~4)

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
TCG Enable/Disable MBR Mode	Enable or disable MBR Mode	MyCV Approved mode global indicator is true	MBR Control Table Data	Status	None	Admins(1~4)

Authenticated User Data Read/Write	Read or Write user data from/to Locking range	MyCV Approved mode global indicator is true	R: Data address and range
			W: User data
				R: User data, W: Status	User Data Protection	Admins(1~4)
						- Data Encryption Key (DEK): E
						Users(1~9)
						- Data Encryption Key (DEK): E

Update Firmware	Update the firmware. The firmware image must be validated for updating.	MyCV Approved mode global indicator is true	Firmware Image	Status	Digital Signature Verification	SID - RSA Firmware Integrity Public Key: E - Hash value of the RSA Firmware Integrity Public Key: E
Show Module Version Information	Showing device information by Compliance Descriptor (i.e. firmware version, hardware part number, module name, compliance version, etc.)	Module name or identifier: byte 276-281 of response data. Hardware part number and revision: byte 20-59 of response data. Firmware version byte 148-155 of response data.	N/A	Return requested module data	None	Unauthenticated
Clear FW	Zeroize the hash value of	MyCV Approved	PSID	Status	None	PSID - RSA

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Integrity Public Key	the RSA Firmware Integrity Public Key in eFuse by PSID account	mode global indicator is true				Firmware Integrity Public Key: Z
Self-Test	The Cryptographic Module performs self-tests when it powers up	N/A	N/A	Drive ready or MyCV Error State	Deterministic Random Bit Generation Key Wrapping Digital Signature Verification Password-Based Key Derivation	Unauthenticated
Show Status	Showing Approved Mode state	TCG Level0 Discovery Byte 47 be set to 1.	N/A	Return requested module data	None	Unauthenticated

Table 12: Approved Services

When cryptographic module is in approved mode, a global indicator is used.
The successful completion of a service is an implicit indicator for the use of an approved service.

After power cycling, authentication will be cleared, while operator needs to use the authentication service, re-authenticated for the operator is needed.

4.4 Non-Approved Services

The CM does not support non-approved services.

4.5 External Software/Firmware Loaded

Firmware can be upgraded (replaced) through a signed firmware download operation. If the downloaded code is successfully authenticated, the module will begin operating with the new firmware image.

When loading new firmware, the module performs an Update Firmware service using RSA 4096 (Cert #MyCV-CAV006) with SHA-512 (Cert #MyCV-CAV006) to verify the integrity of the firmware before uploading it into the CM.

Data output is inhibited via the data output interface during the firmware loading and load test, because the CM does not process other tasks when performing the firmware loading and load test.

5 Software/Firmware Security

5.1 Integrity Techniques

The Cryptographic Module uses the RSA signature verification method to verify the firmware binary image within the Cryptographic Module before execution. Operators can initiate the firmware integrity test anytime by power cycling the Cryptographic Module.

If the integrity test does not pass, the cryptographic module will undergo a transition to the Boot Code Failed Loop State.

5.2 Initiate on Demand

The operator initiates the integrity test on demand by power cycling the Cryptographic Module.

5.3 Open-Source Parameters [O]

No open-source firmware code has been included in the CM development process or used in this cryptographic module.

5.4 Additional Information [O]

The form of the executable code is binary file.

6 Operational Environment

6.1 Operational Environment Type and Requirements

The CM operates in a limited operational environment. Firmware inside the CM could be updated by an external source by firmware update operation. Before accepting the new firmware, the CM will conduct RSA signature verification of the incoming firmware.

Type of Operational Environment: Limited

7 Physical Security

7.1 Mechanisms and Actions Required [O]

Mechanism	Inspection Frequency	Inspection Guidance
Opaque epoxy resin	As often as feasible	Inspection of the epoxy resin for any evidence of scratches, gouges, cuts and other deficiencies. In any case of evidence

Mechanism	Inspection Frequency	Inspection Guidance
		of tampering, the module shall be removed from service.
Production grade cases	The frequency of the physical inspection should be determined by the Crypto Officer. It is recommended that the enclosure be inspected monthly.	Periodic inspection to detect evidence of tampering: * Check enclosure for physical damage * Check for missing or loose screws If tampering is detected, remove the module from service. per the "End of Life" section of this document.
Two tamper-evident security labels	The frequency of the physical inspection should be determined by the Crypto Officer. It is recommended that the tamper-evident security labels be inspected monthly.	Periodic inspection to detect evidence of tampering: * Checkerboard pattern on tamper-evident security labels * Security label cutouts do not match original * Security label over PCBA screws not penetrated If tampering is detected, remove the module from service. per the "End of Life" section of this document.

Table 13: Mechanisms and Actions Required

Following physical security mechanisms are implemented by the module:

- Production grade components.
- For M.2 2280 modules, the 512GB, 1TB, 2TB, and 4TB capacities all share the same PCBA design, while the 8TB capacity uses a different PCBA. All complete modules with form factor of M.2 2280 is covered with an opaque epoxy resin within the visible spectrum, leaving only the host interface connector (PCIe PHY and power ports) exposed.
- The complete module with form factor of U.2 is attached with production grade cases together with the tamper-evident security labels, leaving only the host interface connector (PCIe PHY and power ports) exposed.

The complete module with form factor E1.S is covered with an opaque epoxy resin within the visible spectrum, leaving only the host interface connector (PCIe PHY and power ports) exposed. This module is also attached with production grade cases with the tamper-evident security labels.

8 Non-Invasive Security

Non-invasive security is not applicable for this cryptographic module.

9 Sensitive Security Parameters Management

9.1 Storage Areas

Storage Area Name	Description	Persistence Type
DRAM	Volatile memory	Dynamic
NAND	Non-volatile memory	Static
One-time Programmable	eFuse	Static

Table 14: Storage Areas

The module stores temporary SSPs in dynamic random-access memory (DRAM). Non-ephemeral SSPs are stored in static memory (NAND). The module has an eFuse to store the Secure boot SSP used to power-up firmware integrity testing.

9.2 SSP Input-Output Methods

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
Input 1 of RSA Firmware Integrity Public Key	External source	DRAM	Plaintext	Manual	Electronic	Digital Signature Verification
Input of Operator Password	External source	DRAM	Plaintext	Manual	Electronic	Password-Based Key Derivation

Table 15: SSP Input-Output Methods

The cryptographic module limits the input of SSPs to Operator Passwords and RSA Public Key. The cryptographic module stores the SHA-512 digest of the operator Password, and the SHA-256 digest of the RSA Public Key only exists during the FW loading flow. The module does not support the output of SSPs.

9.3 SSP Zeroization Methods

Zeroization Method	Description	Rationale	Operator Initiation
Power Cycle	Power cycling involves disconnecting and reconnecting the Cryptographic Module to its source of power.	Power cycling the module will zeroize all SSPs in DRAM due to it being volatile memory.	The operator physically or remotely disconnects the Cryptographic Module from its source of power.
Return to uninitialized state	Exit the MyCV Approved Mode. Cryptographic Module will enter uninitialized state and keys and SSPs will zeroize.	This service is akin to a "Restore factory defaults" operation, and provides a means to zeroize keys and CSPs.	The operator transmits TCG Revert() to the Cryptographic Module to initiate a zeroisation process.
TCG_GenKey	Generate new keys	Use the TCG GenKey method to generate new keys, replacing the old ones. The old key will be zeroized first then only the new key will be generated to replace the old key.	The operator transmits TCG GenKey command to the Cryptographic Module to initiate a zeroisation process.
TCG Set C_PIN	Change the C PIN	Change the operator password by TCG Set method.	The operator transmits TCG Set C Pin command to the

Zeroization Method	Description	Rationale	Operator Initiation
			Cryptographic Module to initiate a zeroisation process.
Clear FW Integrity Public Key	Zeroize the hash value of the RSA Firmware Integrity Public Key in eFuse by PSID account	A VUC command to set the RSA firmware integrity public key in eFuse to 1.	The operator issues a VUC command to the Cryptographic Module to initiate a zeroisation process.

Table 16: SSP Zeroization Methods

Receipt of the Completion Queue (CQ) by the host implicitly indicates that zeroization has been successfully completed.

9.4 SSPs

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
Data Encryption Key (DEK)	Key to encrypt user data	256 - 256	Symmetric Key - CSP	HMAC DRBG (MyCV-CAV006)		AES-XTS Testing Revision 2.0 (MyCV-CAV006)
User Key Encryption Key (All Range)	Key to encrypt DEK	256 - 256	Symmetric Key - CSP	HMAC DRBG (MyCV-CAV006)		AES-KW (MyCV-CAV006)
PBKDF Master Key	Password-based-key of operator passwords in Locking SP. Used to encrypt UKEK	256 - 256	Private - CSP	Password-Based Key Derivation		AES-KW (MyCV-CAV006)
Operator Password	Crypto Officer password/user password	80 ~ 256 - 80 ~ 256	Authentication - CSP			PBKDF (MyCV-CAV006) SHA2-512 (MyCV-CAV006)
Password Hash	Hash value of passwords	512 - 256	Authentication - CSP	Password Protection		

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
PBKDF Internal State	Temporary variable created during the PBKDF process.	8192 - 256	Private - CSP	Password-Based Key Derivation		PBKDF (MyCV-CAV006)
Entropy Input String	Internal state associated with the [SP 800 90A] HMAC_DRBG using SHA-256	256 - 256	Entropy - CSP	HW RNG		HMAC DRBG (MyCV-CAV006)
Seed	Seed = Entropy Input String || Nonce Entropy Input String is 32 bytes Nonce is 16 bytes Total Seed: 48 bytes	384 - 384	Entropy - CSP	Deterministic Random Bit Generation		HMAC DRBG (MyCV-CAV006)
Internal State (V and Key) of SP800-90A	Internal state associated with the [SP 800 90A] HMAC_DRBG using SHA-256 K is 32 bytes V is 32 bytes	256,256 - 256,256	Entropy - CSP	Deterministic Random Bit Generation		HMAC DRBG (MyCV-CAV006)
Hash value of the RSA Firmware Integrity Public Key	Hash value of the FW Integrity Key	256 - 256	Authentication - CSP	SHA2-256 (MyCV-CAV006)		Digital Signature Verification
RSA Firmware Integrity Public Key	Key for FW Load Self-Test	4096 - 152	Authentication - PSP			Digital Signature Verification

Table 17: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
Data Encryption Key (DEK)		DRAM:Plaintext NAND:Encrypted	Plaintext exists until Cryptographic Module is READ and Write locked.	Power Cycle Return to uninitialized state TCG_GenKey	
User Key Encryption Key (All Range)		DRAM:Plaintext NAND:Encrypted	Plaintext exists until Cryptographic Module is READ and Write locked and Close Session	Power Cycle Return to uninitialized state	Data Encryption Key (DEK):Encrypts Data Encryption Key (DEK):Decrypts
PBKDF Master Key		DRAM:Plaintext	Ephemeral, destroyed after using	N/A	User Key Encryption Key (All Range):Encrypts User Key Encryption Key (All Range):Decrypts Operator Password:Derived From
Operator Password	Input of Operator Password	DRAM:Plaintext	Plaintext exists until Close Session	Power Cycle Return to uninitialized state TCG Set C_PIN	
Password Hash		DRAM:Plaintext NAND:Plaintext	Exist during MyCV Approved Mode	Return to uninitialized state TCG Set C_PIN	Operator Password:Derived From
PBKDF Internal State		DRAM:Plaintext	Ephemeral, destroyed after using	N/A	
Entropy Input String		DRAM:Plaintext	Ephemeral, destroyed after exiting MyCV	N/A	Seed:Paired With Internal State (V and Key) of

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
			Approved Mode		SP800-90A:Paired With
Seed		DRAM:Plaintext	Ephemeral, destroyed after exiting MyCV Approved Mode	N/A	Internal State (V and Key) of SP800-90A:Paired With Entropy Input String:Paired With
Internal State (V and Key) of SP800-90A		DRAM:Plaintext	Ephemeral, destroyed after exiting MyCV Approved Mode	Return to uninitialized state	Entropy Input String:Paired With Seed:Paired With
Hash value of the RSA Firmware Integrity Public Key		One-time Programmable:Encrypted	N/A	Clear FW Integrity Public Key	RSA Firmware Integrity Public Key:Derived From
RSA Firmware Integrity Public Key	Input 1 of RSA Firmware Integrity Public Key	DRAM:Plaintext NAND:Plaintext	Ephemeral, destroyed after use.	N/A	RSA Firmware Integrity Public Key:Paired With

Table 18: SSP Table 2

Modification of PSPs by unauthorized operators is prohibited.

10 Self-Tests

Whenever the Cryptographic Module is powered up, it performs cryptographic algorithms self-tests automatically before starting execution security functions. The pre-operational test could also be on-demand tested by power cycling the module. All data output is inhibited during performing self-test. If the self-tests fail, the module enters the Boot Code Fail Loop State or the MyCV Error State which it ceases to provide any services to the host and the error can only be cleared by power cycling the module.

10.1 Pre-Operational Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
Boot Loader Integrity	RSA 4096 SHA-512 PSS Signature Verification	Digital Signature Verification	SW/FW Integrity	Pass: Next step Fail: Boot Code Fail Loop State	Verify
Firmware Integrity	RSA 4096 SHA-512 PSS Signature Verification	Digital Signature Verification	SW/FW Integrity	Pass: Boot to the firmware image Fail: MyCV Error State	Verify

Table 19: Pre-Operational Self-Tests

The Cryptographic Module performs a pre-operational self-test to verify the integrity of the firmware, including the algorithms listed below. An on-demand integrity test can also be initiated via the hardware module interface (HMI) by power cycling the module.

10.2 Conditional Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-XTS Testing Revision 2.0 (MyCV-CAV006)	256-bit	KAT	CAST	Pass: Next test Fail: MyCV Error State	Encrypt, Decrypt	Perform when power up
AES-KW (MyCV-CAV006)	256-bit	KAT	CAST	Pass: Next test Fail: MyCV Error State	Key Wrap, Key Unwrap	Perform when power up
SHA2-256 (MyCV-CAV006)	256-bit	KAT	CAST	Pass: Next test Fail: MyCV Error State	Verify	Perform when power up
SHA2-512 (MyCV-CAV006)	512	KAT	CAST	Pass: Next test Fail: MyCV Error State	Verify	Perform when power up
HMAC-SHA2-256 (MyCV-CAV006)	256	KAT	CAST	Pass: Next test Fail: MyCV Error State	Verify	Perform when power up
PBKDF (MyCV-CAV006)	8 bytes salt, Iteration count: 1	KAT	CAST	Pass: Next test Fail: MyCV Error State	Verify	Perform when power up

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
HMAC DRBG (MyCV-CAV006)	Instantiate, generate, and reseed health tests as per section 11.3 of SP 800-90A	KAT	CAST	Pass: Next test Fail: MyCV Error State	Verify	Perform when power up
ENT	Repetition Count Test (RCT), Adaptive Proportion Test (APT)	Repetition Count and Adaptive Proportion tests as per SP 800-90B	CAST	Pass: Next test Fail: MyCV Error State	Verifies that the RCT/APT threshold was not exceeded as specified in [SP 800 90B]	Perform when power up
RSA 4096 Signature Verification	RSA 4096 SHA-512 PSS Signature Verification	Digital Signature Verification	SW/FW Load	Pass: Boot to new image Fail: FW will perform an additional RSA 4096 SHA-512 PSS KAT to attempt error recovery. If the KAT fails, module immediately enters the MyCV Error State. If the KAT succeeds module is operational.	Verify	Firmware Commit
RSA SigVer (FIPS186-4) (MyCV-CAV006)	k=4096 with SHA512	KAT	CAST	Pass: Next Step Fail: MyCV Error State	Verify	RSA 4096 Signature Verification failed

Table 20: Conditional Self-Tests

10.3 Periodic Self-Test Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
Boot Loader Integrity	Digital Signature Verification	SW/FW Integrity	On Demand	Power cycle
Firmware Integrity	Digital Signature Verification	SW/FW Integrity	On Demand	Power cycle

Table 21: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-XTS Testing Revision 2.0 (MyCV-CAV006)	KAT	CAST	On Demand	Power cycle
AES-KW (MyCV-CAV006)	KAT	CAST	On Demand	Power cycle
SHA2-256 (MyCV-CAV006)	KAT	CAST	On Demand	Power cycle
SHA2-512 (MyCV-CAV006)	KAT	CAST	On Demand	Power cycle
HMAC-SHA2-256 (MyCV-CAV006)	KAT	CAST	On Demand	Power cycle
PBKDF (MyCV-CAV006)	KAT	CAST	On Demand	Power cycle
HMAC DRBG (MyCV-CAV006)	KAT	CAST	On Demand	Power cycle
ENT	Repetition Count and Adaptive Proportion tests as per SP 800-90B	CAST	On Demand	Power cycle
RSA 4096 Signature Verification	Digital Signature Verification	SW/FW Load	On Demand	Power cycle
RSA SigVer (FIPS186-4) (MyCV-CAV006)	KAT	CAST	On Demand	Power cycle

Table 22: Conditional Periodic Information

The operator may initiate an on-demand periodic self-test by power cycling the CM.

10.4 Error States

Name	Description	Conditions	Recovery Method	Indicator
Boot Code Fail Loop State	The module is not operational. Data output is inhibited.	Pre-operational test failure	Power-cycle	The DAS pin will toggle at 8 Hz (0.125s High and 0.125s Low).
MyCV Error State	The module does not provide any security function. Status output is allowed, but data output is inhibited.	Conditional test failure	Power-cycle	The DAS pin will toggle at 1 Hz (1s High and 1s Low).

Table 23: Error States

Boot Code Fail Loop State:
When the module enters Boot Code Fail Loop State, the module can no longer service any host commands, and the Device Activity Signal (DAS) pin will toggle at 8Hz frequency (once per 0.125 second). The DAS signal is high by default.

MyCV Error State:
When the module enters MyCV Error State, the module can no longer service any host commands, and the Device Activity Signal (DAS) pin will toggle at 1Hz frequency (once per second). The DAS signal is high by default.

For different form factors, the assigned DAS PIN number is:
M.2 2280 NVMe NAND FLASH SSD (PIN#10)
U.2 NVMe NAND FLASH SSD (PIN#P11)
E1.S NVMe NAND FLASH SSD (PIN#A10)

10.5 Operator Initiation of Self-Tests [O]

The operator may initiate an on-demand periodic self-test by power cycling the CM.

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

Delivery
The cryptographic module is always shipped to the Crypto Officer in sealed boxes via a commercial bonded carrier. Each box has a tamper-evident label stating, "Once the label is damaged, it is not an original product." The module is shipped from the factory with the required physical security mechanisms in place (e.g., epoxy).

The Crypto Officer should inspect the carton for any irregular tears or openings and check the module itself for signs of tampering (e.g., scratches, tears, etc.) to ensure the module has not been compromised before initialization.

Initialization

The Crypto Officer (Drive Owner) must follow these steps to initialize the cryptographic module into MyCV Approved Mode after receiving the MaiStorage SSD drive. Before configuring the CM to comply with MyCV Approved mode configuration requirements outlined below, it operates in a non-compliant state.

1. Examine the tamper evidence and check that the module has not been tampered.
2. StartSession SID of AdminSP with MSID[1] password and then set new password for SID password. The new password shall be at least 10 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 Step 2 and then set new password for Admin1-4 passwords and User1-9 passwords of LockingSP. The new passwords shall be at least 10 bytes.
6. Configure all LockingRanges of LockingSP by setting ReadLockEnabled and WriteLockEnabled columns to TRUE.
7. Power cycle the module.
8. Check if the module is in MyCV Approved Mode by using the TCG Opal Level 0 Discovery command. This command returns a global indicator at data byte 47, bit 1. If bit 1 is set to 1, it indicates that the cryptographic module is in MyCV Approved Mode.
9. Check the module’s firmware version[2] retrieving bytes 148-155 of the compliance descriptor using the “Show Module Version Information” service. The firmware version must be an approved version as specified in Section 2.2 above.

Note:

1. MSID can be obtained through an unauthenticated command only when the module is in an uninitialized state (fresh out of box). The Crypto Officer (CO) must use the MSID password to log in for the first time and set a new SID password (10 to 32 bytes) that is different from the original MSID password in Step 2.

New firmware versions within the scope of this validation must be validated through MyCV CMV. Any other firmware loaded into this module that is not reflected in section 2.2 above is out of the scope of this validation and requires a separate MyCV validation. After following these steps 1-9 the drive is in the MyCV approved mode of operation, any violation of Section 11.1 or other requirements specified in the Security Policy will place this module in a non-initialized state of operation.

11.2 Administrator Guidance

Periodically examine tamper evidence, if evidence of tamper has been detected then the device must be put out of service and the Crypto Officer (Drive Owner) shall be notified.

When first executing StartSession with the password provided by Crypto Officer (Drive Owner), the Crypto Officer (CO) needs to change to a new password for the CO himself, and the password must contain at least 10 bytes.

The Crypto Officer Guidance Manual_V1.00 provides additional administrator guidance.

11.3 Non-Administrator Guidance

When first executing StartSession with the password which was provided by CO, the user needs to change to a new user password and the password must contain at least 10 bytes.

The User Guidance Manual_V1.00 provides additional administrator guidance.

11.4 Design and Rules [O]

In the MyCV Approved Mode of operation the module shall adhere to the following rules:

1. Operators shall not use passwords less than 10 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 140-3 IG C.I (e.g.: key_1 ≠ key_2).
4. The cryptographic module shall not output CSPs in any form.
5. The cryptographic module enters the MyCV 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-4096 with SHA-512.
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.

Change to the Crypto Officer state from any other role other than the Crypto Officer is prohibited.

11.6 End of Life [O]

When the CM reaches the end of its lifecycle, the Crypto Officer must zeroize all SSPs before discarding the CM. The Crypto Officer shall accomplish this by invoking Return to uninitialized state service and then performing RSA Code Sign Public Key Zeroization services. This process will render the CM inoperable (bricked) upon the next power cycle.

12 Mitigation of Other Attacks

The cryptographic module has not been designed to mitigate any specific attacks beyond the scope of MyCV Level 2.