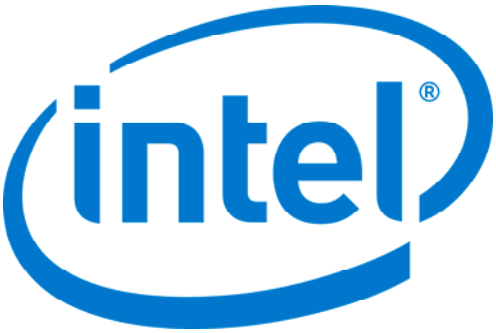

Intel® Optane™ SSD DC D4800X

FIPS 140-2 Non-Proprietary Security Policy

Doc Version: 1.3

Last Updated: August 6, 2020

Table of Contents

List of Tables

List of Figures

Copyrights, Trademarks and Legal Disclaimers

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Performance varies depending on system configuration. No product or component can be absolutely secure. Check with your system manufacturer or retailer or learn more at http://intel.com/ssd

Intel, the Intel logo, and others are trademarks of Intel Corporation or its subsidiaries in the U.S. and/or other countries.

*Other names and brands may be claimed as the property of others.

1. Introduction

This document defines the Security Policy for the Intel® Optane™ SSD DC D4800X module, hereafter denoted the Module. The Module is a PCIe dual-port Gen3 x 2 NVMe SSD with industry leading Intel® Optane™ memory, delivering power-efficient performance with enterprise-ready security and remote manageability capabilities. The Module meets FIPS 140-2 overall Level 2 requirements.

Table 1 – Cryptographic Module Configurations

	Modules	Hardware Part #s and Versions	Tamper-Evident Seals Part #s	Firmware Version
1	Intel® Optane™ SSD DC D4800X 375 GB	SSDPD21K375GAR with J26977-100 rev 2 and J29722-002 rev 7	K33839-001	E201EM0A
2	Intel® Optane™ SSD DC D4800X 750 GB	SSDPD21K750GAR with J26979-100 rev 2 and J29722-002 rev 7		
3	Intel® Optane™ SSD DC D4800X 1.5 TB	SSDPD21K015TAR with J26980-100 rev 2 and J29722-002 rev 7		

The Module is intended for use by US Federal agencies and other markets that require FIPS 140-2 validated Self Encrypting Solid State Drives. The Module is a multi-chip standalone embodiment.

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

Table 2 – Security Level of Security Requirements

Security Requirement	Security Level
Cryptographic Module Specification	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	2
Self-Tests	2
Design Assurance	2
Mitigation of Other Attacks	N/A

The Module implementation is compliant with:

- NVM Express 1.2b:
  - https://nvmexpress.org/wp-content/uploads/NVM_Express_1_2b_20160601-1.pdf
- TCG Opal 2.01:
  - https://trustedcomputinggroup.org/wp-content/uploads/TCG_Storage-Opal_SSC_v2.01_rev1.00.pdf
- NVMe-MI 1.0a:
  - https://nvmexpress.org/wp-content/uploads/NVM_Express_Management_Interface_1_0a_2017.04.08_-_gold.pdf

1.1 Hardware and Physical Cryptographic Boundary

The Module is designed to be embedded in a General Purpose Computer (host) and is connected through the PCIe connector. The physical form of the Module is depicted in Figure 1.

Figure 1 – Module Picture

The cryptographic boundary is defined as the external perimeter of the SSD enclosure represented in Figure 1 – Module Picture.

The physical ports and logical interfaces are identified in Table 3 below:

Table 3 – Ports and Interfaces

Port	Interfaces	Description	Logical Interface Type
PCIe connector	NVMe	NVMe interface	Control in | Data in | Data out | Status out
	UART	Maintenance interface	Data in | Data out | Control in | Status out
	SMBus	Management interface	Control in | Status out
	Power	Power interface	Power

1.1.1 NVMe Interface

The NVMe interface provides the primary interface to interact with the Module. Most services provided by the Module are accessed via the NVMe Interface including Opal configuration, reading and writing user data, retrieving FIPS capability support, and retrieving FIPS status reporting.

1.1.2 UART Interface

The UART interface provides the ability to perform device firmware update, maintenance and retrieve debug logs from the device. This port is available for the Maintenance Role. The UART interface is only exposed outside of the device after successful power on self-tests have been completed.

1.1.3 SMBus Interface

The SMBus interface provides the ability to audit the SSD environment (temperature, Vital Product Data).

1.2 Firmware and Logical Cryptographic Boundary

The Module is composed of the following components:

1. P4800X Controller – The controller ASIC. This component is responsible for terminating PCIe/NVMe commands, reading or writing data to the Host platform, encrypting or decrypting data from the Host platform, and storing or retrieving data to Intel® Optane™ Memory non-volatile memory.
2. AL5 – The PCIe dual-port bridge ASIC. This component is responsible for bridging two PCIe Gen3x2 interfaces into a single PCIe Gen3x4 interface on the storage controller ASIC.
3. DDR – Dynamic RAM. These components are used by the AL5 bridge for temporary storage of data and/or parameters that are needed by the AL5 controller during execution.
4. 3D-XPoint® – non-volatile memory. These components comprise the non-volatile media of the storage device. These components store encrypted user data, firmware for the P4800X controller, and other non-volatile configuration data needed by the P4800X controller during execution.
5. UART Interface – Maintenance interface.
6. PIC – SMBus controller

The Module relies on the PCIe/NVMe interface as input/output devices.

Figure 2 depicts the Module block diagram:

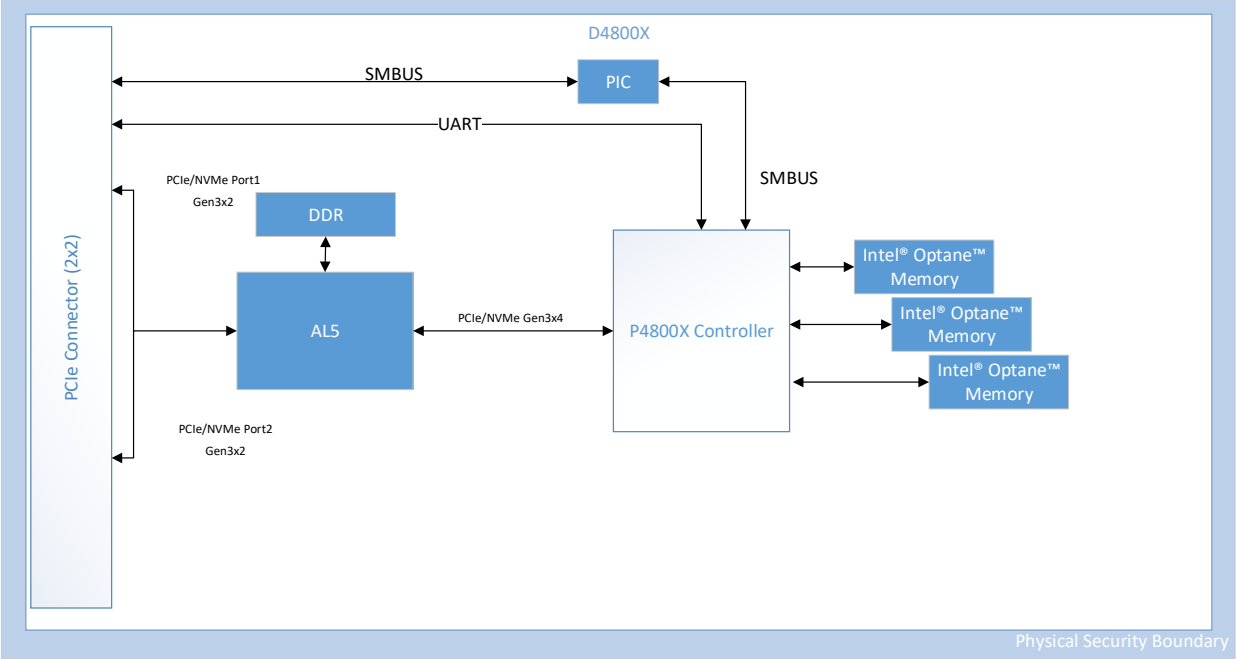

Figure 2 – Module Block Diagram

The PCIe Host is attached to the Module via two PCIe Gen3x2 interfaces supporting 2 lanes each which are bridged by the AL5 ASIC into a single PCIe Gen3x4 interface on the P4800X controller ASIC. The dual PCIe interfaces provide the data input, data output, control and status interface. The NVMe layer handles NVMe 1.2b commands. Some of the NVMe 1.2b commands may be handled by firmware running in the P4800X controller via interrupts to the P4800X controller.

Firmware is located in AL5 and P4800X controller components. AL5 contains neither security relevant implementation, CSPs, nor Public parameters with the exception of the plaintext password that is passed through the AL5 to be processed by the P4800X controller.

1.3 Modes of Operation

The Module ships from the manufacturing facility with either the FIPS Approved firmware identified in Table 1 or a firmware which was not validated.

To determine if a Module is using a FIPS Approved firmware version, the FIPS Compliance Descriptor will be retrieved via the Read FIPS Compliance service and the following information will be verified:

1. Related Standard indicates FIPS 140-2 (2) on byte 13
2. Overall Security Level indicates Level 2 (2) on byte 14
3. Compliance Descriptor Hardware Version (byte 16) matches the HW P/N and Version column of a configuration in Table 1
4. Compliance Descriptor Version (byte 144) matches the FW Version column of a configuration in Table 1
5. Compliance Descriptor Module Name (byte 272) matches the Module column of a configuration in Table 1

When the FIPS firmware is installed, the Module is received in an FIPS uninitialized mode, the user authentication is not enabled and the access to the disk is not set.

When the FIPS firmware is not installed, the user will have to perform the following operations to configure the Module in a FIPS uninitialized mode:

1. Update the firmware with the firmware download verification service to the FIPS approved firmware
2. Reset the Module
3. Enable/Activate Opal
4. Perform an AdminSP Revert method on the AdminSP
5. Apply the tamper-evident seals as shown in Section 5.2.

The Module must be placed into the FIPS approved mode of operation (Initialized) through the following initialization procedure:

1. Taking ownership of Opal by setting the AdminSP SID credential to something other than MSID
2. Activating the LockingSP
3. Setting the WriteLockEnabled and ReadLockEnabled column within the Locking Table of all ranges containing sensitive user data

The CO role is responsible for configuration of other CO roles and User roles as well as enabling locking/unlocking on any of the CO or User role controlled areas (locking ranges). The User roles are responsible for enabling locking/unlocking of the assigned locking ranges as well as performing locking/unlocking of their assigned locking range. In FIPS Approved mode (Initialized), both the CO and User Roles require authentication and unlock prior to allowing access to data, whereas the uninitialized mode does not. The Module will be in non-Approved mode of operation if not initialized.

To discover that a Module is in the FIPS Approved mode of operation (Initialized), the following must be verified:

1. The LockingEnabled bit of the TCG Level 0 Discovery Locking Feature Descriptor is set to 1
2. The ReadLockEnabled column of the Locking Table is set to the True state for all ranges covering sensitive user data

It is possible to switch from the FIPS Approved Initialized mode to uninitialized mode by performing the AdminSP Revert method. However, the Module shall be initialized to be in a FIPS mode of operation.

2 Cryptographic Functionality

The Module implements the *FIPS Approved* and *Non-Approved but Allowed* cryptographic functions listed in the tables below. The terms FIPS Approved and Non-Approved cryptographic functions are defined by FIPS 140-2 specifications.

Table 4 – Approved and CAVP Validated Cryptographic Functions

Algorithm	Description	Cert #
AES	[FIPS 197, SP 800-38F] Functions: underlying cryptographic algorithm of KW (Cert. #C857) Modes: ECB Key sizes: 256 bits	C31
AES	[FIPS 197, SP 800-38F] Functions: Key wrapping and unwrapping Modes: KW Key sizes: 256 bits	C857
AES	[FIPS 197, SP 800-38E] Functions: underlying cryptographic algorithm of AES XTS (Cert. #1431) Modes[1]: ECB Key sizes[1]: 256 bits	617
AES	[FIPS 197, SP 800-38E] Functions: Encryption and Decryption of the data Modes: XTS Key sizes[1]: 256 bits	1431
DRBG	[SP 800-90A] Functions: HMAC DRBG Hash: SHA-256 (Cert. #C31) Security Strengths: 256 bits	C214
HMAC	[FIPS 198-1] Functions: Verification of Firmware on Boot (integrity test) SHA sizes: SHA-256 (Cert. #665)	C32
HMAC	[FIPS 198-1] Functions: Digital Signature Generation (Firmware Download) SHA sizes: SHA-256 (Cert. #665)	C858
HMAC	[FIPS 198-1] Functions: HMAC-DRBG random number generation SHA sizes: SHA-256 (Cert. #C31)	C31

[1] The Module implements only the modes, data size, and key sizes mentioned in the Approved algorithm table.

Algorithm	Description	Cert #
RSA	[FIPS 186-2, ANSI X9.31-1998, and PKCS #1 v2.1 (PKCS1.5)] Functions: Digital Signature Verification (Firmware Download) Key sizes: 2048 bits Hash: SHA-256 (Cert. #C31)	C857
SHS	[FIPS 180-4] Functions: Maintenance Role Password Hash, Digital Signature Generation (Firmware Download), Firmware Integrity test using HMAC SHA sizes[1]: SHA-256	665
SHS	[FIPS 180-4] Functions: Digital Signature Verification (Firmware Download), HMAC DRBG SHA sizes: SHA-256	C31

Table 5 – Approved Cryptographic Functions Tested with Vendor Affirmation

Algorithm	Description	IG Ref.
CKG	[SP 800-133] Section 7.1: Direct symmetric key generation using unmodified DRBG output	Vendor Affirmed IG D.12
Password Based KDF	[SP 800-132] Options: PBKDF with Option 1a Functions: HMAC-based KDF using SHA-256 (Cert. #C 31) Used as part of authentication of User and Cryptographic Officer roles Note: the keys derived from passwords are only used for storage applications.	Vendor Affirmed IG D.6

Table 6 – Non-Approved but Allowed Cryptographic Functions

Algorithm	Description
NDRNG	[Annex C] Hardware Non-Deterministic RNG. The NDRNG provides a seed with a minimum entropy of 256 bits to the FIPS Approved DRBG.
Password Based KDF (no security claimed)	[SP 800-132] HMAC-based KDF with SHA-256. The difference between this algorithm and the Password Based KDF listed in Table 5 is that this version is used for PSID verification only.
Key Based KDF (no security claimed)	[SP800-108] Derivation of the keys used to verify the Firmware Integrity.
AES KW (no security claimed)	[FIPS 197, SP 800-38F] Key storage encryption with a non-Approved AES KW.

The Module does not implement Non-Approved Cryptographic Functions for use in non-FIPS mode.

2.1 Critical Security Parameters

All CSPs used by the Module are described in this section. All usage of these CSPs by the Module (including all CSP lifecycle states) is described in the services detailed in Section 3.3.

Table 7 – Critical Security Parameters (CSPs)

CSP	Description / Usage
DRBG-EI	2048-bit DRBG entropy input
DRBG-State	HMAC_DRBG internal state (V and C)
AdminSPKREK	AdminSP Key Ring Encryption Key, AES-256 key
AdminSPPassword	AdminSP passwords used to authenticate the CO
ASPPKey	AdminSP Key derived from the CO passwords, AES-256 key
MEK	Media Encryption Keys, AES-256 keys
MKEK	Media Key Encryption Keys, AES-256 keys
KREK	Key Ring Encryption Key, AES-256 key
U-Password	Passwords used to authenticate the CO and User
UPKey	Key derived from the CO and User passwords with PBKDF2, AES-256 keys
M-Password	Password used to authenticate the Maintenance role.
REK	Reset Ephemeral Key, AES-256 key

2.2 Public Security Parameters (PSP)

Table 8 – Public Security Parameters

Key	Description / Usage
FW_Pub	2048-bit RSA public Key used to verify the signature of the firmware
PSID	32 bytes value used to call the TCG Revert service
MSID	32 bytes value used to initialize the Module (first authentication)
Salt	PBKDF2 Salt, 20-byte value

3 Roles, Authentication and Services

3.1 Assumption of Roles

The Module supports three distinct operator roles: User, Cryptographic Officer (CO) and Maintenance roles. The cryptographic Module enforces the separation of roles using a credential (named password or PIN) that is provisioned for the administrator (CO) and User roles as part of taking ownership and personalization of the Opal security subsystem. The credential is verified as part of authentication as the specific role during session startup to the Opal Security Subsystem. Access control over configuration mechanisms under control of the administrator is enforced by the Module firmware.

The Maintenance role is entered via authentication of a credential (password). This role grants maintenance and recovery capabilities to the cryptographic Module implementer.

Table 9 lists all operator roles supported by the Module.

The Module does not support concurrent operators. If multiple successful authentications occur in an active session to the Opal security subsystem to multiple roles, modifications are possible to the Opal security subsystem under both roles simultaneously, however, it is assumed that the separation is performed by the human operators and not by the cryptographic Module or the software that is the session owner. Neither the administrator credential nor user credential are discoverable/readable through the Opal Security Subsystem, regardless of the active authentication state in the session.

Table 9 – Roles Description

Role ID	Role Description	Authentication Type	Authentication Data
CO	Cryptographic Officer – - Opal Locking SP Admin Authorities (4) - Opal AdminSP Admin and SID Authorities (2) - Ability to configure start addresses and encryption within the Module (locking ranges) - Ability to provide user roles with the ability to enable/disable locking on a locking range - Ability to enable/disable locking on a locking range - Ability to cryptographically erase a locking range - Ability to move from FIPS Approved Initialized Mode to FIPS Approved Uninitialized mode through AdminSP Revert	Role-based	14-byte to 32-byte password (U-Password) 5 attempts are possible before requiring a power on reset of the storage device
User	User – - Opal Locking SP User Authorities (8) - Ability to enable/disable locking on a locking range - Ability to cryptographically erase a locking range	Role-based	14-byte to 32-byte password (U-Password) 5 attempts are possible before requiring a power on reset of the storage device

Role ID	Role Description	Authentication Type	Authentication Data
Maintenance	Maintenance role - Ability to recover debug logs - Ability to bring device to healthy state when otherwise non-functional - Ability to load authenticated firmware into the Module	Role-based	14-byte to 32-byte password (M-password) 5 attempts are possible before requiring a power on reset of the storage device.

Table 10 – Unauthenticated Roles

Role ID	Role Description	Public Authentication Data (if present)
PSID	PSID role – - PSID Authority - Ability to move from FIPS Approved Initialized Mode to FIPS Approved Uninitialized mode through AdminSP Revert which also causes Zeroization of all CSPs	32-byte value (written on the Module) 5 attempts are possible before requiring a power on reset of the storage device
Anybody	User – - Ability to read MSID - Ability to read all configuration data in AdminSP and LockingSP tables (except for PIN values)	N/A

3.2 Authentication Methods

3.2.1 CO and User Password/PIN Authentication Method

The Module supports a maximum of 4 admin users (CO) and 9 individual users (8 locking ranges plus one global range as defined by [TCG-OPAL]. Each user may insert a unique password/PIN in order to authenticate to the Module and act on the Module in that role. The password/PIN length must be at least 14 bytes, see Security Rules and Guidance.

Thus, the probability of guessing a password/PIN in a single attempt is 1/2^112(=2^14 * 8) when the password is randomly chosen which is smaller than 1/10^6.

The Module enforces a count based access protection mechanism that supports at most 5 password authentication attempts per second. After 5 consecutive unsuccessful password validation attempts have occurred, the Module requires a reset before any more login attempts can be attempted. The reset time required in performing a reset to the Module is one second. Therefore, 5 * 30 = 150 password attempts may be executed in one minute where the overall search space is 2^112 leaving a false acceptance probability in one minute of 150/2^112, which is smaller than 1/10^5 as required for FIPS 140-2.

The password/PIN is received in plaintext by the Module and the Module passes the password through the PBKDF2 algorithm with 20 bytes of salt in order to derive the CO and the User CSPs to access the media.

3.2.2 Maintenance Password Authentication Method

This authentication method is used to verify the maintenance role as part of the maintenance unlock mechanism. The user must insert a password in order to authenticate as the maintenance role.

The Maintenance role password length is at least 14 bytes, see Security Rules and Guidance.

Thus, the probability of guessing a password in a single attempt is 1/2^112 which is smaller than 1/10^6.

The Module enforces a count based access protection mechanism that supports at most 5 password authentication attempts per second. After 5 consecutive unsuccessful password validation attempts have occurred, the Module requires a reset before any more login attempts can be attempted. The reset time required in performing a reset to the Module is one second. Therefore, 150(=30 * 5) password attempts may be executed in one minute where the overall search space is 2^112 leaving a false acceptance probability in one minute of 150/2^112, which is smaller than 1/10^5 as required for FIPS 140-2.

The password is received in plaintext by the Module.

3.3 Services

All services implemented by the Module are listed in Table 11 and Table 12 below. Each service description also describes all usage of CSPs by the service. The service names highlighted in bold in Table 11 and Table 12 can be called in the uninitialized mode.

Note:

- CO = Cryptographic Officer Role
- U = User Role
- FM = Maintenance Role

Table 11 – Authenticated Services

Service	Description	CO	U	FM
Take Ownership	Sets the SID credential to something other than MSID	X		
Data Encryption/Decryption	Protects access to the Media Encryption Keys stored in the Module in ciphertext form. The cryptographic officer or user password is used to generate an intermediate key (Pkey) which is used to unwrap a Key Ring Encryption Key which is then used to unwrap the Media Key Encryption Key which is then used to unwrap the Media Encryption Key.	X	X	
Enable/Disable of Opal (FIPS Approved, Initialized Mode)	Enable through TCG Activate/Disable Opal through AdminSP or LockingSP Revert	X		
Change admin password	Change any password in AdminSP	X		
Zeroize/AdminSP Revert	Destroy user data (TCG Revert)	X		
Disable authorities	Disable authorities to make them invalid and no longer able to authenticate to the drive.	X		
Configure Locking Ranges	Configure locking ranges in the CM.	X		

Service	Description	CO	U	FM
Configure MBR Shadow	Configure/Enable MBR Shadow and write data into the MBR shadow area	X		
Set MBR Shadow	Write data into the MBR Shadow area	X		
Change any password in Admin/Locking SP	Change any password in Locking SP	X		
Format NVM/Sanitize/GenKey	Destroy any data (changing key)	X		
TCG RevertSP and keep data	Revert and keep data. Reset all configuration data in the locking SP but do not destroy user data in the Global Range.	X		
Set data store	Set data store – write data into the Opal data store tables.	X		
Configure Access Control	Change which entity can manage/lock/unlock an encryption range.	X		
Lock, unlock ranges	Lock, unlock ranges from access to read/writes on the data input/output interface	X	X	
Set common name – Locking SP if allowed by Locking SP Admin	If the Locking SP Administrator allows, change the common name to reflect different text in the Locking SP		X	
Set data store if allowed by Locking SP Admin	If Locking SP Administrator allows, change data in the data store tables		X	
FW Maintenance	Retrieve FW Maintenance Logs, recover device from non-functional state			X
Maintenance FW update	The Module allows the firmware to be updated through a vendor unique command in the event of a firmware failure. This authentication mechanism is used to verify the firmware using RSASSA-PKCS1-v1.5 signature verification with SHA256 and an internal public key.			X

Table 12 – Unauthenticated Services

Service	Description
Module Reset (Self-test)	Reset the Module by power cycle, or PERST#. Performs self-tests, firmware integrity check.
Warm Reset	Reset the Module by performing an NVMe Subsystem Reset.
Hot Reset	Reset one of the ports of the Module by performing a PCIe Hot Reset.
Read of configuration (show status)	Opening a session as Anybody does not require authentication. During an active session in this state, the CM will provide Status/Level 0 Discovery information, the version number, and Opal security configuration. This will be invoked during the FIPS Approved Mode check.
Read of FIPS Compliance	Read FIPS 140 compliance descriptor as defined in [SFSC]

Service	Description
NVMe Firmware download verification	The Module allows the firmware to be updated through the NVMe Firmware Download and Commit commands. This authentication mechanism is used to verify the firmware using RSASSA-PKCS1-v1.5 signature verification with SHA256 and FW_Pub.
Zeroization/PSID Revert	Destroys all CSPs after PSID verification
NVMe-MI Basic Management Command	Retrieves drive status (status flags, SMART warnings, temperature, VID, serial number, etc.)
User/Admin Authentication (start session)	Authenticates a user using a TCG credential
FW Maintenance unlock	The Module authenticates the maintenance role using a password that is input in plaintext and upon successful authentication, maintenance capabilities are unlocked.
Random	Generate a random number and return it to the caller of the method.
Recovery	Reinitialize the Module if a non-recoverable error occurs. The Module will transition to uninitialized state.
Telemetry	The Module allows the collection of debugging information through NVMe log pages – host initiated telemetry log page and controller initiated log page. The purpose of the telemetry log data is to provide information required to debug firmware issues remotely.

Table 13 defines the relationship between access to CSPs and the different Module services. The modes of access shown in the table are defined as:

- G = Generate: The Module generates the CSP.
- G' = Generate: The Module generates the CSP – unless the CSP is the Global Range MEK, in which case it is not destroyed, but preserved through the service.
- R = Read: The Module reads the CSP. The read access is typically performed before the Module uses the CSP.
- E = Execute: The Module executes using the CSP.
- W = Write: The Module writes the CSP. The write access is typically performed after a CSP is imported into the Module, when the Module generates a CSP, or when the Module overwrites an existing CSP.
- Z = Zeroize: The Module zeroizes plaintext and ciphertext CSPs.
- Z' = Plaintext Zeroize: The Module zeroizes all plaintext instances of the CSP from memory, if present

Table 13 – CSPs and PSPs Access Rights within Services

Services	CSPs												PSPs			
	DRBG-EI	DRBG-State	AdminSPKREK	AdminSPPassword	ASPPKey	MEK	MKEK	KREK	U-Password	UPKey	M-Password	REK	FW_Pub	PSID	MSID	Salt
Unauthenticated																
Module Reset	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z/G	--	--	--	Z
Warm Reset	Z	Z	--	Z	Z	--	--	--	Z	Z	Z	R/E	--	--	--	--
Hot Reset	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Read of configuration (Show status)	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Read of FIPS Compliance	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
NVMe Firmware download verification	--	--	--	--	--	--	--	--	--	--	--	--	R/E	--	--	--
Zeroization/PSID Revert	--	--	Z	--	--	Z	Z	Z	--	--	--	--	--	R	--	Z
NVMe-MI Basic Management Command	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
User/Admin Authentication (start session)	--	--	R/E	R/E/Z	G/E/Z	R/E	R/E	R/E	R/E/Z	G/E/Z	--	R/E	--	--	--	R/E
FW Maintenance unlock	Z'	Z'	Z'	Z'	Z'	Z'	Z'	Z'	Z'	Z'	E/Z'	Z'	--	--	--	--
Random	G/R/E/W	R/E/W	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Recovery	G/R/E/W	R/E/W	Z	--	--	Z	Z	Z	--	--	--	Z	--	R	--	Z
Telemetry	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Authenticated																
Take Ownership	G/R/E/W	R/E/W	G/E/W	R/E/Z	R/E	--	--	G/E/W	R/E/Z	R/E	--	--	--	--	R/E	G/E/W
Data Encryption/Decryption	--	--	--	--	--	R/E	--	--	--	--	--	--	--	--	--	--
Enable/Disable of Opal	G/R/E/W	R/E/W	R/E	--	G/E	--	--	R/E	--	G/E	--	--	--	--	--	G/R/E/W

Services	CSPs												PSPs			
	DRBG-EI	DRBG-State	AdminSPKREK	AdminSPPassword	ASPPKey	MEK	MKEK	KREK	U-Password	UPKey	M-Password	REK	FW_Pub	PSID	MSID	Salt
Change admin password	GREW	REW	RE	RE	GE	--	--	REW	--	--	--	--	--	--	--	GE
Zeroize/AdminSP Revert	G/R/E/W	R/E/W	Z	--	G/E	Z	Z	Z	--	G/E	--	--	--	--	--	Z
Disable authorities	--	--	GW	--	--	--	--	GW	--	--	--	--	--	--	--	--
Configure Locking Ranges	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Configure MBR Shadow	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Set MBR Shadow	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Change any password in Admin/Locking SP	G/R/E/W	R/E/W	G/E/W	R/E/Z	G/E	--	--	G/E/W	R/E/Z	G/E	--	--	--	--	--	G/R/E/W
Format NVM/Sanitize/GenKey	G/R/E/W	R/E/W	--	--	--	G/W	R/E	--	--	--	--	--	--	--	--	--
TCG RevertSP and keep data	G/R/E/W	R/E/W	--	--	--	G'/Z	G'/Z	Z	--	--	--	--	--	--	--	Z
Set data store	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Configure Access Control	--	--	R/E	--	--	--	R/W	R/E	--	--	--	--	--	--	--	--
Lock, unlock ranges	--	--	R/E	--	G/E	R	R/E	R/E	--	G/E	--	--	--	--	--	--
Set common name – Locking SP if allowed by Locking SP Admin	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Set data store if allowed by Locking SP Admin	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
FW Maintenance	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Maintenance FW update	--	--	--	--	--	--	--	--	--	--	--	--	R/E	--	--	--

4 Self-Tests

Each time the Module is powered up, it tests that the cryptographic algorithms still operate correctly and that sensitive data have not been damaged. Power up self–tests are available on demand by power cycling the Module.

On power up or reset, the Module performs the self-tests described in Table 14 below. All KATs must be completed successfully prior to any other use of cryptography by the Module. If one of the KATs fails, the Module enters an internal error state if the failure is during the ROM boot stage of the device. If the device has exited the ROM boot stage, the Module enters a soft error state requiring reset of the Module.

Table 14 – Power Up Self-tests

Test Target	Description
Firmware Integrity	HMAC-SHA256 (Cert. #C32) (used to verify all firmware upon boot from internal media on the P4800X controller). 32-bit modular sum (used to verify all firmware upon boot from internal media on the AL5 ASIC)
AES-KW	KATs: Encryption, Decryption Modes: KW Key sizes: 256 bits
AES-XTS	KATs: Encryption, Decryption Key sizes: 256 bits
AES-ECB (Cert. #617)	KATs: Encryption, Decryption as part of AES-XTS KAT Key sizes: 256 bits
AES-ECB (Cert. #C31)	KATs: Encryption, Decryption as part of AES-KW KAT Key sizes: 256 bits
DRBG	KATs: HMAC DRBG (inclusive of instantiate, generate and reseed) Mode: HMAC SHA-256 Security Strengths: 256 bits
HMAC (Cert. #C32)	KATs: Verification as part of Firmware Integrity test SHA sizes: SHA-256
HMAC (Cert. #C31)	KATs: Generation as part of DRBG KAT SHA sizes: SHA-256
HMAC (Cert. #C858)	KATs: Generation, Verification SHA sizes: SHA-256
RSA (Cert. #C857)	KATs: Signature Verification with SHA-256 (Cert. #C31) Key sizes: 2048 bits
SHA (Cert. #665)	KATs: SHA-256 as part of HMAC KAT (Cert. #C858) and Firmware Integrity
SHA (Cert. #C31)	KATs: SHA-256 as part of RSA KAT

Table 15 – Conditional Self-tests

Test Target	Description
NDRNG	NDRNG Continuous Test performed when a random value is requested from the NDRNG.
Firmware load test	Firmware signature verification based on RSA PKCS#1 v1.5 with SHA-256 and 2048-bit key

If a self-test failed, the Module will indicate the following information:

- Firmware integrity: the SSD will not enumerate
- KAT: the SSD NVMe Identify service will return 1 at offset 4010
- Firmware upload: the SSD will return Invalid Image
- NDRNG: the SSD NVMe Identify service will return 1 at offset 4010

During the Initialization period, the Module can send to the host the NVMe SSD driver to allow the host to communicate with the SSD after the POST.

5 Physical Security

5.1 Physical Security Policy

The following physical security mechanisms are implemented in the cryptographic Module:

- The Module consists of production-grade components enclosed in an aluminum alloy enclosure, which is opaque within the visible spectrum. The enclosure contains two parts: a top and bottom part that affix together through the use of a hinge on the back side of the Module and two screws that affix the top to the bottom near the PCIe edge connector.
- Two (2) tamper-evident seals (one large and one small) are affixed to the front of the Module such that if the Module top and bottom are separated, exposing the internals of the Module, that the tamper-evident seals will be broken in the process. The position of the two tamper-evident seals is indicated in Figure 3. The two tamper-evident seals are captured as part of one part number that is listed in Table 1.

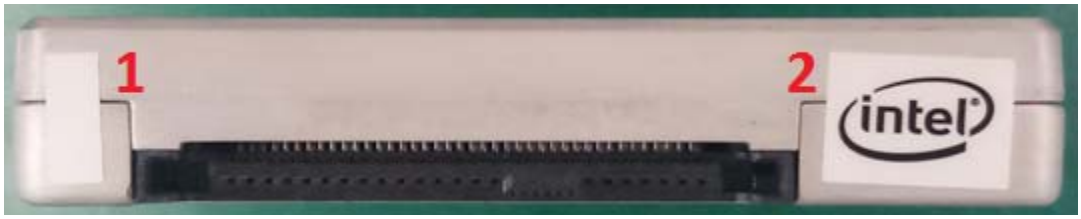

Figure 3 – Module Physical Enclosure - Front

Figure 4 – Module Physical Enclosure - Isometric

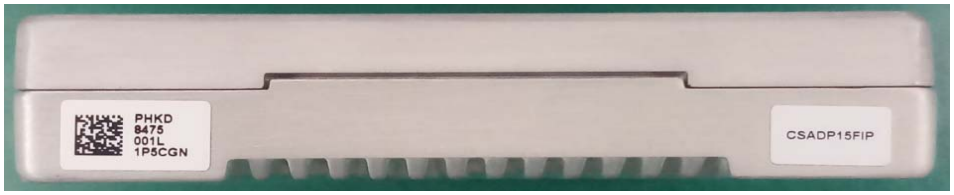

Figure 5 – Module Physical Enclosure - Back

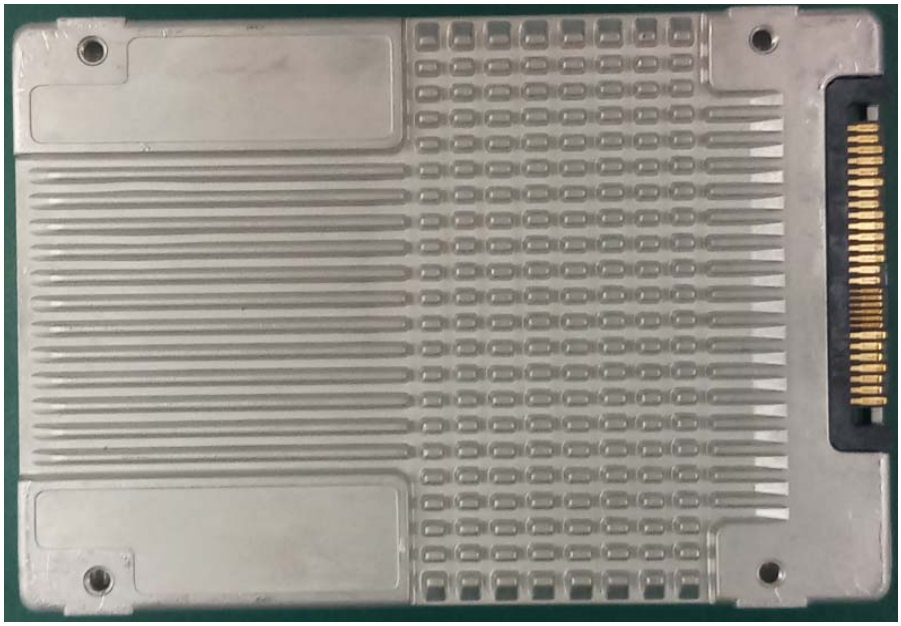

Figure 6 – Module Physical Enclosure - Bottom

The following table summarizes the actions required by the Cryptographic Officer Role to ensure that physical security is maintained:

Table 16 – Physical Security Inspection Guidelines

Physical Security Mechanism	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Production grade cases	On initial receipt of the device and when feasible afterwards.	Inspect the entire perimeter for cracks, gouges, lack of enclosure, bent clips, and other signs of tampering. Remove from service if tampering found.
Tamper-evident Sealing Labels		Inspect the sealing labels for scratches, gouges, cuts and other signs of tampering. Remove from service if tampering found.

5.2 Applying Tamper-Evident Seals for SSDs shipped in FIPS Non-Approved Mode

Modules shipped in FIPS Non-Approved mode may not include the required tamper-evident seals. The tamper-evident seals must be installed for the Module to operate in a FIPS Approved mode of operation.

In such a case, follow the procedure below to apply the provided seals/labels to the Module:

1. Clean surface where tamper-evident seals are to be placed:
   a. Use isopropyl alcohol of equivalent solution to remove any contaminants from the enclosure seam seal/label location.
   b. Handle drive and seal/label with gloves.
2. There are two different size seals with a designated location for each seal. The larger seal is applied to the right front of the Module; the smaller seal on the left front (see Figure 3).
3. Use tweezers to lift seal/label from liner and place in designated area of enclosure seam, as shown in Figure 8.
4. Apply finger pressure to seal/label pressing out any air or lifted edges.

Figure 7 – Applying Tamper-Evident Seals

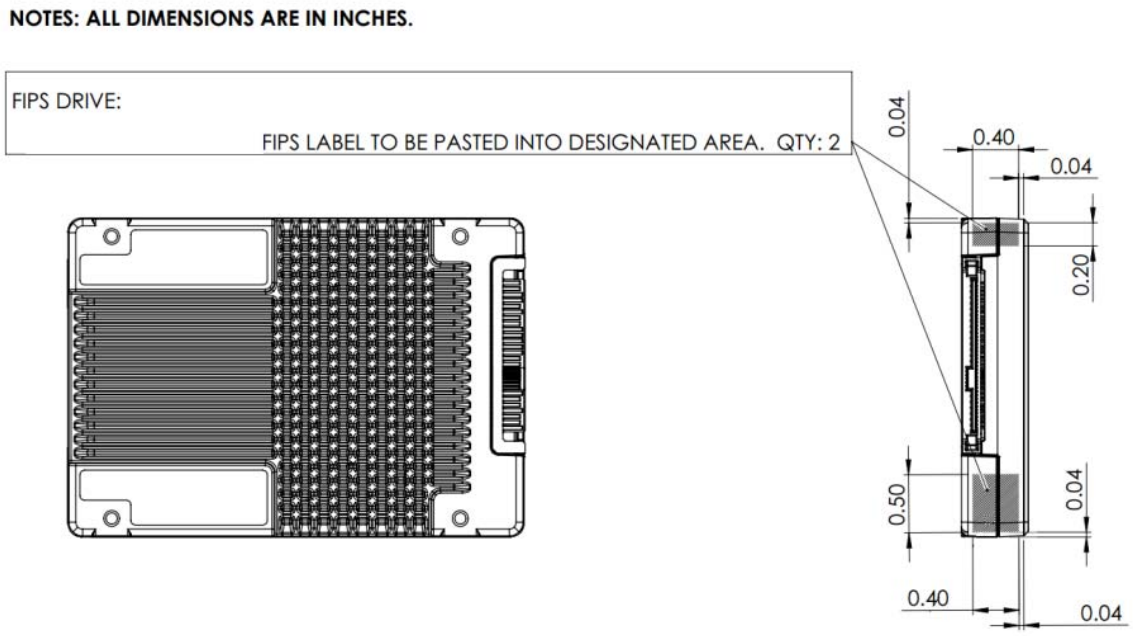

Figure 8 – Tamper-Evident Seal Application Locations

6 Operational Environment

The Module is designated as a non-modifiable operational environment under the FIPS 140-2 definitions. The Module includes a firmware load service to support necessary updates. The Module will not load or execute firmware which is not signed with Intel 2048-bit RSA private key. The mechanisms available to perform a firmware load are the following:

1. Through NVMe using NVMe Firmware Download and Commit operations
2. Through UART/NVMe after entering the Maintenance role

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 is out of the scope of this validation and require a separate FIPS 140-2 validation.

7 Mitigation of Other Attacks Policy

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

8 Security Rules and Guidance

The Module design corresponds to the Module security rules. This section documents the security rules enforced by the cryptographic Module to implement the security requirements of this FIPS 140-2 Level 2 Module.

1. The Module shall provide three distinct operator roles: Maintenance, User and Cryptographic Officer.
2. The Module shall provide role-based authentication.
3. The Module shall clear previous authentications on power cycle.
4. When the Module has not been placed in a valid role, the operator shall not have access to any cryptographic services.
5. The operator shall be capable of commanding the Module to perform the power up self-tests by cycling power or resetting the Module.
6. Power up self-tests do not require any operator action.
7. Data output shall be inhibited during key generation, self-tests, zeroization, and error states.
8. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the Module.
9. There are no restrictions on which keys or CSPs are zeroized by the zeroization service.
10. The Module does not support concurrent operators.
11. The Module does not support manual key entry.
12. The Module does have external input/output devices used for entry/output of data.
13. The Module does not output plaintext CSPs.
14. The Module does not output intermediate key values.
15. The Module does not support a bypass capability service.
16. The Module does not support the update of the logical serial number or vendor ID.

This section documents the security rules imposed by the vendor.

1. The operator is capable of commanding the Module to perform the power up self-tests by cycling power or resetting the Module.
2. The shipping container protecting the Module or set of Modules in transit should be verified for evidence of tampering.
3. If the Module is shipped from the factory with the FIPS firmware installed and uninitialized (TCG Opal is in a manufactured inactive state), the following step will have to be followed. On receipt of the Module, the CO should examine the product to ensure it has not been tampered with during shipping according to the procedures outlined in Section 5. Upon verification that the Module has not been tampered, the user should initialize the Module as described in Section 1.3.

4. If the Module is shipped with the FIPS firmware not installed, labels will need to be applied as described in Section 5 and then the Module must be initialized as described in Section 1.3.
5. The Module CSPs may be zeroized by calling the Revert method on the AdminSP in the Opal interface of the cryptographic Module.
6. The Module shall be zeroized through “Module Reset” prior to performing a Maintenance operation.
7. The Module shall be zeroized using the service: “Module Reset” and “Zeroize/Destroy User Data through TCG Revert” after performing a Maintenance operation. The operator shall follow the procedure contained in “Intel_Optane_SSD_DC_D4800X_Procedure_To_Exit_Maintenance_Mode.pdf” - Version 1.0 to exit the maintenance mode."
8. The password length must be greater than 14 bytes.

9 References and Definitions

The following standards are referred to in this Security Policy.

Table 17 – References

Abbreviation	Full Specification Name
[FIPS140-2]	Security Requirements for Cryptographic Modules, May 25, 2001
[SP800-131Arev1]	Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths, November 2015
[TCG-OPAL]	Storage Work Group Storage Security Subsystem Class: Opal, Version 2.01 Final, Revision 1.00
[SFSC]	Information technology – Security Features for SCSI Commands (SFSC)

Table 18 – Acronyms and Definitions

Acronym	Definition
ASCII	American Standard Code for Information Interchange
AES	Advanced Encryption Standard
CBC	Cipher Block Chain mode of AES encryption/decryption
CO	Cryptographic Officer
CSP	Critical Security Parameters
DRBG	Deterministic Random Bit Generator
ECB	Electronic Code Book mode of AES encryption/decryption
KAT	Known Answer Test
KBKDF	Key Based Key Derivation Function
KDF	Key Derivation Function
MSID	Manufactured SID, Public value that is used as default password
NVMe	Non-Volatile Memory express
PBKDF	Password Based Key Derivation Function
PCIe	Peripheral Component Interconnect express
POST	Power On Self-Test
PSID	Physical SID, a public unique value for each drive
RSA	Rivest Shamir Adleman
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
SID	Secure ID
TCG	Trusted Computing Group
XTS	**X**EX **T**weakable Block Cipher with Ciphertext **S**tealing