Solidigm® Corporation

Solidigm® P5520 SSD (ADP-RR)

FIPS 140-3 Cryptographic Module
Non-Proprietary Security Policy

Version: 1.2

Date: October 18, 2024

Prepared by:

www.acumensecurity.net

Table of Contents

List of Tables

List of Figures

Copyrights and Trademarks

About FIPS 140-3

Federal Information Processing Standards Publication 140-3 — Security Requirements for Cryptographic Modules specifies requirements for cryptographic modules to be deployed in a sensitive but unclassified environment. The National Institute of Standards and Technology (NIST) and Canadian Centre for Cyber Security (CCCS) oversees the Cryptographic Module Validation Program (CMVP). The NVLAP accredits independent testing labs to perform FIPS 140-3 testing and the CMVP validates modules meeting FIPS 140-3 compliance. Validated is the term given to a module that is documented and tested against the FIPS 140-3 criteria.

More information is available on the CMVP website at:
https://csrc.nist.gov/projects/cryptographic-module-validation-program

About this Document

This non-proprietary Cryptographic Module Security Policy for the Solidigm® P5520 Solid State Drive (SSD) (ADP-RR) provides an overview of the product and a high-level description of how it meets the overall Level Security Level 2 security requirements of FIPS 140-3.

The Solidigm® P5520 SSD (ADP-RR) may also be referred to as the “module”, “ADP-RR”, or simply the “drive” in this document.

Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design, and manufacturing. Solidigm® shall have no liability for any error or damages of any kind resulting from the use of this document.

Notices

1. General

1.1 Scope

This document describes the cryptographic module security policy for the Solidigm® P5520 SSD (ADP-RR), Hardware and Firmware versions described in Table 2. It contains specification of the security rules, under which the cryptographic module operates, including the security rules derived from the requirements of the FIPS 140-3 standard.

1.2 Overview

The Solidigm® P5520 SSD (ADP-RR) is a hardware module in a multi-chip embedded embodiment which provides data-at-rest protection, using AES-XTS-256 to encrypt user data prior to being written to media. Authentication and access controls in the module are provided by the Opal Storage Specification (v2.01) by the Trusted Computing Group Storage Workgroup. The module is designed to be installed in a data center environment configured as a Single Port NVMe storage device.

The following table lists the level of validation for each area in FIPS 140-3:

ISO/IEC 24759 Section 6 [Number Below]	FIPS 140-3 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

Table 1 - Security Levels

The module meets the overall Security Level 2 requirements.

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

2. Cryptographic Module Specification

The multi-chip embedded Module, pictured below in Figure 1, is intended for use by US Federal agencies and other markets that require FIPS 140-3 validated Self Encrypting Solid State Disks.

Figure 1 – U.2 Module Picture (Intel Branding)

Figure 2 – U.2 Module Picture (Solidigm Branding)

Figure 3- E1.L Module Picture (Top Side with secured black latch)

Figure 4 - E1.L Module Picture (Bottom Side with secured black latch with Intel Branding)

The cryptographic boundary is defined as the external perimeter of the SSD enclosure represented in Figures 1-4. Figure 5 below shows the module block diagram where the red dotted line depicts the module's physical perimeter.

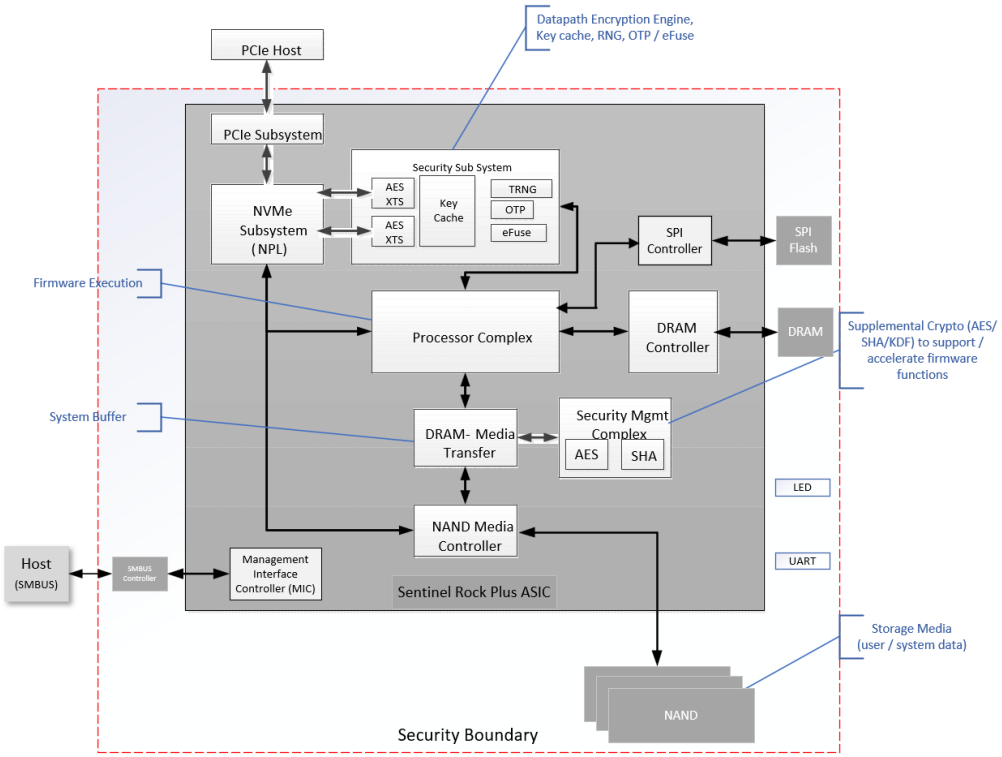

Figure 5 – Module Block Diagram

2.1 Tested Configurations

The module was tested in two different form factors (U.2 and E1.L), each with two different capacities.

Model	Hardware [Part Number and Version]	Firmware Version	Distinguishing Features
Solidigm® P5520 SSD	P/N: SSDPF2KX019T1T Ver: M16410-10005 with TEL P/N: M52551-001	1.3.0	U.2 15mm drive in 1920GB capacity
	P/N: SSDPF2KX038T1T Ver: M16414-10005 with TEL P/N: M52551-001	1.3.0	U.2 15mm drive in 3840GB capacity
	P/N: SSDPF2KX076T1T Ver: M16427-10005 with TEL P/N: M52551-001	1.3.0	U.2 15mm drive in 7680GB capacity
	P/N: SSDPF2KX153T1T Ver: M17283-10010 with TEL P/N: M52551-001	1.3.0	U.2 15mm drive in 15360GB capacity
	P/N: SSDPF2KE016T1T Ver: M16410-10005 with TEL P/N: M52551-001	1.3.0	U.2 15mm drive in 1600GB capacity
	P/N: SSDPF2KE032T1T Ver: M16414-10005 with TEL P/N: M52551-001	1.3.0	U.2 15mm drive in 3200GB capacity
	P/N: SSDPF2KE064T1T Ver: M16427-10005 with TEL P/N: M52551-001	1.3.0	U.2 15mm drive in 6400GB capacity
	P/N: SSDPF2KE128T1T Ver: M17283-10010 with TEL P/N: M52551-001	1.3.0	U.2 15mm in 12800GB capacity
	P/N: SSDPFWKX153T1D Ver: M21006-10101 with TEL P/N: M45818-002 and Latch P/N: AA0015502	9CV1MA90	E1.L 9.5 mm drive in 15360GB capacity

Table 2 - Cryptographic Module Tested Configuration

2.2 Algorithms

The Module implements the Approved cryptographic functions listed in the table below.

CAVP Cert[1]	Algorithm and Standard	Mode/Method	Description / Key Size(s) / Key Strength(s)	Use / Function
A2881	AES [FIPS 197, SP 800-38A]	ECB	256 bits	Encryption and Decryption of encryption Keys
A2881	AES [FIPS 197, SP 800-38F]	KW	256 bits	Encryption and Decryption of the Keys for key storage
A2879	AES [FIPS 197, SP 800-38A, SP 800-38E]	XTS, ECB[2]	256 bits	XTS Encryption and Decryption operations within storage applications
Vendor Affirmed IG D.H	CKG [SP 800-133, rev 2]	Section 4, 6.1, 6.2	256 bits	Direct seed and symmetric key generation using unmodified DRBG output
A2881	DRBG [SP 800-90A, rev 1]	HMAC_DRBG	256 bits	Generate random bits used to create cryptographic keys
ENT	ENT (P) [SP 800-90B]	Physical entropy source		Entropy Source Broadcom TRNG
A2881	HMAC [FIPS 198-1]	HMAC-SHA2-256	256 bits	HMAC-DRBG, KBKDF, KDF
A2881	KBKDF [SP 800-108, rev 1]	Counter Mode	256 bits	Used to derive symmetric encryption keys used internal to the drive
A2881	PBKDF [SP 800-132]	KDF with Option 1a - HMAC-based KDF using SHA2-256 -10,000[3] iteration count	256 bits	Used as part of authentication of Cryptographic Officer role **Note:** The keys derived from passwords are only used for storage applications
A2880	RSA [FIPS 186-4 and PKCS #1 v2.1 (PKCS1.5)]	sigVer PKCS1.5 with SHA2-256	2048 bits	Digital Signature Verification (Firmware Integrity test)
A2881	RSA [FIPS 186-4 and PKCS #1 v2.1 (PKCS1.5)]	sigVer PKCS1.5 with SHA2-256	2048 bits	Digital Signature Verification (Firmware Download, Maintenance authentication)
A2880	SHS [FIPS 180-4]	SHA2-256	N/A	Hashing for Digital Signature Verification for the integrity test
A2881	SHS [FIPS 180-4]	SHA2-256	N/A	Hashing for Digital Signature Verification, HMAC DRBG, Key Based-KDF operations

Table 3 – Approved Algorithms

[1] This table includes vendor-affirmed algorithms that are approved but CAVP testing is not yet available.
[2] ECB is only supported as a prerequisite for XTS and is not directly used by the module.
[3] The iteration count of 10,000 was chosen for security strength and performance.

Algorithm	Caveat	Use/Function
AES-CTR (non-compliant)	Used for added protection of stored keys but is not required for security	Used to wrap key data (Encrypted Key Blob) using a non-SSP. Note, this algorithm was CAVP tested but is not used in a way that claims security.

Table 4 - Non-Approved Algorithms Allowed in the Approved Mode of Operation with No Security Claimed

The module does not implement any of the following algorithms:

- Non-Approved Algorithms Allowed in the Approved Mode of Operation
- Non-Approved Algorithms Not Allowed in the Approved Mode of Operation

2.3 Cryptographic Boundary

The cryptographic boundary is defined as the external perimeter of the SSD enclosure and is composed of the following components:

1. Sentinel Rock Plus ASIC (C0 stepping) – The storage 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 NAND non-volatile memory.
2. DRAM – Dynamic RAM.
3. NAND – non-volatile memory. These components comprise the non-volatile media of the storage device. These components store encrypted user data, firmware for the P5520, and other non-volatile configuration data needed by the ASIC controller during execution.
4. MIC – SMBus controller

The Module relies on the PCIe/NVMe interface as input/output devices. Two capacitors within the module boundary are excluded from the FIPS 140-3 requirements. The exclusion of these components does not affect the security of the module.

2.4 Approved Mode of Operation

The Module ships from the manufacturing facility with either the Approved firmware identified in Table 2 or a firmware which has not been validated.

To determine if a module is using an Approved firmware version, the Compliance Descriptor will be retrieved via the Read Compliance (show status) service and the following information will be verified (Note: Byte references below are from a starting index of zero):

1. Related Standard indicates FIPS 140-3 (3) 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 2.

4. Compliance Descriptor Version (byte 144) matches the FW Version column of a configuration in Table 2.
5. Compliance Descriptor Module Name (byte 272) matches the Module column of a configuration in Table 2.

When the Approved firmware is installed, the module is in an uninitialized state and user authentication is not enabled.

When the Approved firmware is not installed, the Cryptographic Officer will have to perform the following procedure to transition the module to an uninitialized state:

1. Update the firmware with the Firmware Update service to the Approved firmware
2. Reset the module
3. Enable/Activate Opal
4. Perform an AdminSP Revert method on the AdminSP

Once in the uninitialized state, the Module must be placed into the 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 (default password)
2. Activating the LockingSP
3. Setting the WriteLockEnabled and ReadLockEnabled column within the Locking Table of all ranges containing sensitive user data via the Lock, Unlock Ranges service.
4. Power cycle the drive or set the WriteLock and ReadLock columns to True within the Locking Table of all ranges containing sensitive user data.

The CO role is responsible for configuration of other CO and user roles as well as enabling locking/unlocking of any of the CO 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 Approved mode (Initialized), the CO Role requires authentication and unlock prior to allowing access to data, whereas the uninitialized mode does not. The module will be in a non-compliant state if not initialized.

To determine if a Module is in the 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. Minimally, 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 Initialized state to an uninitialized state by performing the AdminSP Revert service. However, the module shall be initialized to be in an Approved mode of operation before any User accesses the Module and calls any services different than those described in this section's instructions.

2.5 Rules of Module Operation

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 140-3 Level 2 Module.

1. The Module shall provide three distinct operator roles: Cryptographic Officer, User, and Maintenance.
2. The Module shall provide role-based authentication.
3. The Module shall clear previous authentications on power cycle.
4. If an operator has not been successfully authenticated, no cryptographic services are available to the operator.
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. Control Input and Data output shall be inhibited during self-tests and error states.
8. Data output shall be logically disconnected during key generation and zeroization.
9. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the Module.
10. There are no restrictions on which keys or CSPs are zeroized by the zeroization service.
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.

The following 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 tamper evidence.
3. If the Module is shipped from the factory with the Approved firmware installed and uninitialized (TCG Opal is in a manufactured inactive state), the steps in section 2.4 will have to be followed.
4. If the module is shipped with the Approved firmware not installed, seals will need to be applied as described in Section 7 and then the module must be initialized as described in Section 2.4
5. The module CSPs may be zeroized by calling the Revert method on the AdminSP in the Opal interface of the cryptographic Module.

6. Successful execution of the challenge / response protocol zeroizes the module prior to allowing 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 “Solidigm SSD_DC_D7-D4512 _Procedure_To_Exit_Maintenance_Mode.pdf” - Version 1.0 to exit the maintenance mode.
8. The password length must be equal or greater to 8 bytes.
9. The Module shall be initialized by the CO before any User access the Module and calling any services different than those described in Section 2.4

3. Cryptographic Module Interfaces

The physical ports and logical interfaces[4] are identified in Table 4 below:

Physical port	Logical interface	Data that passes over port/interface
PCIe Connector	Data input	NVMe interface used for both normal and maintenance operations
	Data output	NVMe interface used for both normal and maintenance operations
	Control input	NVMe interface used for both normal and maintenance operations, SMBus management interface, VDM interface, UART interface MUX for Debug accessed only during maintenance
	Status output	NVMe interface used for both normal and maintenance operations, SMBus management interface, VDM interface, UART interface MUX for Debug
	Power interface	Power interface
UART	Control input	UART interface for Debug (available with latch removal in E1.L)
	Status output	UART interface for Debug (available with latch removal in E1.L)
LED (E1.L only)	Status output	Signals to illuminate module LED status

Table 5 – Ports and Interfaces

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 capability support, and retrieving status reporting. The SMBus interface provides the ability to audit the SSD environment (temperature, Vital Product Data).

[4] Control output is not supported.

4. Roles, Services, and Authentication

4.1 Assumption of Roles

The Module supports three (3) distinct roles: Cryptographic Officer (CO), User, and Maintenance roles. The cryptographic Module enforces the separation of CO and User roles using a credential (named password or PIN) that is provisioned for the administrator (CO) role 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 an RSA 2048-bit challenge/response protocol with 512-bit nonce and PSID verification (to prove physical presence). This role grants maintenance and recovery capabilities to the Module implementer. The PSID is a unique identifier of each device and is classified as a non-CSP. A unique PSID value is printed on each device label and stored in the module's OTP. No security is claimed from this value but is used solely to prove physical presence.

It is feasible for the Module to process concurrent operations by roles. However, the Module can only support one Opal session at a time. This implies that authentication to the Module by various roles must be serialized. Once authenticated, various roles may interact with the Module simultaneously. As an example, the CO role may perform administrative tasks while the User role is simultaneously reading and writing data to the module.

Role	Service	Input	Output
Cryptographic Officer (CO)	• Take Ownership • Data Encryption/Decryption • Activate Opal • Change Admin Password • Zeroise/AdminSP Revert • Disable Authorities • Configure Locking Ranges • Format NVM/ Crypto Erase • TCG RevertSP and Keep Data • Set data store • Configure Access Control • Lock, Unlock Ranges	• TCG Opal commands tunneled over NVMe Security Send / Receive administrative commands • NVMe IO commands (Read, Write, etc.)	• Status information and information regarding Opal configuration state • Status and user data

Role	Service	Input	Output
	• Module Reset (Self-Test) • Low Power State Entry • Low Power State Exit • Read Compliance (show status) • Firmware Update • Block SID • MBR Shadow		
Maintenance	• FW Maintenance • Maintenance FW update • Firmware Update	• Authentication credentials • Commands for retrieving debug logs • Device Recovery commands • Firmware download and commit commands	• A 512-bit nonce which is used as part of the Authentication protocol Authentication results • Debug log pages • Command status

Role	Service	Input	Output
User (Opal LockingSP User Authority)	• Data Encryption/Decryption • Configure Locking Ranges • Format NVM/ Crypto Erase • Set data store • Configure Access Control • Lock, unlock ranges • Set common name – Locking SP if allowed by Locking SP Admin • Module Reset (Self-test) • Low Power State Entry • Low Power State Exit • Read Compliance (show status) • Firmware Update • NVMe-MI Basic Management Command • NVMe Administration	• Opal commands that the user has been authorized to perform by the CO role • NVMe IO commands (Read, Write, etc.)	• Status information and information regarding Opal configuration state • Status and user data

Table 6 – Roles, Service Commands, Input and Output

Role	Authentication Method	Authentication Strength
Cryptographic Officer	Role-based: 8-byte to 32-byte password (AdminSP SID) A maximum of 5 for attempts are possible before requiring a power-on reset of the storage device	• The probability of guessing a password/PIN in a single attempt is 1/2^64 (= 1/2^(8*8)) which is smaller than 1/10^6 • Since each reset takes approximately 2 seconds, 5 * 30 = 150 password attempts may be executed in one minute where the overall search space is 2^64 leaving a false acceptance probability in one minute of 150/2^64
Maintenance	Role-based: RSA 2048-bit challenge/response protocol w/ 512 bit nonce and PSID	• The Maintenance role challenge response authentication mechanism leverages a 2048-bit signature verification

Role	Authentication Method	Authentication Strength
	verification (to prove physical presence)	The security strength of the authentication method is greater than 112 bits Therefore, the probability of a random attempt of generating a matching signed challenge is 1/2^112 which is smaller than 1/10^6 • The module can perform up to 1,500 authentication verifications per one minute where the overall search space is 2^112 leaving a false acceptance probability in one minute of 1,500/2^112 (= 2.88E-31)
User	Role-based: 8-byte to 32-byte password (User-Password) A maximum of 5 attempts are possible before requiring a power-on reset of the storage device	• The probability of guessing a password/PIN in a single attempt is 1/2^64 (= 1/2^(8*8)) • Since each reset takes approximately 2 seconds, 5 * 30 = 150 password attempts may be executed in one minute where the overall search space is 2^64 leaving a false acceptance probability in one minute of 150/2^64

Table 7 – Roles and Authentication

4.2 Services

All services implemented by the Module in Approved mode are listed in Table 7 below. Each service description also describes all usage of CSPs by the service. The service names highlighted in bold can be called in the uninitialized state.

Note:

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

The following abbreviations of the access rights are used in Table 7 below:

G = Generate: The module generates or derives the SSP.

R = Read: The SSP is read from the module (e.g. the SSP is output).

W = Write: The SSP is updated, imported, or written to the module.

E = Execute: The module uses the SSP in performing a cryptographic operation.

Z = Zeroise: The module zeroises the SSP.

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys and/or SSPs	Indicator
Take Ownership	Obtain the default credential (SID = MSID) for the Opal and configure the Opal credential to a unique value (SID != MSID)	PBKDF2	AdminSP SID, Salt	CO	W	Compliance descriptor and success return code
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	AES-XTS	MEK	CO, U	E	Compliance descriptor and success return code
Activate Opal	Enable through TCG Opal Activate command	PBKDF2, AES-KW, AES-ECB, KBKDF, HMAC, SHS	User Password, User PKey, User KREK, MKEK, Opal Admin PKey, Opal Admin KREK	CO	G, E	Compliance descriptor and success return code

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys and/or SSPs	Indicator
Change Admin Password	Change any password in AdminSP	PBKDF2	Opal Admin PKey	CO	G, E	Compliance descriptor and success return code
Zeroise/Admin SP Revert	Destroy user data (TCG Revert)	DRBG, ENT, HMAC, SHS	All CSPs	CO	Z	Compliance descriptor and success return code
Disable Authorities	Disable authorities to make them invalid and no longer able to authenticate to the drive	PBKDF2	Opal Admin KREK	CO	E	Compliance descriptor and success return code
Enable Authorities	Enable authorities to make them valid for a user to be able to authenticate to the drive	PBKDF2	Opal Admin KREK	CO	E	Compliance descriptor and success return code
Configure Locking Ranges	Configure locking ranges in the CM	PBKDF2	User KREK	CO, U (if enabled by CO)	G	Compliance descriptor and success return code
Format NVM/ Crypto Erase	Destroy any data (changing key)	PBKDF2, DRBG, ENT, HMAC, SHS, CKG, AES-CTR	MEK, MKEK, Device Root Key (Non-SSP), Ephemeral Blob Encryption Key (Non-SSP), DRBG-EI, DRBG-Seed, DRBG-State	CO, U	G, E	Compliance descriptor and success return code

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys and/or SSPs	Indicator
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	PBKDF2, AES-KW, AES-ECB, KBKDF, HMAC, SHS	MKEK, User KREK	CO	Z, E	Compliance descriptor and success return code
Set Data Store	Set data store – write data into the Opal data store tables	PBKDF2	AdminSP SID, User Password	CO, U	E	Compliance descriptor and success return code
Configure Access Control	Change which entity can manage/lock/unlock an encryption range	PBKDF2	AdminSP SID, User Password	CO, U (if enabled by CO)	E	Compliance descriptor and success return code
Lock, Unlock Ranges	Lock, unlock ranges from access to read/writes on the data input/output interface	PBKDF2	AdminSP SID, User Password, User KREK, MKEK	CO, U	E	Compliance descriptor and success return code
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	N/A	N/A	U	N/A	N/A
FW Maintenance	Retrieve FW Maintenance Logs, recover device from non-functional state	RSASSA-PKCS1-v1.5, SHS	RSA Public ADU Verification Key	MR	E	Compliance descriptor and success return code

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys and/or SSPs	Indicator
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 SHA2-256 and the internal RSA Public FW Verification Key	RSASSA-PKCS1-v1.5, SHS	RSA Public ADU Verification Key, RSA Public Firmware Verification Key	MR	E	Compliance descriptor and success return code
Module Reset (Self-Test)	Reset the Module by power cycle, or performing NVMe Controller or NVM Subsystem reset Performs self-tests, firmware integrity check	N/A	N/A	CO, U	N/A	N/A
Low Power State Entry	Place the module into a low power state	CKG [SP 800-133, rev2] AES KW [SP800-38F]	REK MEK	CO, U	G, E	The module stops processing commands from the host
Low Power State Exit	Resume the module from the low power state	AES KW [SP800-38F]	REK MEK	CO, U	E	The module resumes processing commands from the host

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys and/or SSPs	Indicator
Read Compliance (show status)	Query the module for configuration information by reading the TCG defined Level 0 Feature Descriptor, the NVMe defined Identify command, and the T10 Compliance Descriptor as defined in [SFSC]. This service provides the module version information.	N/A	N/A	CO, U	N/A	N/A
Firmware Update	Download new firmware images to the module using NVMe defined Firmware Download and Commit commands	RSASSA-PKCS1-v1.5, SHS	RSA Public Firmware Verification Key	CO, U, MR	E	Compliance descriptor and success return code
NVMe-MI Basic Management Command	Retrieves drive status (status flags, SMART warnings, temperature, VID, serial number, etc.)	N/A	N/A	U	N/A	N/A
NVMe Administration	Issue administrative commands (not previously mentioned) to the module, as defined in the NVMe specification This may include Vendor Unique public commands that are in compliance with the NVMe specification	N/A	N/A	U	N/A	N/A

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys and/or SSPs	Indicator
Block SID	Allows host pre-OS application to lock access to the SID authority by subsequently loaded host software	PBKDF2	AdminSP SID	CO	E	Compliance descriptor and success return code
MBR Shadow	Read/write Pre-Boot Application (PBA) to a reserved area of Module non-volatile memory	PBKDF2	AdminSP SID	CO	E	Compliance descriptor and success return code

Table 8 – Approved Services

The module does not implement any non-Approved services.

5. Software/Firmware Security

The Module is designated as a limited operational environment under the FIPS 140-3 definitions and operates on the Sentinel Rock Plus C0 ASIC processor. The Module includes a firmware load service to support necessary field updates. The Module will not load or execute firmware which is not signed with the Solidigm 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 NVMe, SMBUS or UART (after removing tamper evident label for E1.L) after entering the Maintenance role

New firmware versions within the scope of this FIPS 140-3 validation must be validated through the CMVP. Any other firmware loaded into this Module is out of the scope of this validation and will require a separate FIPS 140-3 validation.

The module's integrity test can be run on demand by power cycling the Module or by the Module Reset service.

6. Operational Environment

This section is **not applicable** to the module.

7. Physical Security

The following physical security measures are implemented in the module, which meet the requirements for a multi-chip embedded embodiment at Security Level 2:

- The Module consists of production-grade components enclosed in an aluminum alloy enclosure, which is opaque within the visible spectrum.
- The U.2 enclosure contains two parts: a top and bottom part that affix together using a hinge on the back side of the Module and two (2) screws that affix the top to the bottom near the PCIe edge connector.
- The E1.L enclosure contains three parts: a top and a bottom part that affix together using eight (8) screws that affix the top and bottom together as well as a latch affixed with two (2) screws.
- For the U.2 model, one (1) tamper-evident seal is 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 seal will be broken in the process. The position of the one (1) tamper-evident seal is indicated in Figure 1 and Figure 2. The tamper-evident seals are captured as part of the model part number that is listed in Table 2.
- For the E1.L model, three (3) tamper-evident seals are affixed to the bottom of the Module such that if the Module top and bottom are separated, exposing internals of the Module, that the tamper-evident seals will be broken in the process. The position of the two (2) tamper-evident seals are indicated in Figure 3 and Figure 4. The tamper evident seals are captured as part of the model number that is listed in Table 2.

Physical Security Mechanism	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Three (3) tamper-evident labels affixed to the module's back face (E1.L)	12 months	Inspect the tamper-evident seals for scratches, gouges, cuts, and other signs of tamper. Remove from service if tampering is found.
One (1) tamper-evident label affixed to the module's front (U.2)	12 months	Inspect the tamper-evident seal for scratches, gouges, cuts, and other signs of tamper. Remove from service if tampering is found.
Production grade cases	12 months	Inspect the entire perimeter for cracks, gouges, lack of enclosure, bent clips, and other signs of tamper. Remove from service if tampering is found.

Table 9 – Physical Security Inspection Guidelines

The Cryptographic Officer is responsible for obtaining, storing, and applying new tamper-evident labels should the module require maintenance or repair upon inspection. The Crypto Officer can order new tamper evident seals using the part number M45818-002 (E1.L form factor) or M52551-001 (U.2 form factor).

Figure 6 - U.2 Module Seal Application Locations - Front

Figure 7 - E1.L Module (Intel Branded) Seal Application Locations -- Back

7.1 Applying Tamper-Evident Seals

Some modules may be shipped without the required tamper- evident seals. The tamper-evident seals shall be installed for the module to operate in Approved mode of operation.

To convert the module to Approved mode of operation, the following procedure must be followed to apply the provided seals to the module:

1. Clean seal surface
   a. Use isopropyl alcohol of equivalent solution to remove any contaminants from the enclosure seam seal location
   b. Handle drive and seal with gloves
2. Locate the Tamper Evident Label Locations
   a. **For U.2 Module:** There is just one seal to be placed on the right front of the module (see Figure 6)
   b. **For E1.L Module** There are two seals to be placed on the bottom side of the module; one seal over the upper far right screw next to the PCIe connector, one seal over the lower third screw from the PCIe connector and a third seal on the screw on the lower far left attaching the black latch (see Figure 8).
3. Use tweezers to lift seal from liner and place on the seam of the enclosure for the designated area (see Figure below for an example on the U.2 Module).
4. Apply finger pressure to seal pressing out any air or lifted edges

Figure 8 - Applying Tamper-Evident Seals

EFP/EFT testing of the module is not applicable as the module does not claim Security Level 3 or above.

8. Non-invasive Security

This section is **not applicable** to the module.

9. Sensitive Security Parameter Management

Key/SSP Name/Type	Strength	Security Function and Cert. Number	Generation	Import/ Export	Establishment	Storage	Zeroisation	Use & related keys
DRBG-EI (CSP)	256	DRBG [SP 800-90A, rev1] (#A2881)	ENT (P) (Whenever encryption keys are derived by the module)	N/A	N/A	Volatile memory (plaintext)	Cleared automatically after key derivation operation completes or Reset	DRBG entropy input used to derive the DRBG-Seed
DRBG-State (CSP)	256	DRBG [SP 800-90A, rev1] (#A2881)	DRBG (Whenever encryption keys are derived by the module)	N/A	N/A	Volatile memory (plaintext)	Cleared automatically after key derivation operation completes or Reset	HMAC_DRBG internal state (V and Key) derived from the DRBG-Seed
DRBG-Seed (CSP)	256	DRBG [SP 800-90A, rev1] (#A2881)	DRBG (Whenever encryption keys are derived by the module)	N/A	N/A	Volatile memory (plaintext)	Cleared automatically after key derivation operation completes or Reset	DRBG HMAC seed derived from the DRBG_EI
Opal Admin KREK (CSP)	256	AES KW [SP800-38F] (#A2881)	KBKDF [SP 800-108, rev1] (At TCG Opal Activation	N/A	N/A	ASIC internal memory (plaintext), NAND (encrypted with Opal	AdminSP Revert	Opal Admin Key Ring Encryption Key is used to protect/encrypt the Admin Locking Range Key Ring(s)

						Admin Pkey)		
AdminSP SID (CSP)	Varies, must be of minimum length of 8 bytes enforced by the module	PBKDF2 [SP 800-132] (#A2881)	External to the module (By the CO role)	Import: Plaintext (electronically) Export: N/A	N/A	Temporarily in volatile memory (plaintext)	Internally zeroized once the Admin has been authenticated	AdminSP SID (Password)is used to authenticate the CO and is used to derive the Opal Admin PKey
Opal Admin PKey (CSP)	256	AES KW [SP800-38F] (#A2881)	PBKDF2 [SP 800-132] - Derived from admin password and salt (During Authentication)	N/A	N/A	ASIC internal volatile memory (plaintext)	Internally zeroized once the Admin has been authenticated	Admin password Key used to encrypt / decrypt Opal Admin KREK and is derived from the AdminSP SID
MEK (CSP)	256	AES XTS [SP800-38E] CKG [SP 800-133, rev2] (#A2879)	CKG [SP 800-133, rev2]	N/A	N/A	ASIC internal volatile memory (plaintext), NAND (encrypted by MKEK)	From ASIC internal memory during Power Cycle, Hard Reset, Maintenance Mode From NVM at Opal Activation and Crypto Erase commands, or issuance of NVMe Format	Media Encryption Keys are used to protect user data when stored to non-volatile memory

							NVM, Crypto Erase, or Sanitize commands	
MKEK (CSP)	256	AES KW [SP800-38F] CKG [SP 800-133, rev2] (#A2881)	CKG [SP 800-133, retv2]	N/A	N/A	ASIC internal volatile memory (plaintext), NAND (encrypted by User KREK)	From ASIC internal memory during Power Cycle, Hard Reset, Maintenance Mode From NAND at TCG Opal Activation or Reactivate	Media Key Encryption Keys are used to protect Media Encryption Keys (MEKs)
User KREK (CSP)	256	AES KW [SP800-38F] (#A2881)	KBKDF [SP 800-108, rev1] (During Opal Activation; During User Locking Range Creation)	N/A	N/A	ASIC internal volatile memory (plaintext), NAND (encrypted with User PKey)	On AdminSP Revert	User Key Ring Encryption Key is used to protect the MKEK
User Password (CSP)	Varies, must be of minimum length of 8 bytes enforced by the module	PBKDF2 [SP 800-132] (#A2881)	Externally (By the User role)	Import: Plaintext (electronically) Export: N/A	N/A	Temporarily in volatile memory (plaintext)	Internally zeroized once the User has been authenticated	Opal User password is used to authenticate the User and is used to derive the User PKey

User PKey (CSP)	256	AES KW [SP800-38F] (#A2881)	PBKDF2 [SP 800-132] Derived from user password and salt (During Authenticati on)	N/A	N/A	ASIC internal volatile memory (plaintext)	Power Cycle, Hard Reset, Maintenance Mode	User password Key used to encrypt / decrypt User KREK
Reset Ephemeral Key (REK) (CSP)	256	AES KW [SP800-38F] CKG [SP 800-133, rev2] (#A2881)	CKG [SP 800-133, rev2] At Power on of the Device	N/A	N/A	ASIC internal volatile memory (plaintext)	Power Cycle, Hard Reset, Maintenance Mode	Reset Ephemeral Key enables recovery of Media Encryption Keys across Low Power transitions
RSA Public Firmware Verification Key (PSP)	112	RSA Key Verification [FIPS 186-4 and PKCS #1 v2.1 (PKCS1.5)] (#A2880, #A2881)	External	N/A	N/A	Burned into Hardware ROM (plaintext)	N/A (Protected from modification and stored with an integrity value per IG 9.7.A)	2048-bit RSA public Key used to verify the RSA Signature of the Module's main firmware (on Boot and Firmware Download / Commit)
Salt (CSP)	160	PBKDF2 [SP 800-132] (#A2881)	DRBG [SP 800-90A, rev1] Whenever symmetric encryption keys are generated by the module	N/A	N/A	ASIC internal volatile memory (plaintext), NAND (encrypted)	On AdminSP Revert	PBKDF2 Salt, 20-byte value
RSA Public ADU	112	RSA Signature Verification [FIPS 186-4 and	External (Built into	Import: Plaintext in	N/A	Built into firmware binary	N/A (Protected	2048-bit RSA public Key used to verify the signature

Verification Key (PSP)		PKCS #1 v2.1 (PKCS1.5)] (#A2881)	firmware binary)	firmware image			from modification)	of the request to unlock the drive for diagnostic access

Table 10 – SSPs

The module includes two non-SSPs, the Device Root Key and the Ephemeral Blob Encryption Key. The 32-bit Device Root Key is burned into device ROM in plaintext and cannot be zeroized. The Device Root Key is used to derive the non-security relevant Ephemeral Blob Encryption Key using the SP 800-108 KBKDF. The Ephemeral Blob Encryption Key is stored in volatile memory and is generated and then zeroized upon every Crypto Erase operation. The Ephemeral Blob Encryption is used to wrap Encrypted Key Blobs (MEKS wrapped with MKEKs) when storing to NAND. The blobs are considered obfuscated, since the wrapping is being done with a non-SSP.

Entropy sources	Minimum number of bits of entropy	Details
SP 800-90B compliant ENT (P)	0.259 bits of min entropy per bit The DRBG is seeded with 2048 bits of random data providing approximately 530 bits of entropy.	Physical noise source from the Broadcom TRNG used to seed the DRBG

Table 11 – Non-Deterministic Random Number Generator Specification

10. Self-Tests

Each time the Module is powered up, it tests that the cryptographic algorithms operate correctly, and that sensitive data has not been damaged. Pre-operational and conditional cryptograph algorithm tests are available on demand by power cycling the Module or the Module Reset service.

On power-up or reset, the Module performs the Self-Tests described below. All Cryptographic Algorithm Self-Tests (CASTS) must be completed successfully prior to any other use of cryptography by the Module. If one of the CASTs fails, the Module enters an error state requiring reset of the Module.

The module uses RSA 2048 with SHA2-256 to satisfy the pre-operational integrity self-test requirement.

Pre-operational Software/Firmware Integrity Test	Description
RSA Integrity Test	Signature verification with RSA 2048 bit key and SHA2-256 (Cert. #A2880)

Conditional Self-Tests Test Target	Description
AES-CTR (Cert. #A2881)	CASTs: Encryption in CTR mode with 256 bit key KAT, Decryption in CTR mode with 256 bit key KAT
AES-KW (Cert. #A2881)	CASTs: Encryption in KW mode with 256 bit key KAT, Decryption in KW mode with 256 bit key KAT
AES-XTS (Cert. #A2879)	CASTs: Encryption in XTS mode with 256 bit key KAT, Decryption in XTS mode with 256 bit key KAT
DRBG (Cert. #A2881)	CASTs: HMAC DRBG (inclusive of instantiate, generate and reseed)
PBKDF (Cert. #A2881)	CASTs: Key Derivation Iterations: 10,000
KBKDF (Cert. #A2881)	CASTs: HMAC-SHA2-256 Key Derivation KAT
RSA (Cert. #A2881)	CASTs: Signature Verification with 2048 bit key and SHA2-256
SP 800-90B Health Tests	NIST SP 800-90B ENT Health Tests, per SP 800-90B Section 4.5

Firmware Load Test	Firmware signature verification based on RSA PKCS#1 v1.5 with SHA2-256 and 2048-bit key.
Key Equality Check	When an XTS key is generated, the module verifies that Key1!=Key2

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

- Firmware integrity: either the Module will not respond or will not enumerate
- CAST: the module will not enumerate
- Key Equality Check: Returns an error
- Firmware upload: the SSD will return Invalid Image
- Entropy Source: the module will retry three times then enter an error state

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

11. Life-Cycle Assurance

11.1 Secure Distribution

The module is shipped using a certified mail carrier. The shipping container protecting the module or set of modules in transit should be verified for tamper evidence. The module is shipped in a shipping container with yellow tape. The tape should be sealing the container. Additionally, the module is contained within a clamshell with seals that should be inspected for tampering. If the shipping container or clamshell appears to be tampered with, the CO should contact Solidigm.

11.2 Secure Installation Procedure

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 the Section 7. Upon verification that the Module has not been tampered with, the user should initialize the module as described in Section 2.4.

11.3 Module Start-up and Initialization Procedure

See instructions in section 2.4 for module start-up information.

12. Mitigation of Other Attacks

This module has not been designed to mitigate any specific attacks beyond the scope of FIPS 140-3.

References and Definitions

The following standards are referred to in this Security Policy.

Abbreviation	Full Specification Name
[ISO/IEC 19790]	Information technology - Security techniques - Security requirements for cryptographic modules, June 25, 2014
[SP800-140C]	CMVP Approved Security Functions
[SP800-131Arev2]	Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths, March 2019
[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)

Acronym	Definition
ASCII	American Standard Code for Information Interchange
AES	Advanced Encryption Standard
CAST	Cryptographic Algorithm Self-Test
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
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

Acronym	Definition
SSD	Solid State Drive
SID	Secure ID
TCG	Trusted Computing Group
XTS	XEX Tweakable Block Cipher with Ciphertext Stealing