PE9110 E1.S and PE9010 M.2 22110D NVMe TCG Opal SSC SEDs

FIPS 140-3 Cryptographic Module
Non-Proprietary Security Policy

Document Version: 0.8
Date: 11/11/2024

Table of Contents

List of Tables

List of Figures

1 General

This document defines the Security Policy for the SK hynix PE9110 E1.S and PE9010 M.2 22110D NVMe TCG Opal SSC SEDs cryptographic module, hereafter denoted the Module. The Module is a multiple chip embedded self-encrypting drive (SED) compliant with TCG Core, TCG Opal, TCG Single User Mode (SUM), PCIe, and NVMe specifications. The Module is also compliant with the IEEE1667 storage specification. The cryptographic module's controller has a built-in AES-XTS HW engine which encrypts and decrypts the user data without any performance loss. The Module meets FIPS 140-3 overall security Level 1.

The FIPS 140-3 security levels for the Module are as follows:

Table 1: Security Level of Security Requirements

Security Requirement	Security Level
General	1
Cryptographic Module Specification	1
Cryptographic Module Ports and Interfaces	1
Roles, Services, and Authentication	1
Software/Firmware Security	1
Operational Environment	1
Physical Security	1
Non-Invasive Security	N/A
Sensitive Security Parameter Management	1
Self-Tests	1
Life-Cycle Assurance	1
Mitigation of Other Attacks	N/A
Overall Level	1

2 Cryptographic Module Specification

The Module is designed to be embedded in a General Purpose Computer (host). The Module does not support a maintenance access interface.

The Module uses a single chip controller (Atomos) with a PCIe/NVMe and SMBus interface on the systems side and SK hynix NAND flash internally.

The Module is composed of the following major components:

- **Atomos Controller** – The controller SoC (System On Chip). 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 SK hynix NAND nonvolatile memory.
  - PMC – Power Management Controller –Manages power control of the Module
  - PCIe/NVMe Interface – Provides PCI/NVMe Interface access to the controller
  - SMBus Interface – Provides SMBus Interface access to the controller
  - CPU – Central Processing Unit of the controller
  - ROM – Read only memory – Non-volatile memory which has first bootable code for controller
  - ECC – Error Correction Code memory provides Error correction and detection access to the controller
  - SRAM – Static Random Access memory
  - DRAM Interface – Provides access to SK hynix DRAM
  - NAND Interface – Provides access to SK hynix NAND Memory
- **SK hynix DRAM** – Dynamic Random Access Memory. DRAM Provides variable storage, instruction memory, data mapping tables and buffer for user data going into and out of the device.
- **SK hynix NAND memory** – NAND flash is the storage medium where encrypted user data, firmware for the Atomos controller, and other non-volatile configuration data needed by the Atomos controller during execution.

2.1 Operational Environment

The following Module configurations were tested:

Table 2: Cryptographic Module Tested Configuration

#	Model	HW P/N	FW Version	Distinguishing Features
1	PE9110 E1.S	HFS1T9GEEWX132N	41089A30	1920GB
2	PE9110 E1.S	HFS3T8GEEWX132N	41089A30	3840GB
3	PE9110 E1.S	HFS7T6GEEWX132N	41089A30	7680GB
4	PE9010 M.2 22110D	HFS960GDJ0X132N	51082A30	960GB
5	PE9010 M.2 22110D	HFS1T9GDJ0X132N	51082A30	1920GB
6	PE9010 M.2 22110D	HFS3T8GDJ0X132N	51082A30	3840GB

2.2 Cryptographic Boundary

The PE9110 has an E1.S physical form factor, while the PE9010 has an M.2 22110D physical form factor as depicted in Figures 1 and 2 respectively. The cryptographic boundary is defined as the entire PCB of each form factor, as outlined with a red dotted line. Note that the PE9110

E1.S includes a metallic enclosure, while the PE9010 M.2 22110D does not. No components have been excluded from the cryptographic boundary.

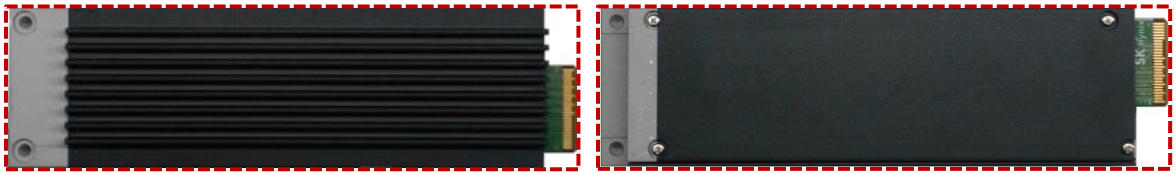

Figure 1: PE9110 E1.S Top and Bottom (Cryptographic Boundary in Red)

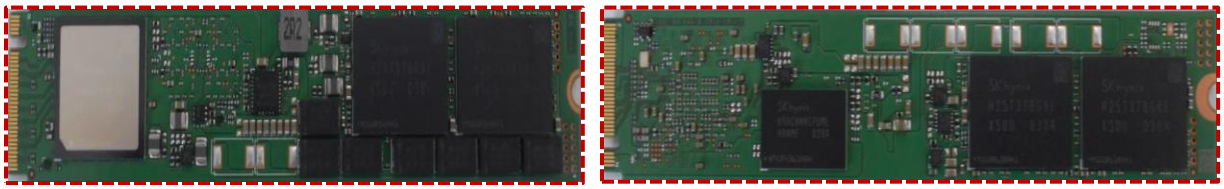

Figure 2: PE9010 M.2 22110D Top and Bottom (Cryptographic Boundary in Red)

2.3 Mode of Operation

The Module only supports an Approved Mode of operation and is thus continually in an Approved mode of operation. In order to confirm the module's versioning information and that it is operating in an Approved manner, the operator may invoke the "Read FIPS Compliance" service, as specified in Section 11.1.

Per IG 2.4.C, Example Scenario #2, a global indicator is used to identify the Approved mode of operation, along with the implicit indicator for the successful completion of each Approved service.

2.4 Security Functions

The Module implements the Approved Mode cryptographic functions listed in the table below. The module does not support any non-Approved cryptographic functions.

Table 3: Approved Algorithms

Cert	Algorithm	Mode	Description	Functions/Caveats
A2596	AES [197]	ECB [38A]	Key Sizes: 256 Boundary: Hardware	Encrypt, Decrypt Support for XTS and KW
		XTS [38E]	Key Sizes: 256 Boundary: Hardware	Encrypt, Decrypt of user data
		KW [38F]	Forward Key Sizes: 256 Boundary: Hardware	Authenticated Encrypt, Authenticated Decrypt for key storage
A2272	Conditioning Component Block Cipher Derivation Function SP800-90B	ECB [90B]	Key Sizes: 128 Boundary: Hardware	SP800-90B Conditioner

Cert	Algorithm	Mode	Description	Functions/Caveats
C1278	DRBG [90Ar1]	CTR	Prediction Resistance: Yes, No Supports Reseed Mode: AES-256 Derivation Function Enabled: No Additional Input: 0-384 Entropy Input: 384 Nonce: 0 Personalization String Length: 0-384 Returned Bits: 512 Additional Input used: No Entropy Input used: 384 Personalization String used: No Boundary: Hardware	Deterministic Random Bit Generation Security strength = 256 bits.
	AES [197]	ECB [38A]	Key Sizes: 256 Boundary: Hardware	Encrypt, Decrypt To support CTR_DRBG
A2595	DRBG [90Ar1]	CTR	Prediction Resistance: Yes, No Supports Reseed Mode: AES-256 Derivation Function Enabled: Yes Additional Input: 0-2048 Increment 128 Entropy Input: 256-2048 Increment 128 Nonce: 128-1024 Increment 128 Personalization String Length: 0-2048 Increment 128 Returned Bits: 512	Tested, but not used
N/A	ENT [90B]	ENT (P)	Hardware Non-Deterministic RNG; minimum of 512 bits per access. Boundary: Hardware	Provides a minimum of 256 bits of security strength to the Approved DRBG
A2596	HMAC [198-1]	SHA2-256	Key Sizes: 256 bits λ = *32 bytes* Boundary: Hardware	Public Security Parameter (PSP) data authentication and support for PBKDF2
A2595	PBKDF [132]	Option 1a	sLen = 32 bytes salt C = 1,000 iterations HMAC-SHA2-256 Cert. #A2596 Boundary: Firmware	Password Based Key Derivation. The keys derived from passwords are used only in storage application
A2595	RSA [186-4]	PSS	n = 2048 – 4096, SHA2-256, 384, 512 Boundary: Firmware	SigVer - Signature Verification: Firmware Updates and Maker Authentication

Cert	Algorithm	Mode	Description	Functions/Caveats
A2597	RSA [186-4]	PSS	n = 3072 – 4096, SHA2-384, 512 Boundary: Hardware	SigVer - Signature Verification: Firmware Integrity
A2595	SHA2-384	SHA2-512	Boundary: Firmware	Message digest
A2595	SHA2-512	SHA2-512	Boundary: Firmware	Message digest
A2596	SHA2-256	SHA2-256	Boundary: Hardware	Message digest
A2597	SHA2-384	SHA2-384	Boundary: Hardware	Message digest
A2597	SHA2-512	SHA2-512	Boundary: Hardware	Message digest

Table 4: Vendor Affirmed Approved Algorithms

Algorithm	Caveat	Use/Function
CKG [IG D.12]	[133r2] Section 6.1 - The "Direct Generation" of Symmetric Keys	Direct Symmetric Key generation using unmodified DRBG output
	[133r2] Section 6.2.3 - Symmetric Keys Derived from Passwords	Derivation of symmetric keys from a Password. The key can only be used for storage applications.
	[133r2] Section 6.3 - Symmetric Keys Produced by Combining (Multiple) Keys and Other Data	Derivation of XTS keys.

Table 5: Non-Approved Algorithms Allowed in the Approved Mode of Operation

Algorithm	Caveat	Use/Function
N/A	N/A	N/A

Table 6: Non-Approved Algorithms Allowed in the Approved Mode of Operation with No Security Claimed

Algorithm	Caveat	Use/Function
PBKDF [132]	IG 2.4.A, Example #1 – Obfuscation of internally stored data	PBKDF is used to derive an obfuscation key based on an optional password. Per TCG specifications, the password must be optional and may be of 0 length.
AES-KW	IG 2.4.A, Example #1 – Obfuscation of internally stored data	Used in conjunction with PBKDF above to obfuscate keys. All keys obfuscated with AES-KW when using a PBKDF derived key are treated as plaintext SSPs.
RSA	IG 2.4.A, Example #2 – Use of an approved algorithm for a purpose that is not security relevant or is redundant to an approved cryptographic algorithm	RSA verification using a 4096-bit key with SHA2-512 serves a redundant purpose to HMAC-SHA2-256 at power on; both RSA 4096 and HMAC-SHA2-256 are applied to PSPs for verifying data integrity.

Table 7: Security Function Implementation (SFI)

Name	Type	Description	SF Propertioes	Algorithms/CAVP Cert
N/A	N/A	N/A	N/A	N/A

Table 8: Entropy Certificates

Vendor Name	Certificate Number
N/A	N/A

2.5 Overall Security Design

Per IG C.I, the module assures Key_1 and Key_2 are not equal for AES-XTS operations.

The module implements the following security elements:

1. No additional interface or service is implemented by the Module which would provide access to CSPs.
2. Data output is inhibited during self-tests, Key generation, Zeroization, error states, and firmware load verification.
3. The module does not support manual key entry.
4. The module does not output plaintext CSPs or intermediate key values.
5. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
6. The Module does not support a bypass capability.
7. Power on self-tests do not require any operator action.
8. The Module does not support the update of the serial number and vendor ID.
9. The Module does not support concurrent operators.

2.6 Rules of Operation

The following security rules must also be considered when operating the module:

1. All CSPs are zeroized by the Zeroization service. Only the Maker role can call the Zeroization service.
2. The Module shall provide five (5) distinct operator roles: Cryptographic Officer, User, Maker, PSID, and Anybody
3. The operator shall be capable of commanding the Module to perform the power up self-tests by power cycling or resetting the Module.

3 Cryptographic Module Interfaces

The Module's ports and associated FIPS defined logical interface categories are listed in Table 9. The module does not support a Control Output interface.

Table 9: Ports and Interfaces

Physical Port	Logical Interface Type	Data that passes over port/interface
PCIe Connector	Power	Power
	Control in, Data in, Data out, Status out	NVMe storage commands and payloads
	Control in, Status out	Management information via SMBus commands and payloads

The module also supports a JTAG and UART port, which are permanently disabled.

3.1.1 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.

3.1.2 SMBus Interface

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

4 Roles, Services, and Authentication

4.1 Assumption of Roles

The module supports five distinct operator roles: Cryptographic Officer (CO), User, Maker, PSID, and Anybody. The method for assuming a role is implicit based on the services invoked. The module only asserts conformance with Level 1 requirements; PINs and passwords are optional as required by TCG standards and are defined as non-SSPs; the module makes no claim to support FIPS 140-3 authentication mechanisms.

The module supports the following operator roles:

1. Crypto Officer (CO):
    a. Admin SP SID - This operator is responsible for transitioning from uninitialized mode to initialized mode.
    b. Admin SP Admin – This operator is disabled by default but can be enabled by SID authority. When enabled, it can transition the Module back to the uninitialized state from the initialized state.
    c. Locking SP Admins – This operator is used to enable and disable Users, create and delete user ranges, lock or unlock the ranges and cryptographically erase the user ranges.
    The CO is also responsible for performing firmware updates.
2. User: The Locking SP Users can unlock and lock the drive to allow the operator to read and write data to the drive. This user can also call the “Cryptographic Erase” service.
3. Maker: This is an assumed role which enables the operator to execute the “Zeroise Service” command.
4. PSID: The TCG PSID Authority has access to perform the “PSID Revert” service.
5. Anybody: This role is assumed when the operator executes services that does not require a TCG role to be assumed.

The Module does not support a maintenance role or bypass capability. The Module does not support concurrent operators.

Table 10: Roles and Authentication

Role	Authentication Method	Authentication Strength
CO	N/A	N/A
User	N/A	N/A
Maker	N/A	N/A
PSID	N/A	N/A
Anybody	N/A	N/A

4.2 Services

All services implemented by the Module are listed in Table 11, while SSP usage for each service is specified in Table 12.

Note:

- CO= Cryptographic Officer Role
- U = User Role
- M = Maker Role
- P = PSID Role
- A = Anybody

Table 11: Roles, Service Commands, Input and Output

Role	Service	Input	Output
CO	Take ownership	Security Send command parameters; Security Send command payload w/ TCG Set method for C_PIN_SID	-; Security Receive command status
CO	Activate OPAL	Security Send command parameters; Security Send command payload w/ TCG Activate method	-; Security Receive command status
CO	Deactivate OPAL	Security Send command parameters; Security Send command payload w/ TCG Revert method	-; Security Receive command status
CO	Admin Set PIN	Security Send command parameters; Security Send command payload w/ TCG Set method for ASP or LSP Admins	-; Security Receive command status
CO U	User Set PIN	Security Send command parameters; Security Send command payload w/ TCG Set method for LSP Users	-; Security Receive command status
CO	Enable/Disable User Set PIN	Security Send command parameters; Security Send command payload w/ TCG Set method for ACE Set User PIN object	-; Security Receive command status
CO	Enable/Disable Admin SP authorities	Security Send command parameters; Security Send command payload w/ TCG Set method for ASP Authority object	-; Security Receive command status
CO	Enable/Disable Locking SP authorities	Security Send command parameters; Security Send command payload w/ TCG Set method for ASP Authority object.	-; Security Receive command status

Role	Service	Input	Output
CO	Enable/Disable SUM	Security Send command parameters; Security Send command payload w/ TCG Reactivate method	-; Security Receive command status
CO	Locking Range Configuration	Security Send command parameters; Security Send command payload w/ TCG Reactivate method	-; Security Receive command status
CO U	Lock/Unlock range	Security Send command parameters; Security Send command payload w/ TCG Set method	-; Security Receive command status
CO U	Set common name	Security Send command parameters; Send command payload w/ TCG Set method for Common Name object	-; Security Receive command status
CO U	Data store table Set	Security Send command parameters; Security Send command payload w/ TCG Set method for Datastore table	-; Security Receive command status
CO U	Crypto Erase of a range	Security Send command parameters; Security Send command payload w/ TCG Erase or Genkey method	-; Security Receive command status
M	Zeroization	Zeroization VU command parameters; Zeroization VU command payload	-; Zeroization VU comma status
P	PSID Revert	Security Send command parameters; Security Send command payload w/ TCG Revert method	-; Security Receive command status
A	Power Cycle (Self-Test)	-; -	-; -
A	Hot reset	Bit 6 (Secondary Bus Reset) of Bridge Control Register (offset 0x3E) PCI Config Space; -	-; -

Role	Service	Input	Output
A	Warm reset	Bit 4 (Link Control Register Offset 0x10) in PCI Express Capability Register of PCI config space; or Offset 0x20 is the NVM Subsystem Reset register(NSSR) in the controller registers (PCIe BAR); -	-; “Negotiated Link width” (Bit 9:4) in the Link Status Register (Offset 0x12) of PCI config space; or Bit 4 of the NVMe Controller status register (Offset 0x1C)
A	Show Status	Level 0 Discovery parameters or NVMe Identify command parameters; -	Level 0 Discovery payload or NVMe Identify; Level 0 Discovery status or NVMe Identify command status
A	Read FIPS Compliance	Security Receive w/ Read FIPS Compliance command parameters; -	Read FIPS Compliance payload; Security Receive command status
A	Block SID Authorization	Security Send w/ Block SID Authorization command parameters; -	-; Security Send command status
A	TCG Authorization	Security Send command parameters; Security Send command payload w/ TCG StartSession or Authorization method	-; Security Receive command status
A	Enable Zeroization Service	Vendor Specific Auth Challenge command parameters; Vendor Specific Command Payload	-; Vendor Specific command status
A	Get Random Number	Security Send command parameters; Security Send command payload w/ TCG Random method	Security Receive command payload; Security Receive command status
A	Telemetry logs	Telemetry Log (Get Log Page) command parameters; -	Telemetry Log (Get Log Page) command payload; Telemetry Log (Get Log Page) command status
A	Read/Write User Data	Read/Write command parameters; Write command payload	Read command response payload; Read/Write command status
CO	Firmware Update	Firmware Update command parameters; Firmware Update command payload	-; Firmware Update command status

Role	Service	Input	Output
A	Format NVM / Namespace Management	Format command parameters / Namespace Management command parameters; Format command / Namespace Management command payload	-; Format command / Namespace Management command status
A	Sanitize	Crypto Sanitize command parameters; -	-; Crypto Sanitize command status
A	Configure Drive	Set Features command parameters; -	-; Set Features command status

- 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.
- - = Not accessed by the service.

Table 12: Approved Services

Service	Description	Approved Security Functions	SSPs	Roles	Access Rights	Indicator
Take ownership	Changes default password of SID to a value other than MSID.	PBKDF (#A2595); DRBG (#C1278); HMAC-SHA2-256 (#A2596); AES-KW (#A2596)	CO Password; AUTH_KEYs; SALT; DRBG-EI; DRBG V; DRBG Key; PSP_HMAC_KEY; TPER_SALT_KEK; TPER_KEK	CO	W, E, Z; G, E, Z; G, E; G, E, Z; G, E; G, E; E; E; G, E	Status output to the host is returned for success or error

Service	Description	Approved Security Functions	SSPs	Roles	Access Rights	Indicator
Activate OPAL	Enables Locking SP via TCG Activate method. Activate method can enable SUM.	PBKDF (#A2585); DRBG (#C1278); HMAC-SHA2-256 (#A2596); AES-KW (#A2596)	CO Password; User Password; AUTH_KEYs; SALT; DRBG-EI; DRBG V; DRBG Key; PSP_HMAC_KEY; TPER_SALT_KEK; SUM_KEKs	CO	W, E, Z; E; G, E, Z; G, E; G, E; G, E; E; E; G, E; G, E, Z	Status output to the host is returned for success or error

Service	Description	Approved Security Functions	SSPs	Roles	Access Rights	Indicator
Deactivate OPAL	Reverts the drive back to the Original Factory State through TCG Revert or Revert SP methods. Note: For Revert SP, 1. Global Range data is preserved if KeepGlobal parameter is TRUE. 2. TPER_SALT_KEK and PSP_HMAC_KEY are also preserved.	PBKDF (#A2585); DRBG (#C1278); HMAC-SHA2-256 (#A2596); AES-KW (#A2596); AES-XTS (#A2596)	CO Password; AUTH_KEYs; SALT; MSID PIN; DRBG-EI; DRBG V; DRBG Key; PSP_HMAC_KEY; HRK; MEK_KEK; TPER_SALT_KEK; TPER_KEK; SUM_KEKs; MEKs	CO	E; G, E, Z; G, E; E; G, E, Z; G, E, Z; G, E, Z; G, E, Z; E; G, E, Z; G, E, Z; E, Z; E, Z; G, E, Z	Status output to the host is returned for success or error

Service	Description	Approved Security Functions	SSPs	Roles	Access Rights	Indicator
Admin Set PIN	Updates Admin authority PIN.	PBKDF (#A2585); DRBG (#C1278); HMAC-SHA2-256 (#A2596); AES-KW (#A2596)	CO Password; AUTH_KEYs; SALT; DRBG-EI; DRBG V; DRBG Key; PSP_HMAC_KEY; TPER_SALT_KEK; TPER_KEK; SUM_KEKs	CO	W, E, Z; G, E, Z; G, E; G, E, Z; G, E; G, E; E; E; E; E	Status output to the host is returned for success or error
User Set PIN	Updates User authority PIN. Locking SP Admins can set PINs for any Non-SUM Users.	PBKDF (#A2585); DRBG (#C1278); HMAC-SHA2-256 (#A2596); AES-KW (#A2596)	User Password; AUTH_KEYs; SALT; DRBG-EI; DRBG V; DRBG Key; PSP_HMAC_KEY; TPER_SALT_KEK; TPER_KEK; SUM_KEKs	CO, U	W, E, Z; G, E, Z; G, E; G, E, Z; G, E; G, E; E; E; E; E	Status output to the host is returned for success or error
Enable/Disable User Set PIN	Disables a non-SUM User's ability to change its own PIN.	HMAC-SHA2-256 (#A2596)	PSP_HMAC_KEY	CO	E	Status output to the host is returned for success or error

Service	Description	Approved Security Functions	SSPs	Roles	Access Rights	Indicator
Enable/Disable Admin SP authorities	Enables or disables an Admin SP authority.	PBKDF (#A2585); DRBG (#C1278); HMAC-SHA2-256 (#A2596); AES-KW (#A2596)	CO Password; AUTH_KEYs; SALT; DRBG-EI; DRBG V; DRBG Key; PSP_HMAC_KEY; TPER_SALT_KEK	CO	E; G, E, Z; G, E; G, E, Z; G, E; G, E; E; E	Status output to the host is returned for success or error
Enable/Disable Locking SP authorities	Enables or disables a Locking SP Admins and non-SUM Users.	PBKDF (#A2585); DRBG (#C1278); HMAC-SHA2-256 (#A2596); AES-KW (#A2596)	CO Password; User Password; AUTH_KEYs; SALT; DRBG-EI; DRBG V; DRBG Key; PSP_HMAC_KEY; TPER_SALT_KEK; TPER_KEK	CO	E; E; G, E, Z; G, E; G, E, Z; G, E; G, E; E; E; E	Status output to the host is returned for success or error

Service	Description	Approved Security Functions	SSPs	Roles	Access Rights	Indicator
Enable/Disable SUM	Configures users and ranges in SUM through TCG Reactivate method.	PBKDF (#A2585); DRBG (#C1278); HMAC-SHA2-256 (#A2596); AES-KW (#A2596)	CO Password; User Password; AUTH_KEYs; SALT; DRBG-EI; DRBG V; DRBG Key; PSP_HMAC_KEY; TPER_SALT_KEK; TPER_KEK; SUM_KEKs	CO	W, E, Z; E; G, E, Z; G, E; G, E, Z; G, E; G, E; E; E; G, E, Z; G, E, Z	Status output to the host is returned for success or error
Locking Range Configuration	For non-SUM ranges: Used to modify a range starting address, capacity and attributes of non-SUM ranges. For SUM Policy 1: Used to modify a SUM range starting address, capacity and attributes by Admins if allowed. For SUM Policy 0: Used to modify a SUM range starting address, capacity and attributes by SUM Users if allowed.	DRBG (#C1278); HMAC-SHA2-256 (#A2596); AES-KW (#A2596); AES-XTS (#A2596)	DRBG-EI; DRBG V; DRBG Key; PSP_HMAC_KEY; MEK_KEK; TPER_KEK; SUM_KEKs; MEKs	CO	G, E, Z; G, E; G, E; E; E; E; E; G, E, Z	Status output to the host is returned for success or error

Service	Description	Approved Security Functions	SSPs	Roles	Access Rights	Indicator
Lock/Unlock range	Controls read and write access to a range by either locking or unlocking the LBA range. In Non-SUM, Admins and Users (if allowed by Admins) have access. In SUM, only Users have access.	HMAC-SHA2-256 (#A2596); AES-KW (#A2596); AES-XTS (#A2596)	PSP_HMAC_KEY; TPER_KEK; SUM_KEKs; MEKs	CO, U	E; E; E; E, Z	Status output to the host is returned for success or error
Set common name	Customizes the name of a TCG Authority. Admins and Users (if allowed by Admins) have access.	HMAC-SHA2-256 (#A2596)	PSP_HMAC_KEY	CO, U	E	Status output to the host is returned for success or error
Data store table Set	Writes a stream of bytes to unstructured storage. Admins and Users (if allowed by Admins) have access.	HMAC-SHA2-256 (#A2596)	PSP_HMAC_KEY	CO, U	E	Status output to the host is returned for success or error

Service	Description	Approved Security Functions	SSPs	Roles	Access Rights	Indicator
Crypto Erase of a range	For Non-SUM Ranges: Erases a range by destroying its existing MEK and generating a new one. This service is performed via TCG GenKey method. By default, Admins have access. If Admins allows, Users also have access. For SUM Ranges via TCG Erase method: Erases a range by destroying its existing MEK and generating a new one. The range's LBA range is unlocked, and the User PIN is reset to the NULL password. This service is performed via the TCG Erase method. For SUM Ranges via TCG GenKey method: Erases a range by destroying its existing MEK and generating a new one. This service is performed via the TCG GenKey method.	PBKDF (#A2585); DRBG (#C1278); HMAC-SHA2-256 (#A2596); AES-KW (#A2596); AES-XTS (#A2596)	User Password; AUTH_KEYs; SALT; DRBG-EI; DRBG V; DRBG Key; PSP_HMAC_KEY; MEK_KEK; TPER_SALT_KEK; TPER_KEK; SUM_KEKs; MEKs	CO, U	E; G, E, Z; G, E; G, E, Z; G, E; G, E; E; E; E; E; E; G, E, Z	Status output to the host is returned for success or error

Service	Description	Approved Security Functions	SSPs	Roles	Access Rights	Indicator
Zeroization	Destruction of plaintext keys and CSPs. This service decommissions the drive.	-	DRBG-EI; DRBG V; DRBG Key; HRK; PSP_HMAC_KEY; MEK_KEK; TPER_SALT_KEK; TPER_KEK; SALT; SUM_KEKs; KS_HMAC_KEY; MEKs	M	Z; Z; Z; Z; Z; Z; Z; Z; Z; Z; Z; Z	Status output to the host is returned for success or error

Service	Description	Approved Security Functions	SSPs	Roles	Access Rights	Indicator
PSID Revert	TCG Revert method using PSID. This service returns the Module to its original factory state. The authentication data (PSID) is printed on the label of the Module.	PBKDF (#A2585); DRBG (#C1278); HMAC-SHA2-256 (#A2596); AES-KW (#A2596)	CO Password; AUTH_KEYs; SALT; MSID PIN; DRBG-EI; DRBG V; DRBG Key; PSP_HMAC_KEY; HRK; MEK_KEK; TPER_SALT_KEK; TPER_KEK; SUM_KEKs; MEKs	P	E; G, E, Z; G, E; E; G, E, Z; G, E; G, E; G, E, Z; E; G, E, Z; G, E, Z; Z; Z; G, Z	Status output to the host is returned for success or error

Service	Description	Approved Security Functions	SSPs	Roles	Access Rights	Indicator
Power Cycle (Self-Test)	Powers the module off and on again. This triggers 1. Power-On Self-Tests of the Module. 2. Unblock locked-out authorities that have exhausted their Try Limit. Enable CO authority (Admins SP SID) if it is previously blocked by Block SID Authorization service.	DRBG (#C1278); HMAC-SHA2-256 (#A2596); AES-KW (#A2596); AES-XTS (#A2596); RSA-3072 SigVer (#A2597); SHA2-384 (#A2597);	DRBG V; DRBG Key; PSP_HMAC_KEY; KS_HMAC_KEY; HRK; MEK_KEK TPER_SALT_KEK; MEKs; FW Public Key; Root Public Key	A	G, E, Z; G, E, Z; E; E; E; E; E; E; E; E	Return code for success or error
Hot reset	Resets one of the ports of the Module by performing a PCIe Hot Reset.	-	-	A	-	
Warm reset	Resets the Module by performing an NVMe Subsystem Reset or PCIe Warm reset.	HMAC-SHA2-256 (#A2596)	PSP_HMAC_KEY	A	E	

Service	Description	Approved Security Functions	SSPs	Roles	Access Rights	Indicator
Show Status	This is a set of commands from the TCG and NVMe protocols to read **Security Configuration**. Specifically, this includes NVMe Security Send/Receive, Identify Controller commands, which can be used for reading Approved mode (Initialized/Uninitialized), error messages, and other status information. The Approved Mode indicator is a subset of the NVMe Security Receive command (TCG Level 0 Discovery) and the returned word of the NVMe Identify Controller command (word at offset 4092, bit 0).	-	-	A	-	The Approved Mode indicator is a subset of the NVMe Security Receive command (TCG Level 0 Discovery) and the returned word of the NVMe Identify Controller command (word at offset 4092, bit 0).
Read FIPS Compliance	The Module's FIPS 140 Compliance descriptor (hardware and firmware versions) can be retrieved in the format specified by SFSC specification using TCG IF-RECV command with Protocol Id 0 and ComID 2.	-	-	A	-	The indicator follows the SFSC specification using TCG IF-RECV command with Protocol Id 0 and ComID 2.

Service	Description	Approved Security Functions	SSPs	Roles	Access Rights	Indicator
Block SID Authorization	Disables CO (Admin SP SID) authorization when ownership of the drive is not taken.	-	-	A	-	Status output to the host is returned for success or error.
TCG Authorization	Authorizes an operator using TCG PIN through Start session or TCG Authentication method.	PBKDF (#A2585); DRBG (#C1278); HMAC-SHA2-256 (#A2596); AES-KW (#A2596)	CO Password; User Password; AUTH_KEYs; SALT; PSID PIN; DRBG-EI; DRBG V; DRBG Key; PSP_HMAC_KEY; TPER_SALT_KEK; TPER_KEK; SUM_KEKs	A	W, E, Z; W, E, Z; G, E, Z; G, E; W, E; G, E, Z; G, E; G, E; E; E; G, E; E	Status output to the host is returned for success or error.
Enable Zeroization Service	Authorizes the Zeroization service for the Maker role.	DRBG (#C1278); RSA-2048 SigVer (#A2595); SHA2-256 (#A2596)	DRBG-EI; DRBG V; DRBG Key; Maker Public Key	A	G, E, Z; G, E; G, E; E	Status output to the host is returned for success or error.

Service	Description	Approved Security Functions	SSPs	Roles	Access Rights	Indicator
Get Random Number	TCG Random method used to generate and output a random number from the DRBG.	DRBG (#C1278)	DRBG-EI; DRBG V; DRBG Key	A	G, E, Z; G, E; G, E	Status output to the host is returned for success or error.
Telemetry logs	The Module allows the collection of debugging information through NVMe log pages. The purpose of the telemetry log data is to provide information required to debug firmware issues remotely. No sensitive information is included.	-	-	A	-	Status output to the host is returned for success or error.
Read/Write User Data	Reads/Writes user data. In uninitialized mode, this service is always successful. In initialized mode, this service is only successful if the range is unlocked for read/write access via Lock/Unlock range service.	AES-XTS (#A2596)	MEKs	A	E	Status output to the host is returned for success or error.

Service	Description	Approved Security Functions	SSPs	Roles	Access Rights	Indicator
Firmware Update	Loads a firmware image. All firmware loaded into the module is validated with RSA signature verification over the entire firmware image.	AES-KW (#A2596); HMAC-SHA2-256 (#A2596); RSA-3072 SigVer (#A2595); SHA2-384 (#A2595)	HRK; KS_HMAC_KEY; FW Public Key; Root Public Key	CO	E; E; E; E	Status output to the host is returned for success or error.
Format NVM / Namespace Management	Wipes the data of a particular namespace by generating new MEK. This service is only successful if the range is unlocked for read/write access via Lock/Unlock range service.	DRBG (#C1278); HMAC-SHA2-256 (#A2596); AES-KW (#A2596); AES-XTS (#A2596)	DRBG-EI; DRBG V; DRBG Key; PSP_HMAC_KEY; MEK_KEK; TPER_KEK; SUM_KEKs; MEKs	A	G, E, Z; G, E; G, E; E; E; E; E; G, E, Z	Status output to the host is returned for success or error.

Service	Description	Approved Security Functions	SSPs	Roles	Access Rights	Indicator
Sanitize	Wipes the data of a particular namespace by generating new MEK. This service is accessible only in Uninitialized mode.	DRBG (#C1278); HMAC-SHA2-256 (#A2596); AES-KW (#A2596); AES-XTS (#A2596)	DRBG-EI; DRBG V; DRBG Key; PSP_HMAC_KEY; MEK_KEK; MEKs	A	G, E, Z; G, E; G, E; E; E; G, E, Z	Status output to the host is returned for success or error.
Configure Drive	Enables or disables IEEE1667 protocol support.	-	-	A	-	Status output to the host is returned for success or error.

5 Software/Firmware Security

The firmware components are protected by an RSA signature.
The operator can initiate the integrity test on demand by power cycling or resetting the module.

6 Operational Environment

The Module has a limited operational environment under FIPS 140-3 definitions. The tested operational environments are listed in Table 2. The Module includes a firmware load service to support necessary updates. The Module will not load or execute firmware which is not signed with SK hynix 3072-bit RSA Private Key. Firmware versions validated through the FIPS 140-3 CMVP will be explicitly identified on a validation certificate. Any firmware not identified in this Security Policy does not constitute the Module defined by this Security Policy or covered by this validation.

Please see the operator instructions provided in Section 11 for the initialization, un-initialization, and sanitation of the module.

7 Physical Security Policy

The Module meets commercial-grade specifications for power, temperature, reliability, and shock/vibrations. The Module uses standard passivation techniques and only asserts compliance with Level 1 physical security requirements.

8 Non-Invasive Security

The Module does not implement any mitigation method against non-invasive attack.

9 Sensitive Security Parameter (SSP) Management

CSPs and PSPs are defined in the tables below. The following legend is used to describe the generation, storage, input, output, and zeroization methods:

- G1 Generated external to the Module and installed during manufacturing
- G2 Unmodified output of the internal ENT (P) during power-up
- G3 Derived from the DRBG output per SP800-90Ar1
- G4 Derived from PBKDF2
- G5 Symmetric key generated by internal CAVP validated DRBG
- S1 Only stored in volatile, dynamic RAM in plaintext
- S2 Stored in static eFUSE in plaintext, associated by memory location (index)
- S3 Stored in static NAND encrypted with AES-KW by the HRK, associated by memory location (index)

- S4 Stored in static NAND in plaintext, associated by memory location (index)
- S5 Stored in dynamic RAM in plaintext, associated by memory location (index)
- S6 Stored in static NAND encrypted obfuscated (treated as plaintext) with AES-KW using the AUTH_KEY, associated by memory location (index)
- S7 Stored in static NAND encrypted with AES-KW using SUM_KEK, TPER_KEK, or MEK_KEK, associated by memory location (index)
- S8 Stored in static NAND encrypted with AES-KW using the TPER_SALT_KEK, associated by memory location (index)
- S9 Stored in plaintext as part of static firmware, which is RSA signed
- I1 Input in plaintext (Non-SSPs only)
- O1 Plaintext to host (Non-SSPs only)
- Z1 Zeroized by Module power cycle or hard reset
- Z2 Zeroized by the "Zeroization" service by overwriting with zeroes or ones
- Z3 Zeroize after service completion by overwriting the RAM location by zeroes

9.1 Sensitive Security Parameters

All SSPs used by the Module are described in this section.

Table 13: SSPs

SSP	Strength	Security Function/ Cert.	Generation	Import/Export	Establishment	Storage	Zeroization	Description / Usage
DRBG-EI	384	ENT (P)	G2	N/A	N/A	S1	Z1, Z2	Deterministic Random Bit Generator – Entropy Input string and seed. Size: 384 bits of entropy data. Instantiates the DRBG to 256 bits of security strength.
DRBG V	128	DRBG Cert. #C1278	G3	N/A	N/A	S1	Z1, Z2	The secret value *V* (128 bits) in the current DRBG internal working state
DRBG Key	256	DRBG Cert. #C1278	G3	N/A	N/A	S1	Z1, Z2	The secret *Key* (256 bits) in the current DRBG internal working state
HRK	256	AES-KW Cert. #A2596	G5	N/A	N/A	S2	Z2	Hidden Root Key Type: AES wrapping key Purpose: Used to wrap following keys: PSP_HMAC_KEY,

SSP	Strength	Security Function/ Cert.	Generation	Import/Export	Establishment	Storage	Zeroization	Description / Usage
								MEK_KEK, TPER_SALT_KEK, and KS_HMAC_KEY.
PSP_HMAC_KEY	256	HMAC Cert. #A2596	G5	N/A	N/A	S3, S5	Z1, Z2, Z3	Public Security Parameter HMAC Key Type: 256-bit Purpose: Key is used to check the integrity of the SALT and PSID PIN
KS_HMAC_KEY	256	HMAC Cert. #A2596	G5	N/A	N/A	S3, S5	Z1, Z2, Z3	Key Storage HMAC Key Type: 256-bit Purpose: Key is used to check the integrity of the FW Public Key and Root Public Key
MEK_KEK	256	AES-KW Cert. #A2596	G5	N/A	N/A	S3, S5	Z1, Z2, Z3	Type: AES 256 Purpose: Key wraps the MEKs when in the Uninitialized state
TPER_SALT_KEK	256	AES-KW Cert. #A2596	G5	N/A	N/A	S3, S5	Z1, Z2, Z3	Type: AES 256 Purpose: Key wraps the SALT.
TPER_KEK	256	AES-KW Cert. #A2596	G5	N/A	N/A	S5, S6	Z1, Z2, Z3	Type: AES 256 Purpose: Key wraps the MEKs for OPAL.
SUM_KEKs	256	AES-KW Cert. #A2596	G5	N/A	N/A	S5, S6	Z1, Z2, Z3	Type: AES 256 Purpose: It is the key wrapping key used for MEKs for SUM.
MEKs	256	AES-XTS Cert. #A2596	G5	N/A	N/A	S5, S7	Z1, Z2, Z3	Type: AES 256 Purpose: MEK_0 is the Global Range Key. MEK_{1-8} keys are used for User data encryption in XTS mode.
AUTH_KEYs (Non-SSP)	N/A	PBKDF Cert. #A2595	G4	N/A	N/A	S1	Z1, Z3	Type: AES 256-bit key wrap key derived from PBKDF using the CO or User password, which may be 0 length. Purpose: Key is used for TPER_KEK (OPAL) and

SSP	Strength	Security Function/ Cert.	Generation	Import/Export	Establishment	Storage	Zeroization	Description / Usage
								SUM_KEK (SUM) obfuscation.
CO Password (Non-SSP)	N/A	PBKDF Cert. #A2595	N/A	I1	N/A	S1	Z1, Z3	Crypto Officer password Type: Password Purpose: May be used for authorizing the CO role
User Passwords (Non-SSP)	N/A	PBKDF Cert. #A2595	N/A	I1	N/A	S1	Z1, Z3	User Password Type: Password Purpose: May be used for authorizing User roles
SALT (Non-SSP)	256	PBKDF Cert. #A2595	G5	N/A	N/A	S5, S8	Z1, Z2, Z3	256-bit non-secret salt used as input to = PBKDF. A unique salt is associated with the derivation of each AUTH_KEY.
PSID PIN (Non-SSP)	N/A	PBKDF Cert. #A2595	G1	I1	N/A	S5	Z1	32 byte PIN is used to access the TCG Revert service. The PSID PIN is visibly printed on a production label on the Module.
MSID PIN (Non-SSP)	N/A	PBKDF Cert. #A2595	G1	I1, O1	N/A	S5, S9	Z1	32 byte default PIN is used to authorize the Initialize service. It can be displayed via the Show Status/Read Security Configuration service.
FW Public Key (Non-SSP)	128	RSA Cert. #A2595, #A2597	G1	N/A	N/A	S4, S5	N/A	Type: 3072 bit RSA Public Key Purpose: Key is used for RSA signature verification of the firmware image.
Maker Public Key (Non-SSP)	112	RSA Cert. #A2595	G1	N/A	N/A	S5, S9	N/A. Protected by RSA Signature.	Type: 2048 bit RSA Public Key Purpose: Key is used to access Zeroise service.
Root Public Key (Non-SSP)	150	RSA Cert. #A2595, #A2597	G1	N/A	N/A	S4, S5	N/A	Type: 4096 bit RSA Public Key Purpose: Key is used to validate the chain

SSP	Strength	Security Function/ Cert.	Generation	Import/Export	Establishment	Storage	Zeroization	Description / Usage
								of trust for the FW Public Key.

Table 14: Non-Deterministic Random Number Generation Specification

Entropy Source	Minimum Number of Bits of Entropy	Details
ENT (P)	Min-entropy of 1 per 1-bit sample	This ENT (P) has been evaluated according to the non-IID evaluation path of the [SP800-90B] standard.

10 Self-Tests

Each time the Module is powered up, tests are run to guarantee the proper functioning of the crypto algorithms. Power on self-tests are available on demand by power cycling or resetting the Module. The module zeroises all temporary values used as part of the pre-operational and conditional self-tests

On power-on or reset, the Module performs self-tests as described in the tables below. All KATs must be completed successfully prior to any other use of cryptography by the Module. If one of the KATs fails during the ROM boot stage of the device, then the Module enters an internal error state. If the Module has exited ROM boot stage, the Module enters SELF_TEST_ERROR state which can be retrieved by NVMe Identify Controller command word at offset 4092, bit 0 will be 1. Power cycle is required to recover the Module from self-test failure.

Table 15: Pre-Operational and Conditional Self-Tests performed at Power-On

Test Target	Description	Failure Behavior
Firmware Integrity	RSA 3072 and SHA2-384 verification performed over all firmware located in NAND storage on the Atomos controller.	Enters INTERNAL_STATE_ERROR state. SMBus bytes offset 243, bit 7 will be 1b.
ENT (P)	Performs ENT (P) startup test. Generates 32 byte noise that will force RCT and APT on 1536 bits.	Enters SELF_TEST_ERROR state.

Table 16: Additional Conditional Self-Tests

Test Target	Description	Failure Behavior
AES-KW Decrypt Cert.# A2596	KAT: Decryption only Mode: KW Key size: 256 bits	Enters INTERNAL_STATE_ERROR state
AES-KW Cert.# A2596	KATs: Both forward and inverse ciphers are tested via encryption and decryption. Modes: KW Key size: 256 bits Note: This test covers AES-ECB and AES-XTS as per IG 10.3.A	Enters SELF_TEST_ERROR state.

Test Target	Description	Failure Behavior
AES-Conditioner Cert.# A2272	KAT: Encryption only, exercises the SP800-90B conditioner. Modes: ECB Key size: 256 bits	Enters SELF_TEST_ERROR state.
AES XTS Key generation	An IG C.I key comparison test is performed on Key1 and Key2 for each generation.	Enters SELF_TEST_ERROR state.
DRBG Cert.# C1278	Performs a fixed input KAT inclusive of the SP 800-90Ar1 instantiate, generate, and reseed health tests. Mode: CTR_DRBG	Enters SELF_TEST_ERROR state.
DRBG Cert.# C1278	SP800-90Ar1 Health Tests (Instantiate, Generate, Reseed)	Enters SELF_TEST_ERROR state.
ENT (P)	SP800-90B Health Tests (RCT and APT)	Enters SELF_TEST_ERROR state.
HMAC (SoC HW) Cert.# A2596	Performs HMAC generates and verify KATs using a 256-bit key and SHA2-256 Note: SHA2-256 is covered by HMAC KAT per IG 10.3.B	Enters INTERNAL_STATE_ERROR state. Status output data via SMBus bytes offset 243, bit 7 will be 1b.
PBKDF2 Cert.# A2595	Performs KAT using a known password and HMAC-SHA2-256 (Satisfies the HMAC KAT).	Enters SELF_TEST_ERROR state.
RSA (ROM) Cert.# A2597	KAT: RSA PSS verify with 3072 bit key and SHA2-384 (Cert. #A2597). Note: SHA2-384 KAT is included in this test. This test is performed prior to the Firmware Integrity Test.	Enters INTERNAL_STATE_ERROR state. Status output data via SMBus bytes offset 243, bit 7 will be 1b
RSA (FW) Cert.# A2595	KAT: RSA PSS verify with 2048 bit key and SHA2-512 (Cert. #A2595). Note: RSA 3072 and 4096 key sizes are covered by testing 2048 bit key. SHA2-512 KAT is included in this test.	Enters SELF_TEST_ERROR state
Firmware Load Test	The Module performs a RSA 3072 signature verification on all firmware loaded into the Module.	The Module returns invalid image for download commit command and the image is discarded.

11 Life-Cycle Assurance

The Module design corresponds to the Module Security rules. This section documents the Cryptographic Officer instructions that are necessary to implement in order to maintain compliance with FIPS 140-3 security requirements.

11.1 Cryptographic Officer Initialization

The Module is shipped from the factory in an Approved mode of operation (uninitialized state). The keys generated during manufacturing are used to encrypt/decrypt the user data. The shipping container protecting the Module or set of Modules in transit should be verified for evidence of tampering.

The CO should initialize the Module by taking the following steps:

11.1.1 Verifying the Module is in an Approved Mode of Operation

To verify that a module is in the Approved mode of operation the operator will perform the **Read FIPS Compliance** by issuing TCG IF-RECV command with Protocol Id 0 and ComID 2. Refer [SFSC] spec.

For example, the sample of data below is returned from the module:

```
----------------FIPS 140 compliance descriptor-----------------------
 COMPLIANCE DESCRIPTOR INFORMATION LENGTH -> 528
 COMPLIANCE DESCRIPTOR DESCRIPTOR TYPE -> 1
 COMPLIANCE DESCRIPTOR DESCRIPTOR LENGTH -> 520
 COMPLIANCE DESCRIPTOR RELATED STANDARD -> 51[1]
 COMPLIANCE DESCRIPTOR OVERALL SECURITY LEVEL -> 49[2]
 COMPLIANCE DESCRIPTOR HARDWARE VERSION -> HFS1T9GEEWX132N
 COMPLIANCE DESCRIPTOR VERSION ->51082A30
 COMPLIANCE DESCRIPTOR MODULE NAME -> SK hynix PE9110 E1.S and PE9010 M.2
22110D NVMe TCG Opal SSC SEDs
--------------------------------------------------------------------
```

11.1.2 Initialize the Module

1. Take Ownership - Set Admin SP SID.
2. Activate Opal with Single User Mode.
3. Set WriteLockEnabled and ReadLockEnabled column of all valid Locking ranges.
4. Power cycle the Module.
5. Verify the module is in initialized mode by checking the
   - LockingEnabled bit of the TCG Level 0 Discovery Locking Feature Descriptor is set to 1.
   - WriteLockEnabled and ReadLockEnabled columns of all valid Locking ranges in the Locking Table are set to True.

11.2 Un-Initialize the Module

The Deactivate OPAL may be invoked by an authorized role to affect a transition into the uninitialized state of operation. The PSID Revert may be done by the PSID role to affect a

[1] "51" is an ASCII data field that indicates "FIPS 140-3" per the Security Features for SCSI Commands, Revision 2, Section 5.1.5.3

[2] "49" is an ASCII data field that indicates the FIPS 140 overall security level of "1" per the Security Features for SCSI Commands, Revision 2, Section 5.1.5.3.

transition into the uninitialized state of operation. This is analogous to restoring the module to the factory default state.

11.3 Sanitization

The Zeroization service may be invoked to destroy all SSPs and render the module inoperable.

12 Mitigation of Other Attacks Policy

The Module does not support the mitigation of other attacks outside the scope of FIPS 140-3.

13 References and Definitions

The following standards are referred to in this Security Policy

Table 17: References

Acronym	Full Specification Name
[FIPS140-3]	Security Requirements for Cryptographic Modules, March 22, 2019
[ISO19790]	International Standard, ISO/IEC 19790, Information technology — Security techniques — Test requirements for cryptographic modules, Third edition, March 2017
[ISO24759]	International Standard, ISO/IEC 24759, Information technology — Security techniques — Test requirements for cryptographic modules, Second and Corrected version, 15 December 2015
[180-4]	NIST, *Secure Hash Standard*, FIPS Publication 180-4, August 2015
[186-4]	NIST, *Digital Signature Standard (DSS)*, FIPS Publication 186-4, July 2013
[197]	NIST, *Advanced Encryption Standard (AES)*, FIPS Publication 197, November 26, 2001
[198-1]	NIST, *The Keyed-Hash Message Authentication Code (HMAC)*, FIPS Publication 198-1, July 2008
[IG]	NIST, *Implementation Guidance for FIPS PUB 140-3 and the Cryptographic Module Validation Program,* last updated October 7, 2022
[NVMe]	Standard spec available online https://nvmexpress.org/wp-content/uploads/NVM-Express-1_3c-2018.05.24-Ratified.pdf Revision 1.3C May 24, 2018
[PKCS#1]	*PKCS #1 v2.1: RSA Cryptography Standard*, RSA Laboratories, June 14, 2002
[SFSC]	Information technology – Security Features for SCSI Commands (SFSC)
[38A]	NIST Special Publication 800-38A, *Recommendation for Block Cipher Modes of Operation*, December 2001
[38E]	NIST Special Publication 800-38E, Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices, January 2010
[38F]	NIST Special Publication 800-38F, *Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping,* December 2012
[90Ar1]	*National Institute of Standards and Technology, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, Special Publication 800-90A Revision 1, June 2015.*
[90B]	*National Institute of Standards and Technology, Recommendation for the Entropy Sources Used for Random Bit Generation, Special Publication 800-90B, January 2018.*
[132]	NIST Special Publication 800-132, *Recommendation for Password-Based Key Derivation,* December 2010
[133r2]	NIST Special Publication 800-133 Revision 2, *Recommendation for Cryptographic Key Generation,* June 2020
[TCG Core]	*TCG Storage Architecture Core Specification, version 2.01 Revision 1.0, 5 August 2015*
[TCG Opal]	*TCG Storage Security Subsystem Class: Opal Specification, Version 2.01 Revision 1.00, 5 August 2015*
[TCG SIIS]	*TCG Storage Interface Interactions Specification (SIIS), Version .08, 14 August 2018*

Acronym	Full Specification Name
[TCG ADS]	*TCG Storage Opal SSC Feature Set: Additional Datastore Tables Specification, Version 1.00 Revision 1.00, 24 February 2012*
[TCG SUM]	*TCG Storage Opal SSC Feature Set: Single User Mode Specification, Version 1.00 Revision 2.00, 5 August 2015*
[TCG PSID]	*TCG Storage Opal SSC Feature Set: PSID, Version 1.00 Revision 1.00, 5 August 2015*
[TCG Block SID]	*TCG Storage Feature Set: Block SID Authentication, Version 1.00 Final, Revision 1.00, 5 August 2015*
[IEEE 1667]	*IEEE Std 1667-2018 – IEEE Standard for Discovery, Authentication, and Authorization in Host Attachments of Storage Devices, February 2018*

Table 18: Acronyms and Definitions

Acronym	Definition
ACE	Access Control Elements
AES	Advanced Encryption Standard
APT	Adaptive Proportion Test
CO	Cryptographic Officer
CSP	Critical Security Parameter, see [FIPS 140-3]
DRBG	Deterministic Random Bit Generator
ECB	Electronic Code Book mode of AES Encryption/Decryption
KAT	Known Answer Test
PBKDF	Password Based Key Derivation Function
LBA	Logical Block Address
MSID	Manufactured Security Identifier
MEK	Media Encryption Key
NVMe	Non-Volatile Memory express
PBKDF	Password Based Key Derivation Function
PCIe	Peripheral Component Interconnect Express
PSP	Public Security Parameter
PIN	Personal Identification Number (or Password)
PSID	Physical Security Identifier
RCT	Repetitive Count Test
RSA	Rivest Shamir Adleman
SHA	Secure Hash Algorithm
SED	Self-Encrypting Drive
SID	Security Identifier
SSD	Solid-state Drive
SSC	Security Subsystem Class
TCG	Trusted Computing Group
UID	Unique Identifier
VU	Vendor Unique

XTS	**X**EX **T**weakable Block Cipher with Cipher text **S**tealing