SK hynix PE8110 M.2 22110D NVMe TCG Opal SSC SED

HFS960GDE0X098N

HFS1T9GDE0X098N

HFS3T8GDE0X098N

FIPS 140-2 Cryptographic Module
Non-Proprietary Security Policy

Document Version: 1.4
Date: 1/27/2023

CHANGE RECORD

Revision	Date	Author	Description of Change
1.0	10/28/2021	Yongtae Kim	First release
1.1	7/28/2022	Yongtae Kim	Response to CMVP Comments
1.2	10/11/2022	Yongtae Kim	Update firmware version
1.3	1/6/2023	Yongtae Kim	Added Section 8.4 Firmware Update
1.4	1/27/2023	Yongtae Kim	Updated entropy test description in Table 14

Table of Contents

List of Tables

List of Figures

1 Introduction

This document defines the Security Policy for the SK hynix PE8110 M.2 22110D NVMe TCG Opal SSC SED 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. It 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 140-2 overall security Level 1.

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

Table 1: Security Level of Security Requirements

Security Requirement	Security Level
Cryptographic Module Specification	1
Cryptographic Module Ports and Interfaces	1
Roles, Services, and Authentication	1
Finite State Model	1
Physical Security	1
Operational Environment	N/A
Cryptographic Key Management	1
EMI/EMC	1
Self-Tests	1
Design Assurance	1
Mitigation of Other Attacks	N/A
Overall Level	1

The Module has the following configurations:

Table 2: Module Configurations

	HW P/N and Version	FW Version	Description
1	HFS960GDE0X098N	41081A10	960GB
2	HFS1T9GDE0X098N	41081A10	1.9TB
3	HFS3T8GDE0X098N	41081A10	3.8TB

1.1 Hardware and Cryptographic Boundary

The Module is designed to be embedded in a General Purpose Computer (host) and is connected through the PCIe connecter. The module does not support a maintenance access interface.

The Module PE8110 has an M.2 22110D physical form factor as depicted in Figure 1. The components exposed are depicted in Figure 2 and Figure 3. The cryptographic boundary is defined as the entire PCB as indicated by the red outline in Figure 2 and Figure 3.

Figure 1: PE8110 M.2 22110D Form Factor

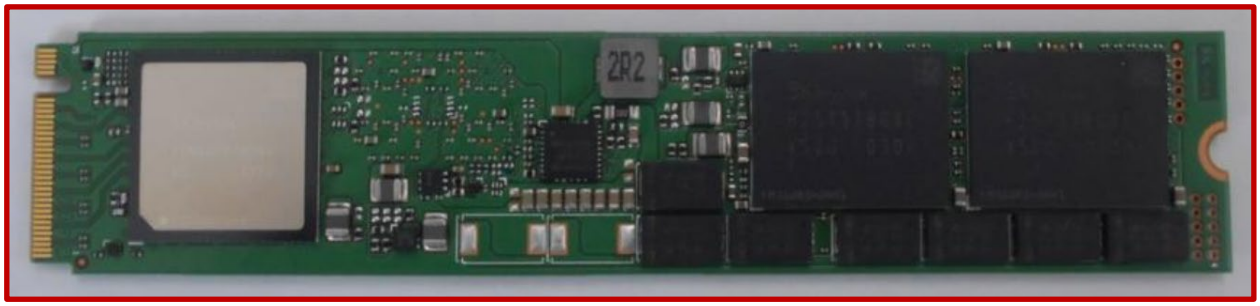

Figure 2: Top View with Physical Cryptographic Boundary

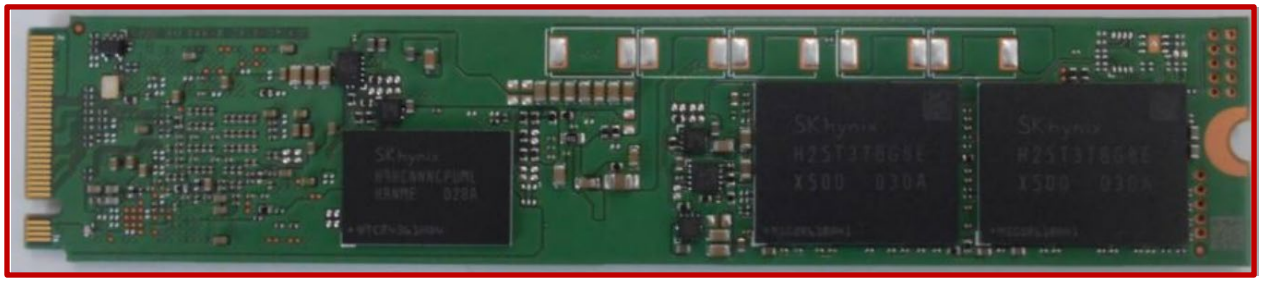

Figure 3: Bottom View with Physical Cryptographic Boundary

Table 3: Ports and Interfaces

Port	Interfaces	Description	Logical Interface Type
PCIe Connector	Power	Power Connector	Power
	NVMe	NVMe interface	Control in, Data in, Data out, Status out
	SMBus	Management Interface	Control in, Status out
JTAG		Debug Port (permanently disabled)	N/A
UART		Debug Port (permanently disabled)	N/A

1.1.1 NVMe Interface

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

1.1.2 SMBus Interface

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

1.2 Block Diagram with Cryptographic Boundary

The Module uses a single chip controller (Aquarius) with a PCIe/NVMe and SMBus interface on the systems side and SK hynix NAND flash internally. The following figure depicts the Module operational environment. The red outline in Figure 4 below depicts the cryptographic boundary which is the physical boundary as depicted above (Figure 3). All firmware runs on the controller within this boundary.

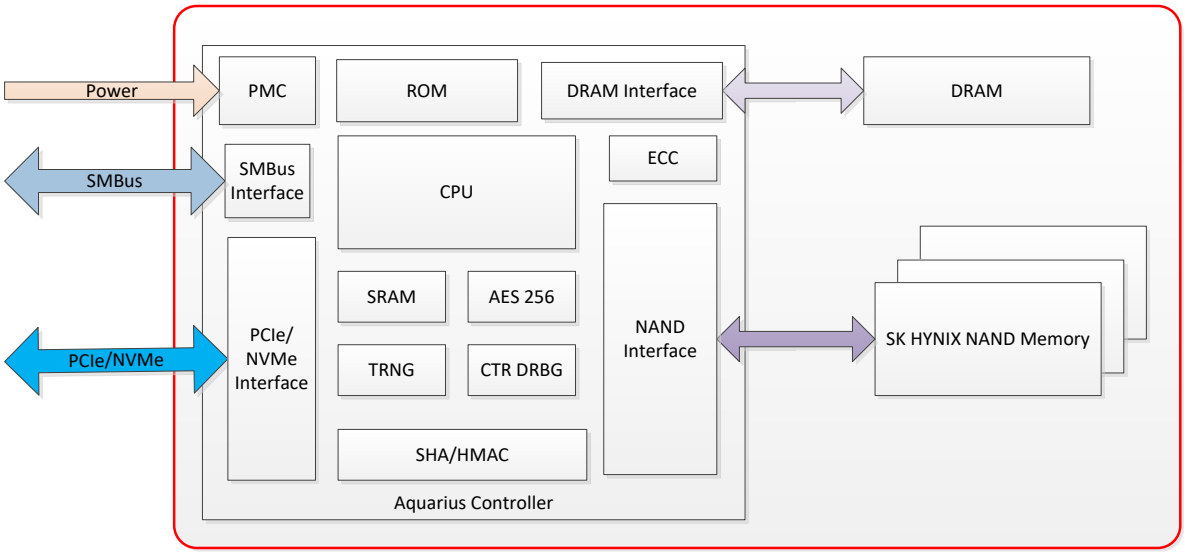

Figure 4: Module Block Diagram

The Module is composed of the following components:

- **Aquarius 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 Aquarius controller, and other non-volatile configuration data needed by the Aquarius controller during execution.

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

1.3 Mode of Operation

The Module is always in the FIPS Approved Mode of operation. The module has two distinct operational modes in the approved mode of operation as described below.

- **Uninitialized Mode** – In this operational state, the ownership of the drive is not taken. Once the ownership is taken, the module transitions to initialized mode.
- **Initialized Mode** - In this operational state, the ownership of the drive is taken. To initialize the drive, the module owner must take ownership of the device and activate Locking SP by following steps in the Crypto Officer Initialization section from the uninitialized mode.

2 Cryptographic Functionality

The Module implements the FIPS Approved cryptographic functions listed in the tables below. The term FIPS Approved cryptographic function is defined by FIPS 140-2 specifications.

Table 4: Approved Cryptographic Functions

Cert	Algorithm	Mode	Description	Functions/Caveats
A913	AES [197]	ECB [38A]	Key Sizes: 256 Boundary: Hardware	Encrypt, Decrypt Underlying for XTS, KW, and CTR_DRBG
		XTS [38E]	Key Sizes: 256 Per IG A.9, the module assures Key_1 and Key_2 are not equal. Boundary: Hardware	Encrypt, Decrypt
A913	AES [197]	KW [38F]	Forward Key Sizes: 256 Boundary: Hardware	Authenticated Encrypt, Authenticated Decrypt
VA	CKG [IG D.12]	[133 Rev2] Section 6.1[1]		Direct Symmetric Key generation using unmodified DRBG output
		[133 Rev2] Section 6.2.3[2]		Derivation of symmetric keys from a Password
A912	DRBG [90A]	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 Additional Input used: 256 Bits Entropy Input used: 1792 Bits Nonce used: 896 Bits Personalization String: 256 Bits	Deterministic Random Bit Generation

[1] CKG – The module performs Cryptographic Key Generation (CKG) meeting the requirements in FIPS 140-2 IG D.12 and SP 800-133 rev2, Section 6.1. The generated symmetric key is the unmodified output from the Approved SP 800-90A AES-256 CTR DRBG.

[2] CKG – The module performs Cryptographic Key Generation (CKG) meeting the requirements in FIPS 140-2 IG D.12 and SP 800-133 rev2, Section 6.2.3. The symmetric key is derived from a password using the Approved SP 800-132 PBKDF. The key can only be used for storage applications.

Cert	Algorithm	Mode	Description	Functions/Caveats
			Boundary: Firmware	
A913	HMAC [198-1]	SHA-256	Key Sizes: 256 bits λ = *32 bytes* Boundary: Hardware	Integrity Check Public Security Parameter (PSP) and PBKDF
ENT (P)	ENT (P) [90B] [Annex C]	–	Hardware Non-Deterministic RNG; minimum of 512 bits per access. Boundary: Hardware	The ENT (P) output is used to seed the Approved DRBG. Synopsys
A912	PBKDF [132]	Option 1a	sLen = 32 bytes salt C = 1,000 iterations HMAC SHA-256 Cert. #A913 Boundary: Firmware	Password Based Key Derivation. The keys derived from passwords are used only in storage application. The probability of guessing the key is 1/(2^256) = 1.16e+77.
A912	RSA [186-4]	PSS	n = 2048 SHA 256 Boundary: Firmware	SigVer - Digital Signature verification (Firmware Download, Maker Authentication) Firmware
A914	RSA [186-4]	PSS	n = 2048 SHA 256 Boundary: Hardware	SigVer - Digital Signature verification (ROM Secure Boot) Hardware
A913	SHS [180-4]	SHA-256	Boundary: Hardware	Firmware Integrity Self-Test and HMAC-SHA-256

2.1 Critical Security Parameters

All CSPs used by the Module are described in this section. All usage of these CSPs is described in the services detailed in Section 4.

Table 5: Critical Security Parameters

CSP	Description / Usage
DRBG-EI	Deterministic Random Bit Generator – Entropy Input Size: 1792 bits of entropy data. Provides 268 bits of security strength. (268.8 bits of min-entropy input without a nonce.)
DRBG V	The secret value *V* (128 bits) in the current DRBG internal working state
DRBG Key	The secret *Key* (256 bits) in the current DRBG internal working state
DRBG seed_material	The DRBG-internal seed_material value (2944 bits) used within the CTR_DRBG algorithm
CO Password	Crypto Officer password Type: Password Purpose: used for authenticating the CO role
User Password	User Password Type: Password Purpose: used for authenticating User roles
HRK	Hidden Root Key Type: AES wrapping key Purpose: Used to wrap following keys: PSP_HMAC_KEY, MEK_KEK, TPER_SALT_KEK, and KS_HMAC_KEY.
PSP_HMAC_KEY	Public Security Parameter HMAC Key Type: 256-bit Purpose: Key is used for PSP Integrity Check
MEK_KEK	Type: AES 256 Purpose: Key wraps the MEKs.
TPER_SALT_KEK	Type: AES 256 Purpose: Key wraps the SALT PSP.
KS_HMAC_KEY	Type: HMAC Purpose: Key is used to RSA public key integrity check
TPER_KEK	Type: AES 256 Purpose: Key wraps the MEKs.
SUM_KEK_i	Where *i* is 0-8 keys. Type: AES 256 Purpose: It is the key wrapping key used for MEKs.
MEK_j	Where *j* is 0-8 keys. Type: AES 256 Purpose: MEK_0 is the Global Range Key. MEK_{1-8} keys are used for User data encryption.
$AUTH\_KEY_m$	Where *m* is 0-15 keys. Type: key derived from PBKDF2 using password provided by the host. This includes the CO and User passwords. Purpose: Key is used for KEK wrapping.

2.2 Public Security Parameters

Table 6: Public Security Parameters

Key	Description / Usage
SALT	This is the 256-bit salt used as input to the PBKDF2. A unique salt is associated with the derivation of each AUTH_KEY.
PSID PIN	This 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	This 32-byte default PIN is used to authenticate the CO role (Admin SP SID) during the Initialize service. It can be displayed via the Show Status/Read Security Configuration service.
FW Public Key	Type: 2048-bit RSA Public Key Purpose: Key is used for RSA signature verification of the firmware image.
Maker Public Key	Type: 2048-bit RSA Public Key Purpose: Key is used to authenticate Maker role to access Zeroize service.

3 Roles, Authentication and Services

3.1 Assumption of Roles

The module supports Cryptographic Officer (CO), User, Maker and PSID roles. The method for assuming a role is explicit by the TCG authentication. The operator of the module is not required to authenticate as this is a Level 1 module. However, a password authentication is required to assume CO, User and PSID role as per the module design, although the provided mechanism does not fully comply with FIPS authentication requirement and so cannot be claimed as Authentication in this context.

The cryptographic module enforces the separation of roles by enforcing re-authentication with the appropriate password (or PIN) when changing roles. Note that although each TCG role includes a unique identifier (UID) as part of the authentication process, authentication is still considered role-based because the UID corresponds to the TCG role itself, not an individual operator.

Table 7 lists all operator roles supported by the module. The Module does not support a maintenance role and/or bypass capability. The Module does not support concurrent operators. Authentication data is stored encrypted and never output from the module. Authentication is cleared during each power cycle.

Table 7: Authenticated Roles

Role Name	Description / Corresponding Roles	Authentication Data	Authentication Type
CO	Crypto Officer – - **Admin SP SID -** This role is responsible for transitioning from uninitialized mode to initialized mode. - **Admin SP Admin 1 –** This role is disabled by default but can be enabled by SID authority. When enabled, it can transition the Module back to uninitialized mode from initialized mode. - **Locking SP Admin 1, 2, 3, and 4** –This role is used to enable and disable Users, create and delete user ranges, lock or unlock the ranges and cryptographically erase the user ranges.	Password - After five (5) failure attempts requires power cycle to authenticate again	Authentication is not required for FIPS 140-2 Level 1. A password mechanism is provided but does not comply with FIPS 140-2.
User	User – - **Locking SP User 1 – 9** - This role 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.	Password - After five (5) failure attempts requires power cycle to authenticate again	Authentication is not required for FIPS 140-2 Level 1. A password mechanism is provided but does not comply with FIPS 140-2.

Maker	Maker – This is an assumed role which enables the operate to execute Zeroize Service command.	RSA Signature - After five (5) failure attempts requires power cycle to authenticate again	Role-based
PSID	**TCG PSID Authority** – This authority is considered an authenticated role because the PSID PIN (32 bytes) must be entered to perform the PSID Revert as an authenticated service. The PSID PIN is intended to only be available to an operator that is physically present with the Module. This role is used to access PSID Revert service.	PIN After five (5) failure attempts requires power cycle to authenticate again	Authentication is not required for FIPS 140-2 Level 1. A PIN mechanism is provided but does not comply with FIPS 140-2.

Table 8: Unauthenticated Roles

Role Name	Description
Anybody	- **TCG Anybody Authority** – This authority is considered unauthenticated because no password is needed for this authority. This authority can read the MSID PIN, and other security configuration data through TCG Get method. It has a 64-bit UID.

3.2 Authentication Methods

The module supports PIN authentication and RSA Signature verification methods. The strength of authentication is described in Table 9.

Table 9: Authentication Description

Authentication Method	Description
Password (or PIN)	The module's minimum Password/PIN length is zero bytes, but a 32 byte length is recommended. If a particular Password/PIN has a length of zero bytes, then authentication by Password/PIN is disabled.
RSA Signature	Key Length is 2048-bit, Key strength is equal to 112 bits. RSA 2048 has a key strength of 112 bits, which is the minimum approved by CMVP. The probability of guessing the key of 112 bit strength is 1/(2^112) = 1/(5.19e+33) = 1.9e-34, which is less than 1/1,000,000. This effectively eliminates the possibility of determining the private key through exhaustive methods. Each verification takes 86 milliseconds. Limiting it to less than 11 attempts per second. After five (5) consecutive unsuccessful authentication attempts have occurred, the Module requires a reset before any more login attempts can be attempted. The reset time required in performing a reset to the Module is eight (8) seconds. Therefore, a maximum of (60/(11 + 8))*5 = 15 attempts are possible in one minute and the probability that a false acceptance occurs over a one minute interval is 15/ 2^112 = 2.89e-33, which is smaller than 1/100,000.

3.3 Services

All services implemented by the Module are listed in the tables below. CSP usage for each service described is specified in Table 10 below. The services highlighted in bold in Table 10 and Table 11can be called in uninitialized mode.

The unauthenticated Anybody role can do unauthenticated services.

Table 10: Unauthenticated Services

Service	Description
Power Cycle (Self-Test)	Powers the module off and on again. This triggers the following: 1. Power-On Self-Tests of the Module. 2. Unblock locked-out authorities that have exhausted their Try Limit. 3. Enable CO authority (Admins SP SID) if it is previously blocked by Block SID Authentication service.
Hot reset	Resets one of the ports of the Module by performing a PCIe Hot Reset.
Warm reset	Resets the Module by performing an NVMe Subsystem Reset or PCIe Warm reset.
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 FIPS mode (Initialized/Uninitialized), error messages, and other status information. The FIPS 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.
Block SID Authentication	Disables CO (Admin SP SID) authentication when ownership of the drive is not taken.
TCG Authentication	Authenticates an operator using TCG PIN through Start session or TCG Authentication method.
Enable Zeroization Service	Authenticates an operator using RSA 2048 signature verification using Zeroization Public Key (the Maker Public Key).
Get Random Number	TCG Random method used to generate and output a random number from the DRBG
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.
Read/Write User Data	Reads/Writes user data. This service is only successful if the module is in uninitialized mode.

Service	Description
Firmware Update	Loads a firmware image. All firmware loaded into the module is authenticated with RSA signature verification over the entire firmware image. Loaded firmware only executes if the firmware load test is successful. The version of the loaded firmware must be listed on the Module's FIPS certificate in order to remain in an Approved Mode.
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.
Sanitize	Wipes the data of a particular namespace by generating new MEK. This service is accessible only in Uninitialized mode.
Enable/Disable edrive mode	Enables or disables edrive mode. In edrive mode, the Probe Silo specific commands can be issued, and the TCG commands and responses can be transported within the IEEE1667 protocol.
Probe Silo specific commands (edrive mode only)	The Probe Silo specific commands can be issued only in the edrive mode to configure silos within the module and get IEEE1667 capabilities of the module.

Note:

- CO= Cryptographic Officer Role
- U = User Role
- M = Maker Role
- ASP = Admin SP (Security Provider)
- LSP = Locking SP (Security Provider)
- P = PSID Role

Table 11: Authenticated Services

Service	Description	CO			U	M	P
		ASP SID	ASP Admin 1	LSP Admin 1 - 4	LSP User 1 - 9	Maker	PSID
Take ownership	Changes default password of SID to a value other than MSID.	X	-	-	-	-	-
Activate OPAL	Enables Locking SP via TCG Activate method. Activate method can enable SUM.	X	-	-	-	-	-
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.	X	X	X	-	-	-

Service	Description	CO			U	M	P
		ASP SID	ASP Admin 1	LSP Admin 1 - 4	LSP User 1 - 9	Maker	PSID
Admin Set PIN	Updates Admin authority PIN.	X	X	X	-	-	-
User Set PIN	Updates User authority PIN. Locking SP Admins can set PINs for any Non-SUM Users.	-	-	X	X	-	-
Enable/Disable User Set PIN	Disables a non-SUM User's ability to change its own PIN.	-	-	X	-	-	-
Enable/Disable Admin SP authorities	Enables or disables an Admin SP authority.	X	-	-	-	-	-
Enable/Disable Locking SP authorities	Enables or disables a Locking SP Admins and non-SUM Users.	-	-	X	-	-	-
Enable/Disable SUM	Configures users and ranges in SUM through TCG Reactivate method.	-	-	X	-	-	-
Locking Range Configuration	For non-SUM ranges: Used to modify a range starting address, capacity, and attributes of non-SUM ranges.	-	-	X	-	-	-
	For SUM Policy 1: Used to modify a SUM range starting address, capacity and attributes by Admins if allowed.	-	-	X	-	-	-
	For SUM Policy 0: Used to modify a SUM range starting address, capacity and attributes by SUM Users if allowed.	-	-	-	X	-	-
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.	-	-	X	X	-	-
Set common name	Customizes the name of a TCG Authority. Admins and Users (if allowed by Admins) have access.	-	-	X	X	-	-
Data store table Set	Writes a stream of bytes to unstructured storage. Admins and Users (if allowed by Admins) have access.	-	-	X	X	-	-
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.	-	-	X	X	-	-
	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.	-	-	X	X	-	-

Service	Description	CO			U	M	P
		ASP SID	ASP Admin 1	LSP Admin 1 - 4	LSP User 1 - 9	Maker	PSID
	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.	-	-	-	X	-	-
Read/Write User Data	Reads/Writes user data. This service is only successful if the range is unlocked for read/write access via Lock/Unlock range service.	-	-	X	X	-	-
Zeroization	Destruction of plaintext keys and CSPs. This service decommissions the drive.	-	-	-	-	X	-
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.	-	-	-	-	-	X

- G = Generate: The Module generates or derives the CSP.
- I = Input: The CSP is input into the Module.
- X = Execute: The Module reads and uses the CSP.
- W = Write: The Module writes the CSP to storage.
- Z = Zeroize: The module zeroizes the CSP.
- - = Not accessed by the service.

Table 12: CSP Access within Services

Service	CSPs														
	CO Password	User Password	DRBG-EI	DRBG V	DRBG Key	DRBG seed_material	HRK	PSP_HMAC_KEY	MEK_KEK	TPER_SALT_KEK	KS_HMAC_KEY	TPER_KEK	SUM_KEK_i	MEK_j	$AUTH\_KEY_m$
Authenticated Services															
Take ownership	I, X, Z	-	G, X, Z	X, G	X, G	X, G	-	X	-	X	-	G, X	-	-	G, X, Z
Activate OPAL	I, X, Z	X	G, X, Z	X, G	X, G	X, G	-	X	-	X	-	-	G, X	-	G, X, Z
Deactivate OPAL	X	-	G, X, Z	X, G, Z	X, G, Z	X, G, Z	X	Z, G, X	Z, G, X	Z, G, X	-	X, Z	X, Z	X, Z, G	G, X, Z

Service	CSPs														
	CO Password	User Password	DRBG-EI	DRBG V	DRBG Key	DRBG seed_material	HRK	PSP_HMAC_KEY	MEK_KEK	TPER_SALT_KEK	KS_HMAC_KEY	TPER_KEK	SUM_KEK_i	MEK_j	$AUTH\_KEY_m$
Admin Set PIN	I, X, Z	-	G, X, Z	X, G	X, G	X, G	-	X	-	X	-	X	--	-	G, X, Z
User Set PIN	-	I, X, Z	G, X, Z	X, G	X, G	X, G	-	X	-	X	-	X	X	-	G, X, Z
Enable/Disable User Set PIN	-	-	-	-	-	-	-	X	-	-	-	-	-	-	-
Enable/Disable Admin SP authorities	X	-	G, X, Z	X, G	X, G	X, G	-	X	-	X	-	-	-	-	G, X, Z
Enable/Disable Locking SP authorities	X	X	G, X, Z	X, G	X, G	X, G	-	X	-	X	-	X	-	-	G, X, Z
Enable/Disable SUM	I, X, Z	X	G, X, Z	X, G	X, G	X, G	-	X	-	X	-	Z, G, X	Z, G, X	-	G, X, Z
Locking Range Configuration	-	-	G, X, Z	X, G	X, G	X, G	-	X	X	-	-	X	X	G, X, Z	-
Lock/Unlock range	-	-	-	-	-	-	-	X	-	-	-	X	X	X, Z	-
Set common name	-	-	-	-	-	-	-	X	-	-	-	-	-	-	-
Data store table Set	-	-	-	-	-	-	-	X	-	-	-	-	-	-	-
Crypto Erase of a range	-	X	G, X, Z	X, G	X, G	X, G	-	X	X	X	-	X	X	Z, G, X	G, X, Z
Read/Write User Data	-	-	-	-	-	-	-	-	-	-	-	-	-	X	-
Zeroization	-	-	-	Z	Z	Z	Z	Z,	Z	Z	Z	Z	Z	Z	-
PSID Revert	X	-	G, X, Z	X, G, Z	X, G, Z	X, G, Z	X	Z, G, X	Z, G, X	Z, G, X	-	Z	Z	Z, G	G, X, Z
Unauthenticated Services															
Power Cycle (Self-Test)	-	-	-	X, G, Z	X, G, Z	X, G, Z	X	X	X	X	X	-	-	X	-

Service	CSPs														
	CO Password	User Password	DRBG-EI	DRBG V	DRBG Key	DRBG seed_material	HRK	PSP_HMAC_KEY	MEK_KEK	TPER_SALT_KEK	KS_HMAC_KEY	TPER_KEK	SUM_KEK$_i$	MEK$_j$	AUTH_KEY$_m$
Hot reset	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Warm reset	-	-	-	-	-	-	-	X	-	-	-	-	-	-	-
Show Status	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Read FIPS Compliance	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Block SID Authentication	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
TCG Authentication	I, X, Z	I, X, Z	G, X, Z	X, G	X, G	X, G	-	X	-	X	-	G, X	X	-	G, X, Z
Enable Zeroization Service	-	-	G, X, Z	X, G	X, G	X, G	-	-	-	-	-	-	-	-	-
Get Random Number	-	-	G, X, Z	X, G	X, G	X, G	-	-	-	-	-	-	-	-	-
Firmware update	-	-	-	-	-	-	X	-	-	-	X	-	-	-	-
Telemetry logs	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Read/Write User Data	-	-	-	-	-	-	-	-	-	-	-	-	-	X	-
Format / Namespace Management	-	-	G, X, Z	X, G	X, G	X, G	-	X	X	-	-	X	X	Z, G, X	-
Sanitize	-	-	G, X, Z	X, G	X, G	X, G	-	X	X	-	-	-	-	Z, G, X	-
Enable/Disable edrive mode	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Probe Silo specific commands (edrive mode only)	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

- G = Generate: The Module generates or derives the PSP.
- I = Input: The PSP is input into the Module.
- X = Execute: The Module reads and uses the PSP.
- - = Not accessed by the service.

Table 13: PSP Access within Services

	PSPs				
	SALT	PSID PIN	MSID PIN	FW Public Key	Maker Public Key
Authenticated Services					
Take ownership	G, X	-	-	-	-
Activate OPAL	G, X	-	-	-	-
Deactivate OPAL	G, X	-	X	-	-
Admin Set PIN	G, X	-	-	-	-
User Set PIN	G, X	-	-	-	-
Enable/Disable User Set PIN	-	-	-	-	-
Enable/Disable Admin SP authorities	G, X	-	-	-	-
Enable/Disable Locking SP authorities	G, X	-	-	-	-
Enable/Disable SUM	G, X	-	-	-	-
Locking Range Configuration	-	-	-	-	-
Lock/Unlock range	-	-	-	-	-
Set common name	-	-	-	-	-
Data store table Set	-	-	-	-	-
Crypto Erase of a range	G, X	-	-	-	-
Read/Write User Data	-	-	-	-	-
Zeroization	-	-	-	-	-
PSID Revert	G, X	-	X	-	-
Unauthenticated Services					
Power Cycle (Self-Test)	-	-	-	X	-
Hot reset	-	-	-	-	-
Warm reset	-	-	-	-	-
Show Status	-	-	-	-	-

	PSPs				
	SALT	PSID PIN	MSID PIN	FW Public Key	Maker Public Key
Read FIPS Compliance	-	-	-	-	-
Block SID Authentication	-	-	-	-	-
TCG Authentication	G, X	I, X	-	-	-
Enable Zeroization Service	-	-	-	-	X
Get Random Number	-	-	-	-	-
Firmware update	-	-	-	X	-
Telemetry logs	-	-	-	-	-
Read/Write User Data	-	-	-	-	-
Format / Namespace Management	-	-	-	-	-
Sanitize	-	-	-	-	-
Enable/Disable edrive mode	-	-	-	-	-
Probe Silo specific commands (edrive mode only)	-	-	-	-	-

4 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 the Module.

On power-on or reset, the Module performs self-tests as described in Table 14 below. All KATs must be completed successfully prior to any other use of cryptography by the Module. If one of the KATs fails 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 14: Power-On Self-Tests

Test Target	Description	Failure Behavior
Firmware Integrity	RSA 2048 and SHA-256 verification performed over all firmware located in NAND storage on the Aquarius controller.	Enters INTERNAL_STATE_ERROR state. The SSD will not enumerate, PCI_DEVICE_ID value will be 0x0100
RSA (Cert. #A914)	RSA PSS verify with 2048bit key is used for the firmware integrity test.	Enters INTERNAL_STATE_ERROR state. The SSD will not enumerate, PCI_DEVICE_ID value will be 0x0100 (This error would be found during the firmware integrity self-test.)
SHA	RSA is used to verify the signature of the firmware and a KAT of the underlying SHA-256 hashing function is not required. SHA-256 is tested in the Firmware Integrity test.	Enters INTERNAL_STATE_ERROR state. The SSD will not enumerate, PCI_DEVICE_ID value will be 0x0100 (This error would be found during the firmware integrity self-test.)
RSA (Cert. #A912)	Only RSA PSS verify with 2048-bit key is implemented in the module. This SigVer must be tested separately from the one for Cert. #A914).	Enters INTERNAL_STATE_ERROR state. The SSD will not enumerate, PCI_DEVICE_ID value will be 0x0100.
AES-XTS	Performs encrypt and decrypt KATs using a 256-bit key.	Enters SELF_TEST_ERROR state.
AES-ECB	Encryption and Decryption KATs Key size: 256 bits	Enters SELF_TEST_ERROR state.
AES-KW	KATs: Both forward and inverse ciphers are tested via encryption and decryption. See IG 9.4 Modes: KW Key size: 256 bits	Enters SELF_TEST_ERROR state.

Test Target	Description	Failure Behavior
	Note: This test covers AES-ECB as per IG 9.4, #4 (c).	
HMAC	Performs HMAC generate and verify KATs using a 256-bit key.	Enters SELF_TEST_ERROR state.
PBKDF	Performs KAT using a known password and 256-bit key.	Enters SELF_TEST_ERROR state.
DRBG	Performs a fixed input KAT inclusive of the SP 800-90A instantiate, generate, and reseed health tests. Mode: AES CTR DRBG	Enters SELF_TEST_ERROR state.
ENT (P)	Performs ENT (P) startup test. Generates noise that will force RCT and APT on 1024 bits. The tests are run on each block of consecutive 1024 raw samples.	Enters SELF_TEST_ERROR state.

Table 15: Conditional Self-Tests

Test Target	Description	Failure Behavior
ENT (P)	The Module performs a Continuous Random Number Generator Test (RCT and APT) for each call to the ENT (P).	Enters SELF_TEST_ERROR state.
AES XTS Key generation	An IG A.9 key comparison test is performed on Key1 and Key2 for each generation.	Enters SELF_TEST_ERROR state.
Firmware load Test	The Module performs a SHA-256 and RSA 2048 (Cert. #A912) signature verification on all firmware loaded into the Module.	The Module returns invalid image for download commit command and the image is discarded. The module transitions back to the Unauthenticated Service Processor state without entering an error state.

5 Physical Security Policy

The Module meets commercial-grade specifications for power, temperature, reliability, and shock/vibrations. The Module uses standard passivation techniques.

6 Operational Environment

The Module is designated as a non-modifiable operational environment under the FIPS 140-2 definitions. The Module includes a firmware load service to support necessary updates. The Module will not load or execute firmware which is not signed with SK hynix 2048-bit RSA Private Key. The mechanism available to perform a firmware load is through NVMe Firmware Download and Commit command. New firmware versions within the scope of this validation must be validated through the CMVP under FIPS 140-2. Any other firmware loaded into this module is out of the scope of this validation and require a separate FIPS 140-2 validation.

7 Mitigation of Other Attacks Policy

The Module does not support the mitigation of other attacks outside the scope of FIPS 140-2.

8 Security Rules and Guidance

The Module design corresponds to the Module Security rules. This section documents the security rules enforced by the Module and the Cryptographic Officer instructions that are necessary to implement in order to maintain compliance with FIPS 140-2 security requirements.

8.1 Invariant Rules

The Module implementation also enforces the following security rules:

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 and in error states.
3. Data output is logically disconnected while the Module is performing key generation and zeroization.
4. All the CSPs are zeroized by the zeroization service. Only the Maker role can call the zeroization service.
5. The module does not support manual key entry.
6. The module does not output plaintext CSPs or intermediate key values.
7. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
8. The Module does not support a bypass capability.
9. The Module shall provide four (4) distinct operator roles: Cryptographic Officer, User, Maker, and PSID
10. The Module shall clear previous authentication on power cycle.
11. When the Module has not been placed in a valid role, the operator shall not have access to any cryptographic services.
12. The operator shall be capable of commanding the Module to perform the power up self-tests by power cycling or resetting the Module.
13. Power on self-tests do not require any operator action.
14. The Module does not support the update of the serial number and vendor ID.
15. The Module does not support concurrent operators.

8.2 Cryptographic Officer Initialization

The Module is shipped from the factory in an approved mode of operation (uninitialized mode). 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.

8.2.1 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 -> FIPS 140-2
 COMPLIANCE DESCRIPTOR OVERALL SECURITY LEVEL -> Level-1
 COMPLIANCE DESCRIPTOR HARDWARE VERSION -> HFS960GDE0X098N
 COMPLIANCE DESCRIPTOR VERSION ->41081A10
 COMPLIANCE DESCRIPTOR MODULE NAME -> SK hynix PE8110 M.2 22110D NVMe TCG Opal
SSC SED
--------------------------------------------------------------------
```

8.2.2 Initialize the Module

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

1. Take Ownership - Set Admin SP SID password to a value other than MSID.
2. Activate Opal with Single User Mode.
3. Set WriteLockEnabled and ReadLockEnabled column of all valid Locking ranges.
4. Set PINs for all authorities (Admins and Users) that are enabled.
5. PIN length at least 0 bytes or more but 32 byte length is recommended.
6. Power cycle the Module.
7. 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.

8.3 Un-Initialize the Module

The TCG Revert or Revert SP Methods may be invoked by an authenticated role to affect a transition into the uninitialized mode of operation. The PSID Revert may be done by the PSID role to affect a transition into the uninitialized mode of operation. This is analogous to restoring the module to the factory default state.

8.4 Firmware Update

A firmware update loads a firmware image. All firmware loaded into the module is authenticated with RSA signature verification over the entire firmware image. Loaded firmware only executes if the firmware load test is successful. The version of the loaded firmware must be listed on the Module's FIPS certificate to remain in an Approved Mode.

The firmware update process could be performed with and without the reset, for the first one the host:

1. Issues NVM Firmware Image Download command [NVMe, 5.12].
2. Issues NVM Firmware Commit command [NVMe, 5.11].
3. Performs a Reset.

Reset causes the loaded firmware to be activated. For the firmware update without the reset, the host:

1. Issues NVM Firmware Image Download command.
2. Issues NVM Firmware Commit command with Commit Action set to 3.

Following the Commit Action, the NVMe controller completes the firmware commit by activating the loaded firmware.

9 References and Definitions

The following standards are referred to in this Security Policy

Table 16: References

Acronym	Full Specification Name
[FIPS 140-2]	NIST, *Security Requirements for Cryptographic Modules*, May 25, 2001
[Annex C]	NIST, *Annex C: Approved Random Number Generators for FIPS PUB 140-2*, June 10, 2019
[FIPS 180-4]	NIST, *Secure Hash Standard*, FIPS Publication 180-4, August 2015
[FIPS 186-4]	NIST, *Digital Signature Standard (DSS)*, FIPS Publication 186-4, July 2013
[FIPS 197]	NIST, *Advanced Encryption Standard (AES)*, FIPS Publication 197, November 26, 2001
[FIPS 198-1]	NIST, *The Keyed-Hash Message Authentication Code (HMAC)*, FIPS Publication 198-1, July 2008
[IG]	NIST, *Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program,* last updated May 04, 2021
[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
[SP800-38E]	NIST Special Publication 800-38E, Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices, January 2010
[SP800-38F]	NIST Special Publication 800-38F, *Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping,* December 2012
[SP800-90A Rev1]	*National Institute of Standards and Technology, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, Special Publication 800-90A Revision 1, June 2015.*
[SP800-90B]	*National Institute of Standards and Technology, Recommendation for the Entropy Sources Used for Random Bit Generation, Special Publication 800-90B, January 2018.*
[SP800-108]	NIST Special Publication 800-108, *Recommendation for Key Derivation Using Pseudorandom Functions (Revised),* October 2009
[SP800-132]	NIST Special Publication 800-132, *Recommendation for Password-Based Key Derivation,* December 2010
[SP800-133 Rev2]	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*
[TCG ADS]	*TCG Storage Opal SSC Feature Set: Additional Datastore Tables Specification, Version 1.00 Revision 1.00, 24 February 2012*

Acronym	Full Specification Name
[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 17: Acronyms and Definitions

Acronym	Definition
AES	Advanced Encryption Standard
APT	Adaptive Proportion Test
CO	Cryptographic Officer
CSP	Critical Security Parameter, see [FIPS 140-2]
DRBG	Deterministic Random Bit Generator
ECB	Electronic Code Book mode of AES Encryption/Decryption
ENT (P)	Entropy – Physical validated entropy source
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
XTS	**X**EX **T**weakable Block Cipher with Cipher text **S**tealing