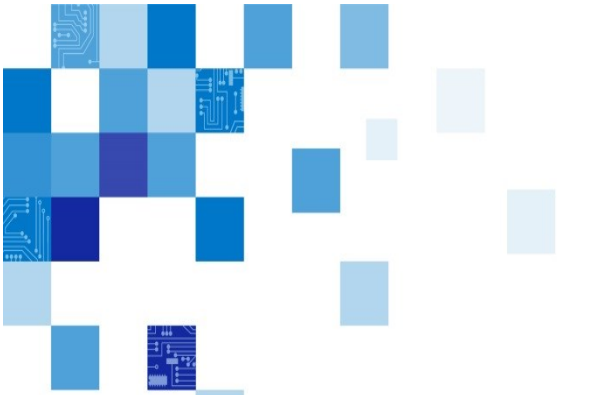

Samsung NVMe TCG Opal SSC SEDs PM1743/PM1745 Series

FIPS 140-3 Non-Proprietary Security Policy

Document Version: 1.0

H/W Version: MZWLO1T9HCJR-00AD9 [1], MZWLO3T8HCLS-00AD9 [1], MZWLO7T6HBLA-00AD9 [1], MZWLO15THBLA-00AD9 [1], MZWLO1T6HCJR-00AD9 [1], MZWLO3T2HCLS-00AD9 [1], MZWLO6T4HBLA-00AD9 [1], MZWLO12THBLA-00AD9 [1], MZWLO1T9HCJR-00AH9 [2], MZWLO3T8HCLS-00AH9 [2], MZWLO7T6HBLA-00AH9 [2], MZWLO15THBLA-00AH9 [2], MZWLO1T9HCJR-00AH8 [3], MZWLO3T8HCLS-00AH8 [3], MZWLO7T6HBLA-00AH8 [3], MZWLO15THBLA-00AH8 [3]

F/W Version: OPP90D5Q [1], 3P00 [2], 3R00 [3]

Revision History

Version	Change
1.0	Initial Version

Table of Contents

1. General

1.1. Scope

This document is a non-proprietary Security Policy for **Samsung NVMe TCG Opal SSC SEDs PM1743/PM1745 Series**, hereinafter referred to as a "cryptographic module" or "module". The SSD (Solid State Drive) satisfies all applicable FIPS 140-3 security level 2 of 'Hardware Module' requirements, supporting TCG Opal SSC based SED (Self-Encrypting Drive) features. It is designed to protect unauthorized access to the user data stored in its NAND Flash memories. The built-in AES hardware engines in the cryptographic module's controller provide on-the-fly encryption and decryption of the user data without performance loss. The SED's nature also provides instantaneous sanitization of the user data via cryptographic erase.

ISO/IEC 24759 Section 6. [Number Below]	FIPS 140-3 Section Title	Security Level
1	General	2
2	Cryptographic module specification	2
3	Cryptographic module interfaces	2
4	Roles, services, and authentication	2
5	Software/Firmware security	2
6	Operational environment	N/A
7	Physical security	2
8	Non-invasive security	N/A
9	Sensitive security parameter management	2
10	Self-tests	2
11	Life-cycle assurance	2
12	Mitigation of other attacks	N/A

Table 1. Security Levels

1.2. Acronyms

Acronym	Description
CPU	Central Processing Unit (ARM-based)
CTRL	Controller
DRAM I/F	Dynamic Random Access Memory Interface
LBA	Logical Block Address
MEK	Media Encryption Key
NAND I/F	NAND Flash Interface
PMIC	Power Management Integrated Circuit
ROM	Read Only Memory
NVMe	Non-Volatile Memory Host Controller Interface Specification
SED	Self-Encrypting Drive
SSC	Security Subsystem Class
SSP	Sensitive Security Parameter
TCG	Trusted Computing Group

Table 2. Acronyms

2. Cryptographic Module Specification

2.1. Cryptographic Boundary

This firmware version, within the scope of this validation, must undergo validation through the FIPS 140-3 CMVP. Any other firmware loaded into this module is beyond the scope of this validation and requires a separate FIPS 140-3 validation.

The following photographs depict the top and bottom views of the cryptographic module. This multiple-chip standalone cryptographic module comprises both hardware and firmware components, all enclosed within two aluminum alloy cases. These cases serve as the cryptographic boundary of the module.

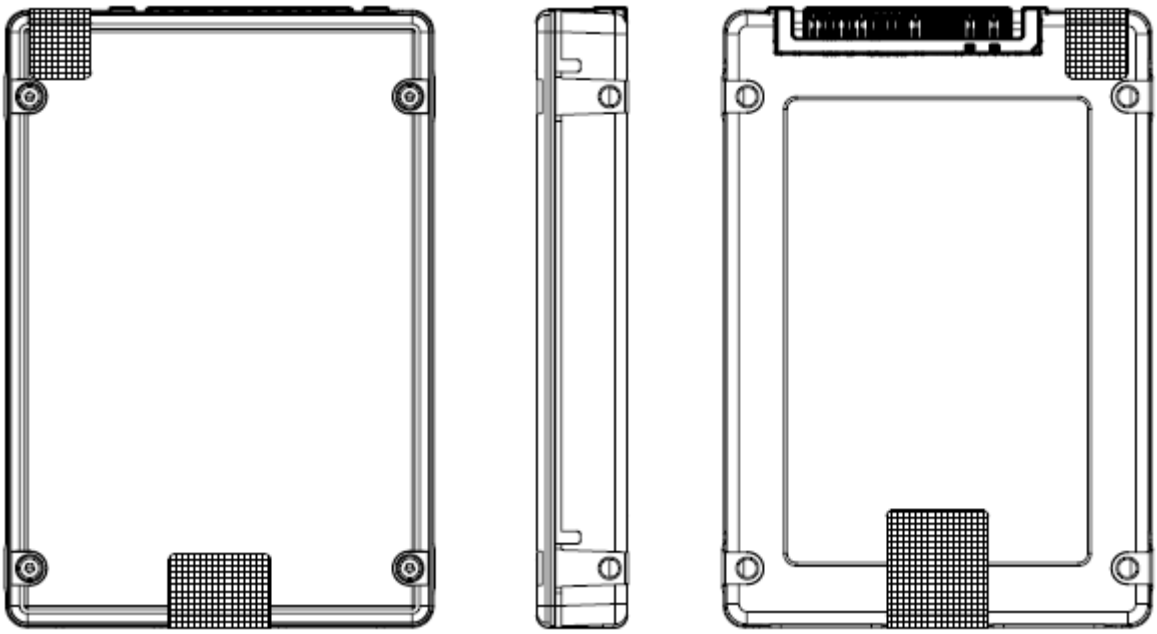

Figure 1. Samsung NVMe TCG Opal SSC SEDs PM1743/PM1745 Series

The PM1743/PM1745 series utilizes a single-chip controller with an NVMe interface on the system side and internally integrates Samsung NAND flash. The following figure illustrates the operational environment of the module.

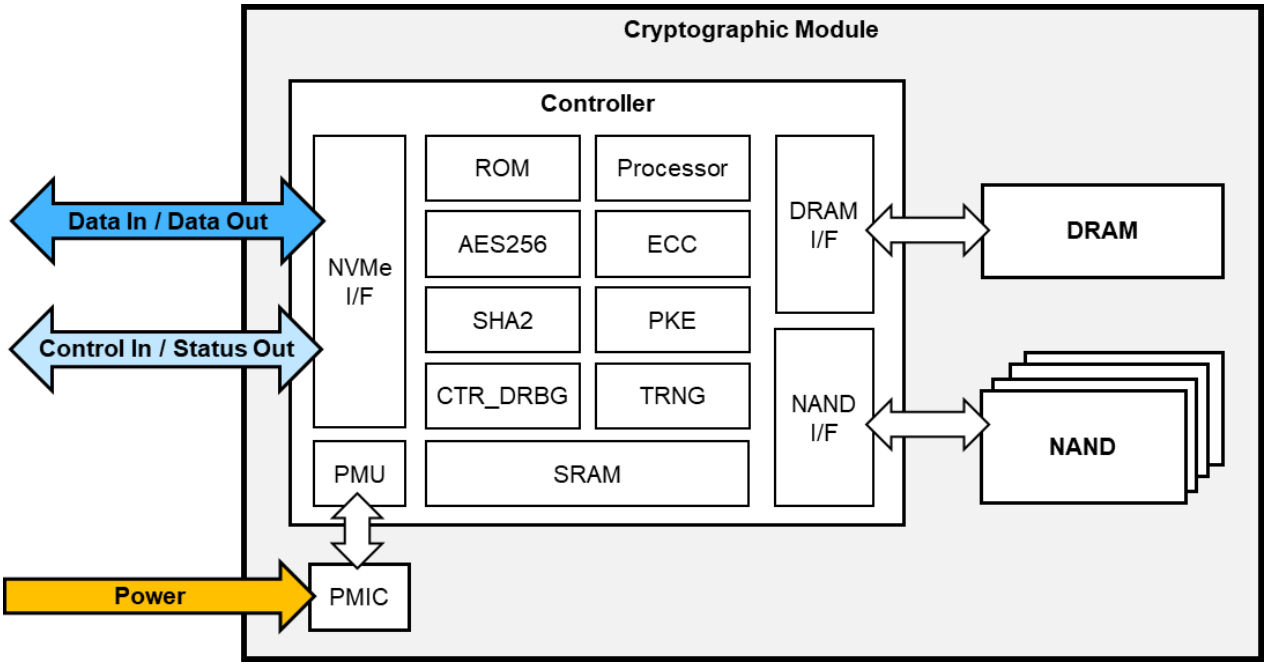

Figure 2. Block Diagram for Samsung NVMe TCG Opal SSC SEDs PM1743/PM1745 Series

2.2. Version Information

Model	Hardware [Part Number and Version]	Firmware Version	Distinguishing Features
PM1743	MZWLO1T9HCJR-00AH9	3P00	1.92TB
	MZWLO3T8HCLS-00AH9		3.84TB
	MZWLO7T6HBLA-00AH9		7.68TB
	MZWLO15THBLA-00AH9		15.36TB
	MZWLO1T9HCJR-00AH8	3R00	1.92TB
	MZWLO3T8HCLS-00AH8		3.84TB
	MZWLO7T6HBLA-00AH8		7.68TB
	MZWLO15THBLA-00AH8		15.36TB
	MZWLO1T9HCJR-00AD9	OPP90D5Q	1.92TB
	MZWLO3T8HCLS-00AD9		3.84TB
	MZWLO7T6HBLA-00AD9		7.68TB
	MZWLO15THBLA-00AD9		15.36TB
PM1745	MZWLO1T6HCJR-00AD9		1.6TB
	MZWLO3T2HCLS-00AD9		3.2TB
	MZWLO6T4HBLA-00AD9		6.4TB
	MZWLO12THBLA-00AD9		12.8TB

Table 3. Cryptographic Module Tested Configuration

2.3. Cryptographic Functionality

2.3.1. Approved Algorithm[1]

The cryptographic module supports the following Approved algorithms for secure data storage:

CAVP Cert	Algorithm and Standard	Mode/ Method	Description/ Key Size(s)/ Key Strength(s)	Use/Function
A4661	AES-ECB / FIPS 197, SP 800-38A	ECB	256-bit keys with 256-bit key strength	Prerequisite for AES-XTS (A4661)
A4661	AES-XTS / FIPS 197, SP 800-38E	XTS[2]	256-bit keys with 256-bit key strength	Data Encryption / Decryption
A4662	AES-ECB / FIPS 197, SP 800-38A	ECB	256-bit keys with 256-bit key strength	Prerequisite for Counter DRBG (A4662)
A4662	Counter DRBG / SP 800-90Arev1	CTR_ DRBG[3] (AES-256)	AES 256 bits with Derivation Function Enabled	All Cryptographic Key Generation for version 'OPP90D5Q' firmware
A4846	AES-ECB / FIPS 197, SP 800-38A	ECB	256-bit keys with 256-bit key strength	Prerequisite for Counter DRBG (A4846)
A4846	Counter DRBG / SP 800-90Arev1	CTR_ DRBG[4] (AES-256)	AES 256 bits with Derivation Function Enabled	All Cryptographic Key Generation for version '3P00' and '3R00' firmware
A4663	AES-ECB / FIPS 197, SP 800-38A	ECB	256-bit keys with 256-bit key strength	Prerequisite for AES-GCM (A4663)
A4663	AES-GCM / FIPS 197, SP 800-38D	GCM[5]	256-bit keys with 256-bit key strength IV: 96 bits	Key Encryption / Decryption
A4663	ECDSA SigVer / FIPS 186-4	ECDSA SigVer	Curve P-384 with SHA2-384	Digital Signature Verification
A4663	HMAC-SHA2-256 / FIPS 198-1	HMAC[6]	256-bit keys HMAC-SHA2-256 with λ=256	Message Authentication

[1] Not all algorithms/modes that appear on the module's CAVP certificates are utilized by the module.
[2] AES-ECB is the pre-requisite for AES-XTS (#4661); AES-ECB alone is NOT supported by the cryptographic module in Approved Mode.
[3] AES-ECB is the pre-requisite for Counter DRBG (#4662); AES-ECB alone is NOT supported by the cryptographic module in Approved Mode.
[4] AES-ECB is the pre-requisite for Counter DRBG (#4662); AES-ECB alone is NOT supported by the cryptographic module in Approved Mode.
[5] 2nd technique of IG C.H for generating an IV is implemented in this module. In other words, Key and IV are generated internally using by approved CTR-DRBG (A4662 and A4846). And AES-ECB is the pre-requisite for AES-GCM (#4663); AES-ECB alone is NOT supported by the cryptographic module in Approved Mode.
[6] HMAC is the pre-requisite for PBKDF2 (#4663); HMAC alone is NOT supported by the cryptographic module in Approved Mode.

A4663	SHA2-256 / FIPS 180-4	SHA2-256[7]	SHA2-256	Message Digest
A4663	SHA2-384 / FIPS 180-4	SHA2-384	SHA2-384	Message Digest
A4663	PBKDF2 / SP 800-132	HMAC SHA2-256 Option 2a using AES-GCM encryption	256 bits	Key Derivation[8]
Vendor Affirmed	CKG / SP 800-133rev2	Section 4 Section 6.1 Section 6.3	N/A	Symmetric Cryptographic Key Generation
-	ENT (P) / SP800-90B	N/A	N/A	ENT (P) provides a minimum of 256 bits of entropy for DRBG seed materials in key generation.

Table 4. Approved Algorithms

2.3.2. Non-Approved Algorithm

The module does not implement any Non-Approved Algorithms Not Allowed in the Approved Mode of Operation. The following algorithms are not intended to be used as a security function and are not implemented to meet any FIPS 140-3 requirements. Additionally, these algorithms are not provided through a non-approved service to an operator

Algorithm	Caveat	Use / Function
AES-XTS / FIPS 197, SP 800-38E	No Security Claimed; AES-XTS is used remove obfuscation from the firmware during ROM initialized.	Removal of firmware obfuscation
	No Security Claimed; AES-XTS is used for obfuscation and removal of obfuscation the CSP. (IG 2.4.A Scenario #1)	Key obfuscation and Removal of obfuscation
AES-GCM / FIPS 197, SP800-38D	No Security Claimed; AES-GCM is only used for obfuscation and removal of obfuscation the CSP. (IG 2.4.A Scenario #1)	Key obfuscation and Removal of obfuscation

Table 5. Non-Approved Algorithms Allowed in the Approved Mode of Operation with No Security Claimed

2.4. Approved Mode of Operation

The module defaults to an Approved mode of operation, and as long as the guidance outlined in section 11 is followed, the module will remain in the Approved mode. The cryptographic module indicates the approved mode through the validated version status, as shown by the 'Show Status Service' in Table 8 via the NVM Express Identify Controller command.

[7] SHA2-265 is the pre-requisite for PBKDF2 (#4663); SHA2-256 alone is NOT supported by the cryptographic module in Approved Mode.
[8] The Iteration Count parameter is 281. It was set accordingly in order to meet the minimum response time required from the application while maintaining acceptable performance.

3. Cryptographic Module Interfaces

The module does not support a Control Output Interface.

Physical port	Logical Interface	Data that passes over port/interface
NVMe Connector	Data Input	plaintext data; signed data; authentication data
	Data Output	plaintext data
	Control Input	commands input logically via an API; signals input logically or physically via one or more physical ports
	Status Output	status information output logically via an API; signal outputs logically or physically via one or more physical ports;

Table 6. Ports and Interfaces

4. Roles, Services, and Authentication

4.1. Role

The following table defines the roles, associated services, and inputs/outputs supported by the cryptographic module:

Role	Service	Input	Output
Cryptographic Officer (CO) and User	Lock/Unlock an LBA Range	LBA Range	Status
	Erase an LBA Range's Data	LBA Range	Status
	IO Command	LBA	Status
CO	Change the Password	CO Password	Status
User	Set User Password	User Password	Status
None	Update the firmware	Firmware image binary	Status
	Show Status	None	Status
	Authentication	Authority, Authenticated data	Status
	Get Random Number	None	Status
	Revert	None	Status
	FormatNVM	Namespace ID, LBA Format	Status
	Sanitize / DeleteNS	Namespace ID	Status
	Perform Self-tests	None	Status

Table 7. Roles, Service Commands, Input and Output

4.2. Authentication

The module supports role-based authentication that necessitates verification for assuming the authorization of each role. The authentication mechanism allows a minimum 8-byte length or longer (up to 32-byte) password, with each byte ranging from 0x00 to 0xFF, applicable to every Cryptographic Officer and User role supported by the module. This implies that a single random attempt can succeed with a probability of $1/2^{64}$ or lower. Each password authentication attempt takes at least 750 ms. The maximum number of attempts possible in a one-minute period is 80 (60000 ms/750 ms). The Password is considered a Memorized Secret Authenticator Type as per SP 800-140E/SP 800-63B.

The module claims compliance with IG 4.1.A by implementing a Lock-based authentication model for the "IO command" service. This protects data-at-rest. The "Lock/Unlock an LBA Range" service enables or disables the "IO command" service. Power cycling the module completely disables the "IO command" service if it was enabled. Afterward, the service reverts to its original state, requiring authentication and being enabled/disabled by the "Lock/Unlock an LBA Range" service.

Role	Authentication Method	Authentication Strength
CO	Password (Min: 8 bytes, Max: 32 bytes)	Probability of $1/2^{64}$ in a single random attempt Probability of $80/2^{64}$ in multiple random attempts in a minute
User		

Table 8. Roles and Authentication

4.3. Service

The cryptographic module only supports the following approved services and does not support any non-approved services. The abbreviations of the type of access to keys and SSPs have the following interpretation:

- E = Execute: The module performs approved security functions with the SSPs.
- G = Generate: The module generates or derives the SSP.
- W = Write: The SSP is updated, imported, or written to the volatile storage specified in Table 12.
- Z = Zeroise: The module zeroises the SSP.

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access right to Keys and/or SSPs				Indicator[9]
					E	W	G	Z	
Change the Password	Change CO password	A4663 PBKDF2 HMAC-SHA2-256 SHA2-256	CO Password	CO	O	O		O	UID: AdminSP_SID_C_PIN / AdminSP_Admin1_C_PIN TCG Method: Set Result: TCG status code (Success: 00h)
			CPK			O	O	O	
			KPK			O	O	O	
Set User Password	Set User Password	A4663 PBKDF2 HMAC-SHA2-256 SHA2-256	User Password	User	O	O		O	UID: LockingSP_Admin1~4_C_PIN / LockingSP_User1~9_C_PIN TCG Method: Set Result: TCG status code (Success: 00h)
			CPK			O	O	O	
			KPK			O	O	O	
Lock/Unlock an LBA Range[10]	Block or allow read (decrypt) / write (encrypt) of user data.	A4663 AES-GCM	MEK	CO, User		O		O	UID: Locking_GlobalRange / Locking_RangeNNNN TCG Method: Set Result: TCG status code (Success: 00h)
			KEK		O	O		O	
			KPK		O			O	
IO Command[11]	Encrypt / Decrypt User data	A4661 AES-XTS	MEK		O				NVM Command: Write / Read Result: NVM Status Code (Success: 00h)
Erase an LBA Range's Data	Erase user data by changing the data encryption key.	A4662/A4846 CTR_ DRBG (AES-256) ENT (P)	DRBG V		O	O	O	O	UID: K_AES_256_GlobalRange_Key / K_AES_256_RangeNNNN_Key TCG Method: GenKey Result: TCG status code (Success: 00h)
			DRBG Key		O	O	O	O	
			DRBG Seed		O	O	O	O	
		CKG	MEK			O	O	O	

Table 9. Approved Services - Authenticated

- The following table displays unauthenticated services. Initially, it is possible to use the services in the table without authentication. The operator can configure settings that comply with NVM and TCG specifications.

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access right to Keys and/or SSPs				Indicator[12]
					E	W	G	Z	
Show Status	Show approved version status of the module / Error state	N/A	N/A	N/A	N/A				NVM Command: Identify Controller command Result: NVM Status Code (Success: 00h)
Authentication	Authenticate the module	A4663 PBKDF2 HMAC-SHA2-256 SHA2-256	CO Password	N/A	O	O		O	UID: AdminSP_SID / AdminSP_Admin1 / LockingSP_Admin1~4 / LockingSP_User1~9 TCG Method: Authenticate Result: TCG status code (Success: 00h)
			User Password		O	O		O	
			CPK		O	O		O	
			KPK				O		

[9] *The result of NVMe or TCG command is used as an indicator.*

[10] *This service can lock/unlock an "IO Command" Service that doesn't require any authentication specified in the Role column.*

[11] *The "IO Command" service is unlocked in advance by using the "Lock/Unlock an LBA Range" service, which complies with IG 4.1.A Additional Comment 8. Power cycling the module re-locks this service.*

[12] *The result of NVM or TCG command is used as an indicator. NVM status code is stated in NVM Express® Base Specification and TCG status code is stated in TCG Storage Architecture Core Specification.*

Get Random Number	Provide a random number generated by the CM.	A4662/A4846 CTR_ DRBG (AES-256) ENT (P)	DRBG V		O	O	O	O	UID: ThisSP TCG Method: Random Result: TCG status code (Success: 00h)
			DRBG Key		O	O	O	O	
			DRBG Seed		O	O	O	O	
			Entropy Input		O	O	O	O	
Revert	Erase user data in all Range by changing the data	A4662/A4846 CTR_ DRBG (AES-256) ENT (P)	DRBG V		O	O	O	O	UID: SPObj(AdminSP) TCG Method: Revert Result: TCG status code (Success: 00h)
			DRBG Key		O	O	O	O	
			DRBG Seed		O	O	O	O	
			Entropy Input		O	O	O	O	
		A4663 PBKDF2 HMAC-SHA2-256 SHA2-256	CPK			O	O	O	
		CKG	MEK			O	O	O	
			KEK			O	O	O	
FormatNVM	Erase user data by changing the data encryption key.	A4662/A4846 CTR_ DRBG (AES-256) ENT (P)	DRBG V		O	O	O	O	Admin Command: Format NVM Result: NVM Status Code (Success: 00h)
			DRBG Key		O	O	O	O	
			DRBG Seed		O	O	O	O	
			Entropy Input		O	O	O	O	
		A4663 PBKDF2 HMAC2-SHA-256 SHA2-256	CPK			O	O	O	
		CKG	MEK			O	O	O	
			KEK			O	O		
Sanitize / DeleteNS	Erase user data by changing the data encryption key.	A4662/A4846 CTR_ DRBG (AES-256) ENT (P)	DRBG V		O	O	O	O	Admin Command: Sanitize / Namespace Management Result: NVM Status Code (Success: 00h)
			DRBG Key		O	O	O	O	
			DRBG Seed		O	O	O	O	
			Entropy Input		O	O	O	O	
		A4663 PBKDF2 HMAC-SHA2-256 SHA2-256	CPK			O	O	O	
		CKG	MEK			O	O	O	
			KEK			O	O	O	
Update the firmware[13]	Update the firmware	A4663 ECDSA, A4663 SHA2-384	Firmware Verification Key		O				Admin Command: Firmware Commit Result: NVM Status Code (Success: 00h)
Perform Self-tests	Power cycling the module to perform self-tests	All cryptographic algorithms listed in Table 14 and Table 15 “Self-tests”.	N/A		N/A				The module enters operational state upon successful completion; otherwise, it indicates failure via the Show Status Service.

Table 10. Approved Services - Unauthenticated

[13] *This service is exempted from being authenticated by exception clause (c) of IG 4.1.A.*

5. Software/Firmware Security

- The cryptographic module employs ECDSA P-384 with SHA2-384 for firmware integrity testing, which is performed during power-on reset.

6. Operational Environment

- The cryptographic module operates in a limited operational environment, consisting of the module's firmware because this module does not have any operating system but designed in a manner to allow controlled validated firmware modification by an authenticated limited operator. This limited operational setting does not require any specific security rules, settings/configurations, or restrictions to be set.
- The cryptographic module does not provide any general-purpose operating system to the operator.
- Unauthorized modification of the firmware is prevented by the pre-operational firmware integrity test and conditional firmware load test.

7. Physical Security

The following physical security mechanisms are implemented in a cryptographic module:

- The module consists of production-grade components enclosed in an aluminum alloy enclosure, which is opaque within the visible spectrum. The top panel of the enclosure can be removed by unscrewing screws. However, the module is sealed with tamper-evident labels in accordance with FIPS 140-3 Level 2 Physical Security requirements so that tampering is easily detected when the top and bottom cases are detached.
- Two tamper-evident labels are initially applied over the top case of the module during factory production. Once applied, these labels cannot be removed and reapplied without evidence of tampering.
- The tamper-evident label is applied by Samsung at Manufacturing.

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

Physical Security Mechanisms	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Production grade cases	As often as feasible	Inspect the entire perimeter for cracks, gouges, lack of screw(s) and other signs of tampering. Remove from service if tampering found.
Tamper-evident Sealing Label		Inspect the sealing label for scratches, gouges, cuts and other signs of tampering. Remove from service if tampering found.

Table 11. Physical Security Inspection Guidelines

Figure 3. Tamper Evident Label Placement

Figure 4. Example of Signs of Tamper

8. Non-Invasive Security

- Non-invasive security is not applicable to this cryptographic module

9. Sensitive Security Parameter Management

- Temporary SSPs stored in RAM are zeroised during power on reset.
- The zeroisation is performed by overwriting the target SSP with a random value generated through the DRBG.
- The module does not export SSPs.
- All SSPs in volatile memory, including HW SFR, are automatically zeroised instantly either after key generation/use or upon performing power-on-reset, depending on the characteristics of volatile memory.
- This module does not support SSP establishment.

Key/SSP Name/ Type	Strength	Security Function and Cert. Number	Generation	Import /Export	Establish -ment	Storage	Zeroisation[14]	Use & related keys
DRBG V / CSP	128-bit	A4662/A4846 CTR_DRBG (AES-256)	SP 800-90A CTR_DRBG (AES-256)	N/A	N/A	N/A (HW internal)	Implicitly zeroised by Power on Reset	Generates the MEK and KEK
DRBG Key / CSP	256-bit	A4662/A4846 CTR_DRBG (AES-256)	SP 800-90A CTR_DRBG (AES-256)	N/A	N/A		Implicitly zeroised by Power on Reset	Generates the MEK and KEK
DRBG Seed / CSP	Entropy input: 512 bits Nonce 256 bits	A4662/A4846 CTR_DRBG (AES-256)	ENT (P)	N/A	N/A		Implicitly zeroised by Power on Reset	Generates the MEK and KEK
Entropy Input / CSP	512-bit / 256-bit	A4662/A4846 CTR_DRBG (AES-256)	ENT (P)	N/A	N/A		Implicitly zeroised by Power on Reset	Generates the MEK and KEK
CO Password / CSP	Min. 64-bit	A4663 PBKDF2	N/A	Manual Distribution / Electronic Entry in plaintext	N/A	Plaintext in RAM	Implicitly zeroised by Power on Reset	Derives CPK/KPK
User Password / CSP	Min. 64-bit	A4663 PBKDF2	N/A	Manual Distribution / Electronic Entry in plaintext	N/A	Plaintext in RAM	Implicitly zeroised by Power on Reset	Derives CPK/KPK
CPK / CSP	256-bit	N/A	Derived via PBKDF2	N/A	N/A	Plaintext in RAM and Flash	Explicitly zeroised via these services: Performing via Set User Password, Change the password and Revert; FormatNVM; Sanitize / DeleteNS service, and zeroisation is shown through	Derived from User and CO Password

[14] *"Zeriosation" performs in non-volatile memory.*

							the indicator of that service in Table 9, 10	
KPK / CSP	256-bit	A4663 AES-GCM	Derived via PBKDF2	N/A	N/A	Obfuscated (AES-XTS [no security claimed]) in Plaintext in RAM	Explicitly zeroised via these services: Performing via Authentication service, and zeroisation is shown through the indicator of those service in Table 9	Derived from User and CO Password Wraps KEK
KEK / CSP	256-bit	A4663 AES-GCM	CKG / SP 800-133rev2; SP 800-90A CTR_DRBG (AES-256)	N/A	N/A	Plaintext in RAM, Cipher text (AES-GCM) and obfuscated (AES-XTS [no security claimed]) in Flash	Explicitly zeroised via these services: Performing via Revert; FormatNVM; Sanitize / DeleteNS; Lock/Unlock an LBA Range service, and zeroisation is shown through the indicator of that service in Table 9, 10	Wraps MEK
MEK / CSP	256-bit	A4661 AES-XTS	CKG / SP 800-133rev2; SP 800-90A CTR_DRBG (AES-256)	N/A	N/A	Plaintext in RAM, Cipher text (AES-GCM) in Flash	Explicitly zeroised via these services: Performing via Revert; FormatNVM; Sanitize / DeleteNS; Lock/Unlock an LBA Range; Erase an LBA Range's Data service, and zeroisation is shown through the indicator of that service in Table 9, 10	IO Command
Firmware Verification Key / Non-SSP	256-bit	A4663 ECDSA	N/A	Entered during manufacturing	N/A	HW SFR[15]	Implicitly zeroised by Right after Firmware Load Test completed.	Firmware Load Test *Note: This is not considered an SSP as

[15] *HW SFR (Special Function Register) is a register within a hardware cryptographic algorithm IP, which has characteristic of volatile memory.*

								per ISO/IEC 19790:2012 section 7.5 but is included in the list for completeness

Table 12. SSPs

The cryptographic module contains an entropy source, compliant with SP 800-90B.

Entropy sources	Minimum number of bits of entropy	Details
ENT (P)[16]	0.5 entropy per bit	Provides 512 bits of entropy input and 256 bits of nonce to construct a seed for CTR_DRBG. The module requests 256 amount of entropy for entropy source to provide 256 security strength.

Table 13. Non-Deterministic Random Number Generation Specification

[16] *Estimated amount of entropy per the source's output bit is 0.85444 and Samsung conservatively claims to be set at 0.5 per bit.*

10. Self-Tests

While executing the following self-tests, all data output is inhibited until the completion of the self-test. The operator can initiate pre-operational tests on-demand by power-cycling the module. Conditional self-tests are conducted before the initial operation of approved algorithms. If a cryptographic module fails a self-test, it will enter an error state, during which all data output is inhibited.

10.1. Pre-Operational Test

Algorithm	Type	Description
ECDSA	Firmware integrity test	Firmware integrity test is performed by using ECDSA with SHA2-384[17] at every power-on-reset.

Table 14. Pre-operational Self-tests

10.2. Conditional Test

Algorithm	Type	Description
DRBG	Cryptographic algorithm self-test	KATs: SP 800-90A Health testing on Instantiate, Generate and Reseed functions
DRBG	Cryptographic algorithm self-test	KAT: DRBG with AES-256 is performed
AES-XTS	Critical function test	Duplicate Key Test for AES-XTS described in FIPS 140-3 IG C.I (i.e. key_1 ≠ key_2)
AES-XTS	Cryptographic algorithm self-test	KAT: Encrypt is performed
AES-XTS	Cryptographic algorithm self-test	KAT: Decrypt is performed
ECDSA	Cryptographic algorithm self-test	KAT: Curve P-384 with SHA2-384 signature verification is performed
SHA2-256	Cryptographic algorithm self-test	KAT: Hash digest is performed
SHA2-384	Cryptographic algorithm self-test	KAT: Hash digest is performed
HMAC	Cryptographic algorithm self-test	KAT: HMAC with SHA2-256 is performed
AES-GCM	Cryptographic algorithm self-test	KAT: Encrypt is performed
AES-GCM	Cryptographic algorithm self-test	KAT: Decrypt is performed
PBKDF2	Cryptographic algorithm self-test	KAT: Password based key derivation using HMAC with SHA2-256 is performed
ECDSA	Firmware load test	ECDSA signature verification is performed if new FW is downloaded or at every power-on-reset
ENT (P)	Cryptographic algorithm self-test	Conditional SP800-90B Heath tests: Repetition count test, Adaptive proportion test

Table 15. Conditional Self-tests

[17] *ECDSA and SHA2-384 KAT are performed prior to the firmware integrity test*

11. Life-Cycle Assurance

Failure to follow the requirements for the Approved Mode of Operation or the rules in Section 11 will result in the module operating in a non-compliant state, which is out of scope for this validation.

The following specifies the security rules under which the cryptographic module shall operate in accordance with FIPS 140-3:

- The cryptographic module always operates in Approved Mode once the Secure Installation instructions are followed.
- The steps required for the secure installation, initialization, and start-up of the cryptographic module, as per FIPS 140-3 VE11.33.01 are as follows:

11.1. Secure Installation

1. The user should examine for tamper evidence.
   - Inspect the entire perimeter for cracks, gouges, missing screw(s), and other signs of tampering, including the tamper-evident sealing label.
   - If there is any sign of tampering, do not use the product and contact Samsung.
2. Identify the firmware version in the device.
   - Confirm that the firmware version is equivalent to the version(s) listed in this document via NVM express Identify Controller command.
3. Take the drive's ownership.
   - Change SID's PIN by setting a new PIN.
   - Activate the Locking SP by using the Activate method.

   Note: If required to enable the additional Admin authorities in Locking SP, new PINs must be set by the Cryptographic Officer.
4. Periodically examine the tamper evidence
   - If there is any sign of tampering, stop using the product to avoid potential security hazards or information leakage.

11.2. Operational Description of Module

- The cryptographic module maintains strict logical separation of data input, data output, control input, control output, and power.
- The cryptographic module does not output CSPs in any form.
- The cryptographic module provides the Approved DRBG for generating all cryptographic keys which complies with Section 6.1 of the SP 800-133r2.
- Power cycling the module re-locks the previous unlocked "IO command" service.
- The cryptographic module enforces a limited operational environment by the secure firmware load test using ECDSA with SHA2-384.
- The cryptographic module provides a production-grade cryptographic boundary.
- The cryptographic module enters the error state upon failure of Self-tests. Most commands except for supported command from the Host (General Purpose Computer (GPC) outside the cryptographic boundary) are rejected in the error state and the IO command returns Namespace Not Ready (SC=0x82, SCT=0x0), the other commands return Internal Error (SC=0x6, SCT=0x0) defined in NVMe specification via the status output. Cryptographic services and data output are explicitly inhibited when in the error state. When module fails FW Integrity test performed by Mask ROM, the module will fail to boot; module will not service any requests or provide any status output (module hangs).
- The cryptographic module satisfies the requirements of FIPS 140-3 IG C.I (i.e. key_1 ≠ key_2)
- The module generates at a minimum 256 bits of entropy for use in key generation.
- Bypass capability is not applicable to the cryptographic module
- The module generates symmetric keys which are unmodified outputs from the DRBG.
- As specified in NIST SP 800-132, keys derived from passwords/passphrases are only used in storage applications.
- AES-XTS is only approved for storage applications.

12. Mitigation of Other Attacks

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