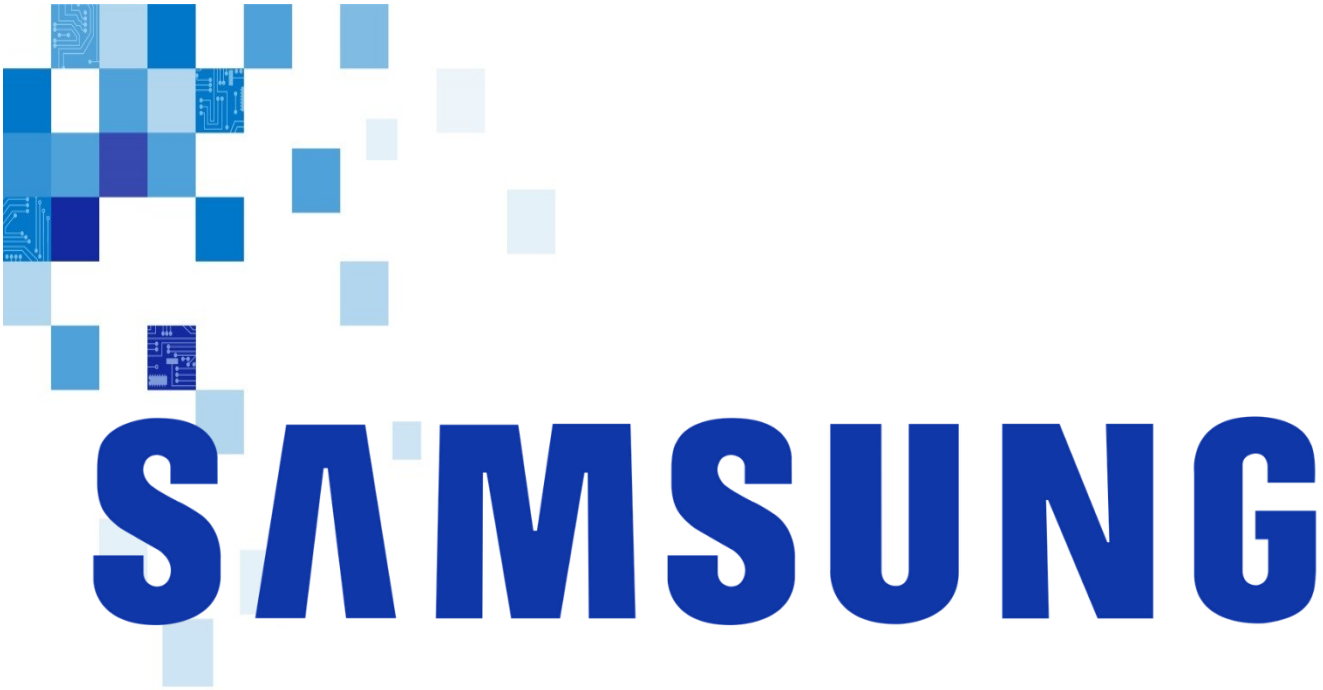

Samsung NVMe TCG Opal SSC SEDs PM9A3 Series

FIPS 140-3 Non-Proprietary Security Policy

Document Version: 1.0

H/W Version: MZ1L2960HCJR-00AMV[1], MZ1L21T9HCLS-00AMV[1], MZ1L23T8HBLA-00AMV[1], MZCL21T9HCJR-00AMV[2], MZCL23T8HCLS-00AMV[2], MZCL27T6HBLA-00AMV[2] and MZEL215THBLA-00AMV[3]

F/W Version: GDC76M4Q[1], GDC79M4Q[1], GDC62M4Q[2], GDC63M4Q[2], GDDB3M2Q[3], GDDB4M2Q[3]

Revision History

Version	Change
1.0	Initial Version

Table of Contents

1. General

1.1. Scope

This document outlines the security policy for Samsung Electronics Co., Ltd. **Samsung NVMe TCG Opal SSC SEDs PM9A3 Series**, herein after referred to as the "cryptographic module" or "module", SSD (Solid State Drive). This module satisfies all applicable FIPS 140-3 Security Level 1 hardware cryptographic module requirements. It supports TCG Opal SSC based SED (Self-Encrypting Drive) features that is designed to protect unauthorized access to the user data stored in its NAND Flash memories. The cryptographic module's controller has built-in AES hardware engines that provide on-the-fly encryption and decryption of the user data without performance loss. The SED design also allows for instant data sanitization via cryptographic erase.

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

Table 1. Security Levels

1.2. Acronyms

Acronym	Description
CTRL	Controller
CPU	Central Processing Unit (ARM-based)
DRAM	Dynamic Random Access Memory
DRAM I/F	Dynamic Random Access Memory Interface
ECC	Error Correction Code
EDC	Error Detection Code
KAT	Known-answer Test
LBA	Logical Block Address
MEK	Media Encryption Key
PSID	Physical Presence SID (Security Identifier)
NAND	NAND Flash Memory
NAND I/F	NAND Flash Interface
NVMe	Non-Volatile Memory Host Controller Interface Specification
ROM	Read-Only Memory

Table 2. Acronyms

2. Cryptographic Module Specification

2.1. Hardware and Physical 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.

Below are photographs showing the cryptographic module views of each form factor. The multiple-chip embedded cryptographic module includes both hardware and firmware components.

The cryptographic boundary of the M.2 module is defined as the physical perimeter of the PCB.

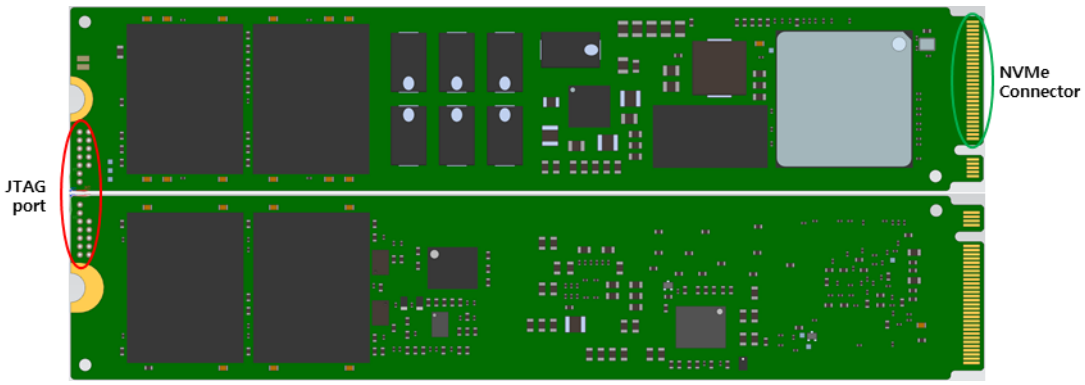

Figure 1. Specification of the PM9A3 M.2 Form Factor Cryptographic Boundary

The E1.S and E1.L cryptographic modules are each enclosed in two aluminum alloy cases. These cases define the modules' cryptographic boundary.

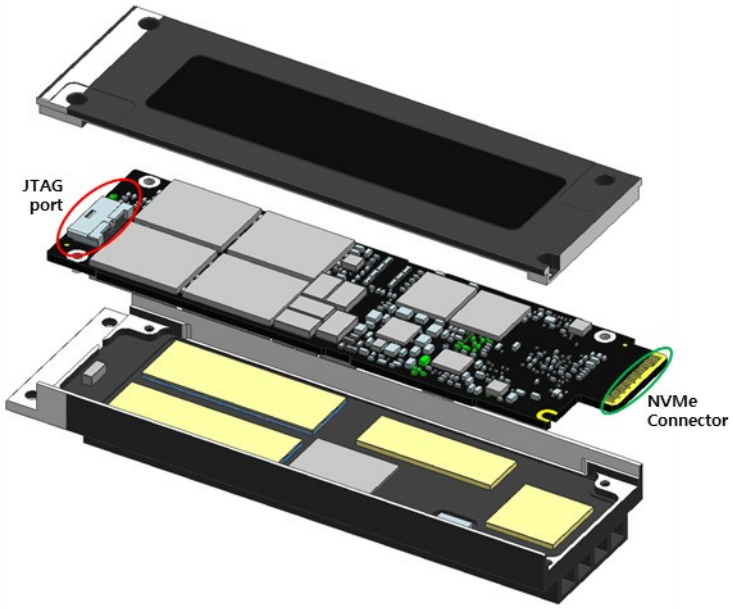

Figure 2. Specification of the PM9A3 E1.S Form Factor Cryptographic Boundary

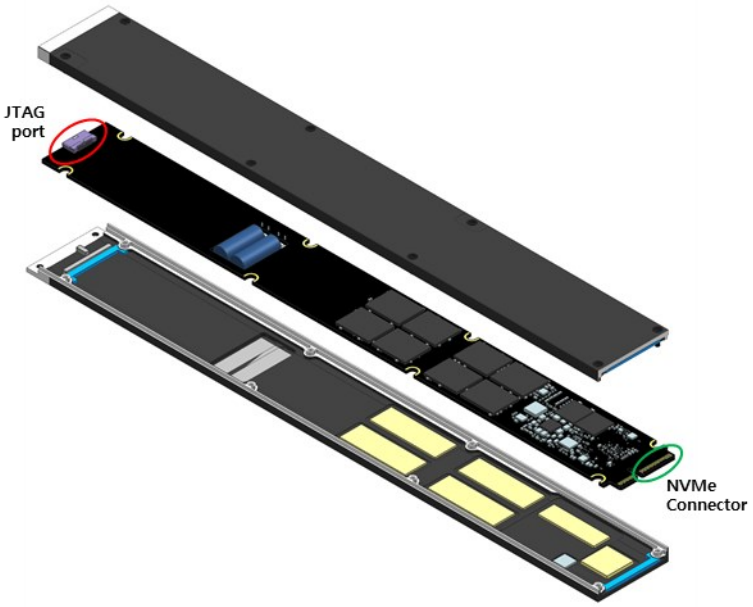

Figure 3. Specification of the PM9A3 E1.L Form Factor Cryptographic Boundary

2.2. Module Cryptographic Boundary

The PM9A3 series utilizes a single-chip controller with an NVMe interface for system side communication and integrates Samsung NAND flash memory for internal storage. The following figure depicts the module's operational environment.

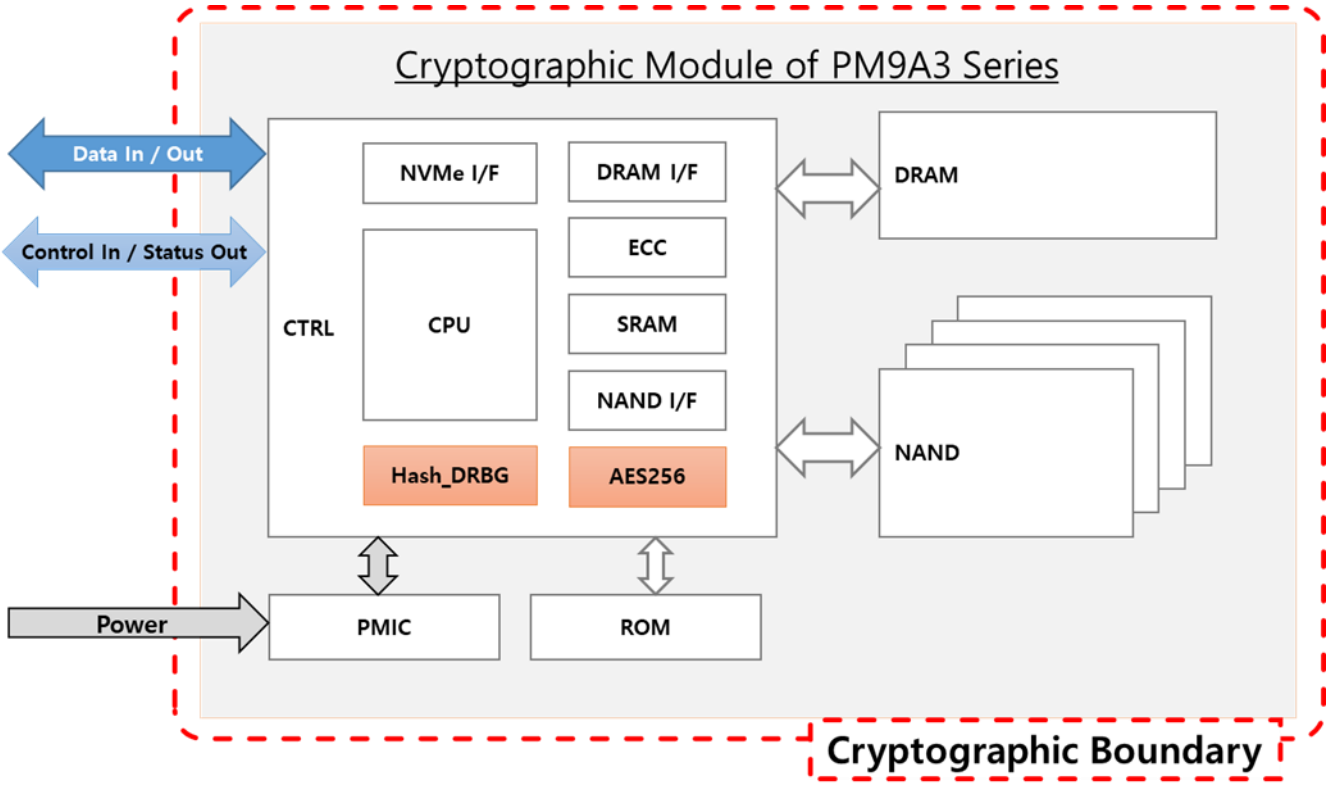

Figure 4. Block Diagram for Samsung NVMe TCG Opal SSC SEDs PM9A3 Series

2.3. Version information

Model	Hardware Version	Firmware Version	Distinguishing Features
PM9A3	MZ1L2960HCJR-00AMV	GDC76M4Q GDC79M4Q	960GB
	MZ1L21T9HCLS-00AMV		1.92TB
	MZ1L23T8HBLA-00AMV		3.84TB
	MZCL21T9HCJR-00AMV	GDC62M4Q GDC63M4Q	1.92TB
	MZCL23T8HCLS-00AMV		3.84TB
	MZCL27T6HBLA-00AMV		7.68TB
	MZEL215THBLA-00AMV	GDDB3M2Q GDDB4M2Q	15.36TB

Table 3. Cryptographic Module Tested Configuration

2.4. Cryptographic Functionality

The module does not implement any "Non-Approved Algorithms Not Allowed in the Approved Mode of Operation".

2.4.1. Approved Algorithm

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
A1157	AES / FIPS 197, SP 800-38A	ECB	256 bits	Prerequisite for AES-XTS (A1157)
A1157	AES / FIPS 197, SP 800-38E	XTS[1]	256 bits	Data Encryption / Decryption
A1153	DRBG / SP 800-90A Rev. 1	Hash_ DRBG (SHA-256)	N/A	Deterministic Random Bit Generation
A1155	RSA / FIPS 186-4	SigVer	3072 bits	Digital Signature Verification
A1158	SHS / FIPS 180-4	SHA-256	N/A	Message Digest
Vendor Affirmed	CKG / SP 800-133 Rev. 2	Section 4 and Section 6.1	N/A	Cryptographic Key Generation (Symmetric keys which are direct unmodified outputs from the DRBG)
N/A	ENT (P) / SP 800-90B	N/A	N/A	Non-deterministic Random Number Generator (only used for generating seed materials for the DRBG). Provides a minimum of 256 bits of entropy for DRBG seed.

Table 4. Approved Algorithms

Note that not all algorithms/modes that appear on the module's CAVP certificates are utilized by the module. Table 4 lists only the algorithms/modes that are utilized by the module.

2.4.2. Non-Approved Algorithm

The following algorithms are not intended to be used as security functions, and not used whatsoever to meet any FIPS 140-3 requirements. These algorithms are not provided through a non-approved services to an operator.

Algorithm	Caveat	Use / Function
AES-XTS / FIPS 197, SP 800-38E	No Security Claimed; AES-XTS is only used for firmware decryption during ROM initialized.	Firmware Decryption
AES-CCM / FIPS 197, SP 800-38C	No Security Claimed; Non-approved algorithms here are only used for encrypting or obfuscating the CSP.	Key Encryption and Decryption
PBKDF2		Key Derivation
HMAC / SHA-256		Key Derivation

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

2.5. Approved Mode of Operation

[1] *AES-ECB is the pre-requisite for AES-XTS; AES-ECB alone is NOT supported by the cryptographic module in approved mode.*

The module always defaults to an Approved mode of operation. To ensure it remains in this mode, operators must strictly follow the guidance outlined in section 11. The user can verify the module's Approved status using the “Show Status” Service in Table 7 via the NVM Express Identify Controller command.

3. Cryptographic Module Interfaces

The module doesn’t support a Control output interface.

Physical port	Logical interface	Data that passes over port/interface
NVMe Connector	Data Input / Output	Plaintext data; signed 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
JTAG	Control Input	Signals input logically or physically via one or more physical ports
	Status Output	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 module does not support role authentication. Roles are implicitly assumed based on the service they are invoking.

Role	Service	Input	Output
Cryptographic Officer (CO)	Show Status	N/A	Status
	Lock/Unlock an LBA Range	LBA Range	Status
	Erase an LBA Range's Data	LBA Range	Status
	Update the firmware	FW image binary	Status
	Get Random Number	N/A	Status
	IO Command	LBA	Status
	FormatNVM / Sanitize / DeleteNS	LBA Range	Status
	Revert	PSID	N/A
Maintenance[2]	Diagnostics	N/A	N/A

Table 7. Roles, Service Commands, Input and Output

4.2. Approved Services

The cryptographic module does not offer bypass capabilities.

E: EXECUTE; W: WRITE; G: GENERATE; Z: ZEROISE

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys and SSPs				Indicator[3]
					E	W	G	Z	
Show Status	Show approved version status of the module / FIPS fail mode	N/A	N/A	Cryptographic Officer (CO)					NVM Command: Identify Controller command Result : Status Code
Lock/Unlock an LBA Range	Block or allow read (decrypt) / write (encrypt) of user data.	N/A	MEK[4]			O		O	UID: Locking_GlobalRange / Locking_RangeNNNN TCG Method: Set Result: TCG status code
Erase an LBA Range's Data	Erase user data by changing the data encryption key.	Hash_ DRBG (SHA-256) CKG ENT (P)	DRBG Internal State V value		O		O		UID: K_AES_256_GlobalRange_Key / K_AES_256_RangeNNNN_Key TCG Method: GenKey Result: TCG status code
			DRBG Internal State C value		O		O		
			DRBG Seed		O		O		
			DRBG Entropy Input String		O		O		
			MEK			O	O	O	
Revert	Erase user data in all Range by	Hash_ DRBG (SHA-256)	DRBG Internal State V value		O		O		UID: SPObj(AdminSP) TCG Method: Revert

[2] *Maintenance role is operator that is responsible for using the JTAG*

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

[4] *Specified type of access of Lock/Unlock an LBA Range service to MEK was limited to only RAM*

	changing the data encryption key, initialize range settings, and reset PINs for TCG.	CKG ENT (P)	DRBG Internal State C value		O		O		Result: TCG status code
			DRBG Seed		O		O		
			DRBG Entropy Input String		O		O		
			MEK			O	O	O	
Update the firmware	Update the firmware	RSA	FW Verification Key		O				Admin Command: Firmware Commit Result : Status Code
Get Random Number	Provide a random number generated by the CM.	Hash_ DRBG (SHA-256) CKG ENT (P)	DRBG Internal State V value		O		O		UID: ThisSP TCG Method: Random Result: TCG status code
			DRBG Internal State C value		O		O		
			DRBG Seed		O		O		
			DRBG Entropy Input String		O		O		
IO Command	Read/Write user data	AES-XTS	MEK		O				NVM Command: Write / Read Result : Status Code
FormatNVM / Sanitize / DeleteNS	Erase user data by changing the data encryption key.	Hash_ DRBG (SHA-256) CKG ENT (P)	DRBG Internal State V value		O		O		Admin Command: Format NVM / Sanitize / Namespace Management Result : Status Code
			DRBG Internal State C value		O		O		
			DRBG Seed		O		O		
			DRBG Entropy Input String		O		O		
			MEK			O	O	O	
Diagnostics	Perform Maintenance	N/A	N/A	Maintenance					N/A

Table 8. Approved Services

5. Software/Firmware Security

- The cryptographic module employs a 428-byte error detection code 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. 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.

- Firmware download is only available for CMVP validated firmware versions. Unauthorized modification of the firmware is prevented by the pre-operational firmware integrity test and conditional firmware load test.

- Since the cryptographic module is zeroised through the procedure for using maintenance role, it is restricted preventing uncontrolled access to CSPs and uncontrolled modifications of SSPs.

7. Physical Security

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

- Production grade components.

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 components	N/A	N/A

Table 9. Inspection/Testing of Physical Security Mechanisms

The cryptographic module supports the Maintenance role. To assume the Maintenance role, operators must comply with the following rule:

- The operator must zeroise all SSPs listed in the Table 10 by invoking the Revert service in the Table 8 and initiate the Power on reset before entering the Maintenance role.
- To exit the Maintenance role, the operator must procedurally perform the Revert service in the Table 8 and perform a power-on reset of the module. To finish with, the operator performing the Show Status service in Table 8 confirms the original firmware version listed in the Table 3 remains unchanged.
- The operator is responsible for managing the module's JTAG port and should conduct regular inspections associated with the enabled JTAG port as frequently as possible in order to prevent potential security risks such as potential code modifications with no firmware load test, reading and writing of register information or other impactful security changes.

8. Non-Invasive Security

- The module does not implement any non-invasive attack mitigation techniques. Therefore, this section is not applicable.

9. Sensitive Security Parameter Management

- Temporary SSPs and SSPs stored in volatile memory are automatically zeroized upon power-on reset.
- The module performs zeroization by overwriting the target SSP with random values generated by the DRBG.
- The module does not import or export SSPs.

Key / SSP Name / Type	Strength	Security Function and Cert. Number	Generation	Establishment	Import / Export	Storage	Zeroisation	Use & related keys
DRBG Internal State V value	440-bit	Hash_ DRBG (SHA-256) / A1153	SP 800-90A HASH_DRBG (SHA-256)	N/A	N/A	Plaintext in RAM	Implicitly zeroised by Power on reset	MEK
DRBG Internal State C value	440-bit	Hash_ DRBG (SHA-256) / A1153	SP 800-90A HASH_DRBG (SHA-256)	N/A	N/A	Plaintext in RAM	Implicitly zeroised by Power on reset	MEK
DRBG Seed	N/A	Hash_ DRBG (SHA-256) / A1153	ENT (P)	N/A	N/A	Plaintext in RAM	Implicitly zeroised by Power on reset	MEK
DRBG Entropy Input String	N/A	Hash_ DRBG (SHA-256) / A1153	ENT (P)	N/A	N/A	Plaintext in RAM	Implicitly zeroised by Power on reset	MEK
MEK	256-bit	AES-XTS / A1157	SP 800-90A HASH_DRBG (SHA-256)	N/A	N/A	Plaintext in RAM	Implicitly zeroised by Power on reset / Explicitly zeroised via “Unlock an LBA Range” service and indicate with its indicator	Data encryption and decryption of user data
						Plaintext in Flash	Explicitly zeroised via “Erase an LBA Range’s Data”, “Revert” and “FormatNVM / Sanitize /	

							DeleteNS" services and indicate with their indicators	
Firmware Verificati on Key[5]	128-bit	RSA / A1155	Generated during the manufacturing process, is included as part of the FW.	N/A	N/A	Plaintext in HW SFR[6]	Implicitly zeroised by Power on reset and after completion of "Update the firmware" service	Firmware Load Test

Table 10. SSPs

- The module contains an entropy source, compliant with SP 800-90B, within the module's cryptographic boundary.

Entropy sources	Minimum number of bits of entropy	Details
ENT (P)	0.5 entropy per bit[7]	Entropy source for Hash_DRBG

Table 11. Non-Deterministic Random Number Generation Specification

[5] *This is not considered an SSP.*

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

[7] *Estimated amount of entropy per the source's output bit is 0.841621 and Samsung conservatively claims to be set at 0.5 per bit.*

10. Self-Tests

All cryptographic algorithm self-tests are executed during power-on. While executing the following self-tests, all data output is inhibited until the self-test completes. To execute the pre-operational tests on-demand, the operator may power-cycle the module. Cryptographic algorithm self-tests are performed prior to the approved algorithms' first use. If a cryptographic module fails a self-test, the module will enter an error state. While in this state, all data output is inhibited.

10.1. Pre-Operational Test

Algorithm	Type	Description
EDC	Firmware integrity test	Firmware integrity test is performed by using 428 byte error correction code (ECC) at power-on.

Table 12. Pre-operational Self-tests

10.2. Conditional Test

Algorithm	Type	Description
AES	Critical function test	Duplicate Key Test for AES-XTS described in FIPS 140-3 IG C.I (i.e. key_1 ≠ key_2) when key is generated
AES	Cryptographic algorithm self-test	KAT: AES-256 XTS mode encryption and decryption
AES	Cryptographic algorithm self-test	KAT: AES-256 ECB mode encryption and decryption
SHS	Cryptographic algorithm self-test	KAT: SHA-256 hash digest
RSA	Cryptographic algorithm self-test	KAT: RSA-3072 verification is performed before firmware load test
RSA	Firmware load test	RSA-3072 with SHA-256 signature verification is performed if new FW is downloaded.
DRBG	Cryptographic algorithm self-test	KATs: HASH-DRBG(SHA2-256), SP 800-90A Health testing on Instantiate, Generate and Reseed functions
ENT (P)	Cryptographic algorithm self-test	Startup and Conditional SP800-90B Heath tests: Repetition count test, Adaptive proportion test

Table 13. Conditional Self-tests

The cryptographic module enters the error state upon failure of Self-tests. All commands from the Host (General Purpose Computer (GPC) outside the cryptographic boundary) are rejected in the error state and the cryptographic module returns an FIPS Fail Mode (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.

11. Life-Cycle Assurance

The cryptographic module operates in the Approved mode of operation by default once shipped from the vendor's manufacturing site and does not support a non-approved mode of operation. The following guidance in section 11.1 describes the rules for secure installation and operation which the operator shall follow to operate the cryptographic module in a FIPS 140-3 security level 1 compliant manner.

11.1. Secure Installation

- Identify the firmware version in the device
  - Confirm the firmware version matches to the version(s) listed in this document using the NVM Express Identify Controller command.

11.2. Operational Description of Module

- The cryptographic module employs AES-XTS exclusively for storage applications.
- The cryptographic module maintains strict logical separation between data input, output, control input, status output, and power.
- The cryptographic module does not output CSPs in any form.
- The cryptographic module utilizes the Approved DRBG for generating all cryptographic keys.
- The module generates at a minimum 256 bits of entropy for use in key generation.
- Operators must perform a power-on reset of the module after using the "Update the firmware" service to execute a new firmware validated by a validation authority.

12. Mitigation of Other Attacks

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