Samsung SATA TCG Opal SSC SEDs PM893 Series

FIPS 140-3 Non-Proprietary Security Policy

Document Version: 1.0

Hardware Version: MZ7L3480HCHQ-00AMV, MZ7L3960HCJR-00AMV

Firmware Version: JXTC1M8Q

Revision History

Version	Change
1.0	Initial Version

Table of Contents

I. Introduction

I.1. Scope

This document is a non-proprietary security policy for **SAMSUNG SATA TCG Opal SSC SEDs PM893 Series**, hereinafter referred to as a "cryptographic module" or "module". The SSD (Solid State Drive) satisfies all applicable FIPS 140-3 Security Level 1 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.

I.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 Correcting 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
SATA	Serial ATA(Advanced Technology Attachment)
ROM	Read-Only Memory

Table 1. Acronyms

1. General

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 2. Security Levels

2. Cryptographic Module Specification

2.1. Cryptographic Boundary

The following photographs depict the different views of the cryptographic module. This multiple-chip embedded module comprises both hardware and firmware components. The module type is hardware.

The cryptographic boundary of the module is the physical perimeter of the PCB as following.

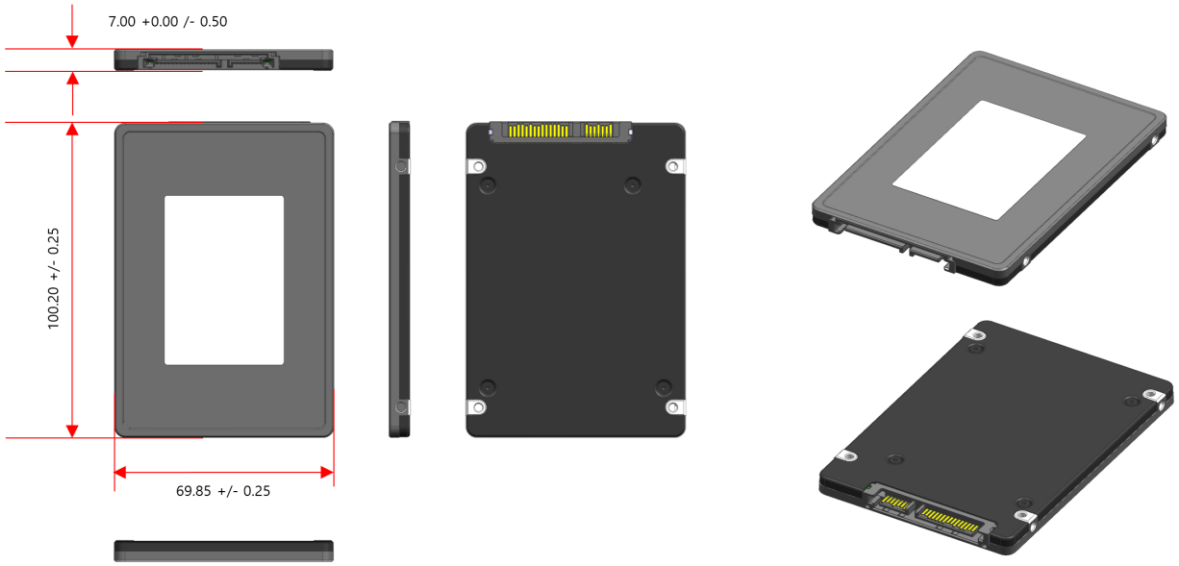

Figure 1. Specification of the PM893 2.5'' Form Factor Cryptographic Boundary

The firmware utilizes a single-chip controller with a SATA interface on the system side, as well as Samsung NAND flash. The following figure depicts the module's operational environment. The firmware version included within the scope of this validation must be validated through the FIPS 140-3 CMVP. Any firmware loaded onto this module that is not shown on the module certificate, is out of the scope of this validation and requires a separate FIPS 140-3 validation.

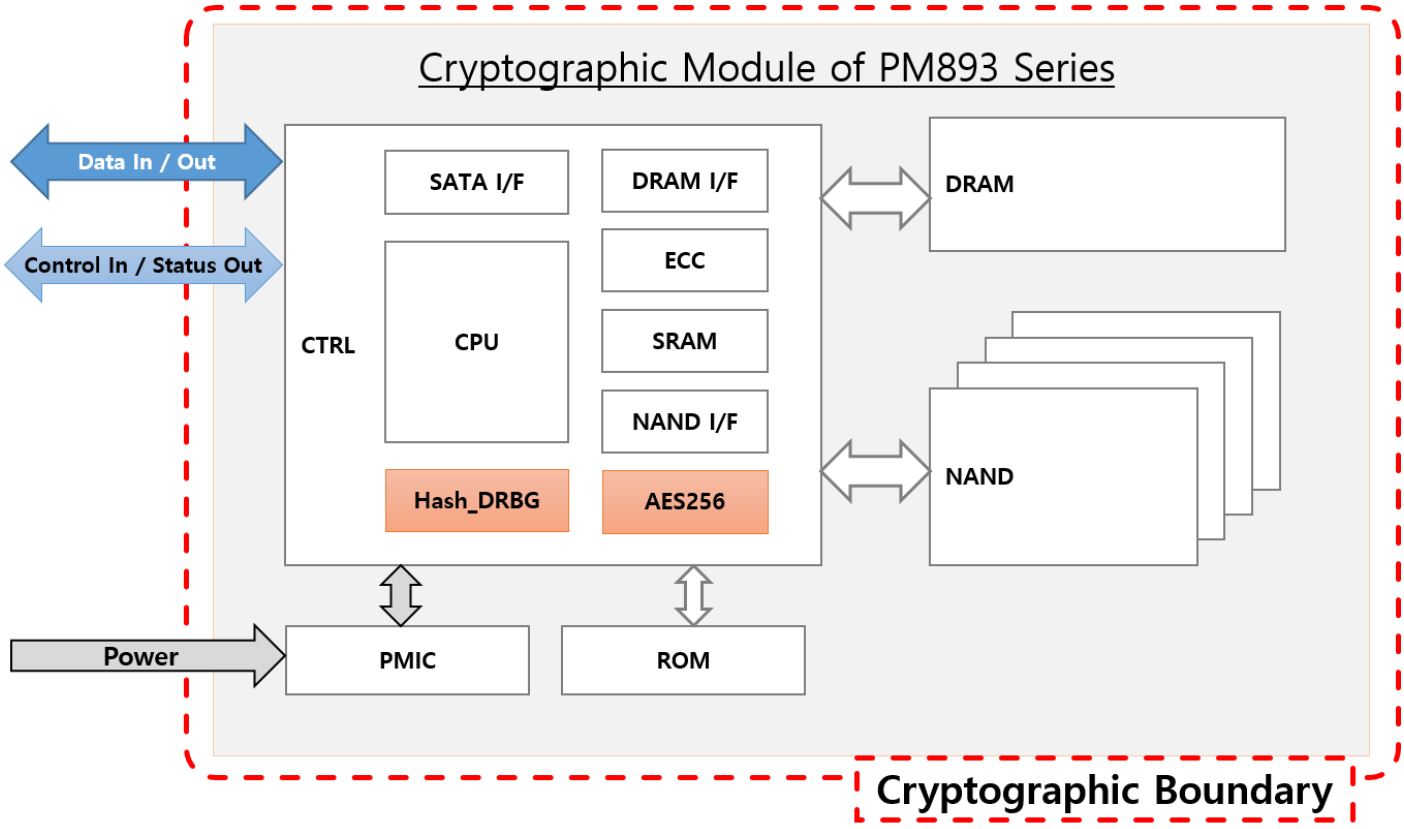

Figure 2. Block Diagram for Samsung SSD SATA TCG Opal SSC SEDs PM893 Series

2.2. Version Information

Model	Hardware Version	Firmware Version	Distinguishing Features
PM893	MZ7L3480HCHQ-00AMV	JXTC1M8Q	480GB
	MZ7L3960HCJR-00AMV		960GB

Table 3. Cryptographic Module Tested Configuration

2.3. Cryptographic Functionality

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

2.3.1. 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
A2107	Hash DRBG / SP 800-90A Rev. 1	Hash_ DRBG (SHA2-256)	Prediction Resistance: No Supports Reseed	Deterministic Random Bit Generation
A2108	AES-ECB / FIPS 197, SP 800-38A	ECB	256-bit keys with 256-bit key strength	Prerequisite for AES-XTS (A2108)
A2108	AES-XTS / FIPS 197, SP 800-38E	XTS	256-bit keys with 256-bit key strength	Data Encryption and Decryption
A2109	SHA2-256 / FIPS 180-4	SHA2-256	SHA2-256	Message Digest
A2110	RSA SigVer / FIPS 186-4	PSS SigVer (SHA2-256)	2048 bits	Digital Signature Verification
Vendor Affirmed	CKG / SP 800-133 Rev. 2 (Section 4, 5.1, 6.3)	N/A	N/A	Cryptographic Key Generation using 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.

2.3.2. Non-Approved Algorithm

Algorithm	Caveat	Use / Function
AES-CCM / FIPS 197, SP 800-38C	No Security Claimed; Non-approved algorithm here is only used for obfuscation and removal of obfuscation the CSP. (IG 2.4.A Scenario #1)	Key obfuscation and removal of obfuscation
AES-XTS / FIPS 197, SP 800-38E	No security claimed; AES-XTS is only used to remove obfuscation from the firmware during ROM initialized.	Firmware obfuscation removal
HMAC-SHA2-256 / FIPS 198-1 (non-compliant)	Non-approved algorithm here are only used as pre-requisite algorithms for PBKDF2 which is used for storing authentication data. (IG 2.4.A Scenario #1)	Store authentication data
PBKDF2 / SP 800-132	Non-approved algorithms here are only used for storing authentication data using PBKDF2 (IG 2.4.A Scenario #1)	Store authentication data
SHA2-256 / FIPS 180-4 (non-compliant)	Non-approved algorithm here are only used as pre-requisite algorithms for PBKDF2 which is used for storing authentication data. (IG 2.4.A Scenario #1)	Store authentication data

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

2.4. Approved Mode of Operation

The module only supports one mode of operation: the Approved mode, in which the Approved cryptographic functions are available. The module automatically transitions to the Approved mode of operation after completing its pre-operational self-tests. The cryptographic module indicates its approved mode through the validated version status, displayed by the Show Status Service in Table 8 via the ATA Identify Controller command. In the approved mode of operation, non-approved algorithms are allowed, but with no security claims in the module.

3. Cryptographic Module Interfaces

The module doesn't support a Control output interface.

Physical Port	Logical Interface Type	Data that Passes Over Port / Interface
SATA Connector	Data Input / Output	Plaintext data; signed data; User Data Input / Output
	Control Input	SATA Command Input logically via an API; signals input logically or physically via one or more physical ports
	Status Output	SATA Command Execution Response logically via an API; signal outputs logically or physically via one or more physical ports
JTAG	Control Input	JTAG signal input logically or physically via physical ports
	Status Output	Diagnostic Information outputs logically or physically via one or more physical ports

Table 6. Ports and Interfaces

4. Roles, Services, and Authentication

4.1. Role

The cryptographic module does not support role-based authentication. Roles are implicitly assumed based on the service they are invoking.

Role	Service	Input	Output
Cryptographic Officer (CO)	Show Status	ATA Command	Status
	Lock/Unlock an LBA Range	LBA Range	Status
	Erase an LBA Range's Data	LBA Range	Status
	Update the firmware	Firmware image binary	Status
	Get Random Number	TCG Command	Status
	IO Command	LBA Range	Status
	Sanitize	LBA Range	Status
	Revert	PSID	N/A
	Perform the Self-tests	N/A	Status
	Authentication	N/A	Status
Maintenance[1]	Diagnostics	N/A	N/A

Table 7. Roles, Service Commands, Input and Output

4.2. Approved Services

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.

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

Service	Description	Approved Security Functions	SSPs	Roles	Type(s) of Access				Indicator[2]
					E	W	G	Z	
Show Status	Show approved version status of the module / FIPS fail mode	N/A	N/A	CO					ATA 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[3]		O	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 / A2107 SHA2-256 / A2109	DRBG "V" Value		O		O		UID: K_AES_256_GlobalRange_Key / K_AES_256_RangeNNNN_Key
			DRBG "C" Value		O		O		
			DRBG Seed		O		O		

[1] *Maintenance role is an operator responsible for using the JTAG.*

[2] *The result of ATA or TCG command is used as an indicator.*

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

		CKG ENT(P)	DRBG Entropy Input String		O		O		TCG Method: GenKey Result: TCG status code
			MEK			O	O	O	
Update the Firmware	Update the firmware	RSA SigVer / A2110	Firmware Verification Key		O				Admin Command: DOWNLOAD MICROCODE Result : Status Code
Get Random Number	Provide a random number generated by the CM	Hash_ DRBG / A2107 SHA2-256 / A2109 CKG ENT(P)	DRBG "V" Value		O		O		UID: ThisSP TCG Method: Random Result: TCG status code
			DRBG "C" Value		O		O		
			DRBG Seed		O		O		
			DRBG Entropy Input String		O		O		
IO Command	Read / Write user data	AES-XTS / A2108	MEK		O				ATA Command: Read / Write Result : Status Code
Sanitize	Erase user data by changing the data encryption key	Hash_ DRBG / A2107 SHA2-256 / A2109 CKG ENT(P)	DRBG "V" Value		O		O		Admin Command: SANITIZE DEVICE / SECURITY ERASE UNIT Result : Status Code
			DRBG "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 changing the data	Hash_ DRBG / A2107 SHA2-256 / A2109 CKG ENT(P)	DRBG "V" Value		O		O		UID: SPObj (Admin SP) TCG Method: Revert Result: TCG status code
			DRBG "C" Value		O		O		
			DRBG Seed		O		O		
			DRBG Entropy Input String		O		O		
			MEK			O	O	O	
Perform the Self-tests	Power cycling the module to perform self-tests	N/A	N/A						Level 0 Discovery CMD return a failure as a failure indicator
Authentication	Authenticate the module. (This is not authentication to meet the FIPS 140-3 requirements)	No Security Claimed – PBKDF2 HMAC-SHA2-256 (non-compliant) SHA2-256 (non-compliant)	N/A						N/A
Diagnostics	Perform Maintenance	N/A	N/A	Maintenance					N/A

Table 8. Approved Services

5. Software/Firmware Security

- The LDPC (Low-density parity-check) code is applied for integrity test to firmware components of cryptographic module.
- When firmware is downloaded into the module, 1024 bytes LDPC parity data per each 8KB data size is generated and integrity test is performed by verifying it every time it is loaded to initiate.
- The firmware integrity test is performed when power on reset.

6. Operational Environment

- The cryptographic module operates in a limited operational environment, consisting of the module's firmware. This limited operational environment 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 zeroized through the maintenance role procedure, it is restricted to prevent uncontrolled access to CSPs and unauthorized modifications to SSPs.

7. Physical Security

The following physical security mechanisms are implemented in a 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	Import / Export	Establish-ment	Storage	Zeroisation	Use & Related Keys
DRBG "C" Value / CSP	440-bit	Hash_ DRBG / A2107 SHA2-256 / A2109	SP 800-90A Hash_ DRBG / A2107 SHA2-256 / A2109	N/A	N/A	Plaintext in RAM	Implicitly zeroised by Power on reset	Generates the MEK
DRBG "V" Value / CSP	440-bit	Hash_ DRBG / A2107 SHA2-256 / A2109	SP 800-90A Hash_ DRBG / A2107 SHA2-256 / A2109	N/A	N/A	Plaintext in RAM	Implicitly zeroised by Power on reset	Generates the MEK
DRBG Seed / CSP	Entropy input: 512-bit Nonce 256-bit	Hash_ DRBG / A2107 SHA2-256 / A2109	ENT (P)	N/A	N/A	Plaintext in RAM	Implicitly zeroised by Power on reset	Generates the MEK
DRBG Entropy Input String / CSP	512-bit / 256-bit	Hash_ DRBG / A2107 SHA2-256 / A2109 ENT (P)	ENT (P)	N/A	N/A	Plaintext in RAM	Implicitly zeroised by Power on reset	Generates the MEK
MEK / CSP	256-bit	AES-XTS / A2108 CKG	SP 800-90A Hash_ DRBG / A2107 SHA2-256 / A2109	N/A	N/A	Plain Text in RAM	Implicitly zeroised by Power on reset / Explicitly zeroised via "Lock an LBA Range" 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 "Sanitize" services and indicate	

							with their indicator	
Firmware Verification Key / Non-SSP	112-bit	RSA SigVer / A2110 SHA2-256 / A2109	Entered during manufacturing	N/A	N/A	Plaintext in Hardware SFR[4]	Implicitly zeroised by Power on reset / Explicitly zeroised by after completion of "Update the firmware" with its indicator	Firmware Load Test
						Plaintext in ROM	N/A	

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[5]	Entropy source for Hash_DRBG

Table 11. Non-Deterministic Random Number Generation Specification

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

[5] *Estimated amount of entropy per the source's output bit is 0.72595 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. During the executing these self-tests, all data output is inhibited until the tests are completed. To execute the periodic self-test on-demand, the operator can power-cycle the module. If a cryptographic module fails a self-test, the module will enter an error state. While in this state, all data output is inhibited. Any additional requests for cryptographic services return a failure indicator.

10.1. Pre-operational Test

Algorithm	Type	Description
LDPC	Firmware integrity test	Firmware integrity test is performed by using 1024 byte error correction code (ECC) at power-on.

Table 12. Pre-operational Self-tests

10.2. Conditional Test

- The module does not support Periodic Self-Testing.

Algorithm	Type	Description
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) when key is generated
AES-XTS	Cryptographic algorithm self-test	KAT: AES-256 XTS mode encryption and decryption
AES-ECB	Cryptographic algorithm self-test	KAT: AES-256 ECB mode encryption and decryption
SHA2-256	Cryptographic algorithm self-test	KAT: SHA2-256 hash digest
RSA SigVer	Cryptographic algorithm self-test	KAT: RSA-2048 with SHA2-256 signature verification is performed before firmware load test
RSA SigVer	Firmware load test	RSA-2048 with SHA2-256 signature verification is performed if new FW is downloaded or at every power-on-reset
Hash DRBG	Cryptographic algorithm self-test	KATs: HASH-DRBG(SHA2-256)
Hash DRBG	Cryptographic algorithm self-test	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

10.3. Error States

Name	Description	Conditions	Recovery Method	Indicator
Error State	The module does not provide any crypto operation.	Any conditional known answer test failure.	Power Cycle	The firmware rejects all subsequent SATA commands by responding with 'Abort,' as specified in the SATA specification, and sets the device status to 'Device Fault.'
Download Mode		When the Integrity Test for the Bootloader fails.		
Hang		When the Integrity Test for the Main Firmware fails.		

Table 14: Error States

11. Life-Cycle Assurance

The cryptographic module operates in the Approved mode of operation by default upon shipment from the vendor's manufacturing site and does not support a non-approved mode of operation. Section 11.1 provides guidance on the rules for secure installation and operation. Operators must follow this guidance to ensure the cryptographic module operates in compliance with FIPS 140-3 security level 1 requirements.

11.1. Secure Installation

- Identify the firmware version in the device.
  - Confirm that the firmware version is equivalent to the version(s) listed in this document via ATA Identify Controller command.

11.2. Operational Description of Module

- The cryptographic module shall maintain logical separation of data input, data output, control input, status output, and power.
- The cryptographic module shall not output CSPs in any form.
- The cryptographic module shall use the Approved DRBG for generating all cryptographic keys.
- The cryptographic module shall enforce a limited operational environment by the secure firmware load test using RSA-2048 with SHA2-256.
- 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 as "Abort" in the error state and the cryptographic module returns "device fault" status as an FIPS Fail Mode defined in SATA specification via the status output. Cryptographic services and data output are explicitly inhibited when in the error state.
- 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.
- 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.
- The module generates symmetric keys which are unmodified outputs from the DRBG.
- If you require the "Samsung SED Product Manual", kindly reach out to the vendor contact information that is posted in certification.

12. Mitigation of Other Attacks

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