Samsung SAS TCG Enterprise SSC SEDs PM1653/PM1655 Series

FIPS 140-3 Non-Proprietary Security Policy

Document Version: 1.0

H/W Version:	**MZILG960HCHQ-00AC9, MZILG1T9HCJR-00AC9, MZILG3T8HCLS-00AC9, MZILG7T6HBLA-00AC9, MZILG15THBLA-00AC9, MZILG800HCHQ-00AC9, MZILG1T6HCJR-00AC9, MZILG3T2HCLS-00AC9, MZILG960HCHQ-00AD9, MZILG1T9HCJR-00AD9, MZILG3T8HCLS-00AD9, MZILG7T6HBLA-00AD9, MZILG800HCHQ-00AD9, MZILG1T6HCJR-00AD9, MZILG3T2HCLS-00AD9, MZILG3T8HCLS-00AG6, MZILG3T8HCLS-00AG7, MZILG3T8HCLS-00AVF, MZILG1T9HCJR-00AH9, MZILG3T8HCLS-00AH9, MZILG7T6HBLA-00AH9, MZILG15THBLA-00AH9**
F/W Version:	**EXG0, EZG0, EXG5, EZG5, EXG6, EZG6, NA50, MS00, 3P00, 3P01, DXG0, DZG0, DXG2, DZG2 and LEB0**

Revision History

Version	Changes
1.0	Initial version

Table of Contents

1. General

1.1. Scope

This document is non-proprietary Security Policy for **Samsung SAS TCG Enterprise SSC SEDs PM1653/PM1655 Series**, herein after referred to as a "cryptographic module" or "module", SSD (Solid State Drive), satisfies all applicable FIPS 140-3 security level 2 requirements, supporting TCG Enterprise SSC based SED (Self-Encrypting Drive) features, 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.

1.2. Acronyms

Acronym	Description
CTRL	RGX Controller (SAMSUNG RGX SAS TLC/MLC SSD Controller)
DRAM I/F	Dynamic Random Access Memory Interface
LBA	Logical Block Address
MD/EE	Manual Distribution/Electronic Entry
MEK	Media Encryption Key
MSID	Manufactured SID (Security Identifier)
NAND I/F	NAND Flash Interface
NDRNG	Non-Deterministic Random Number Generator
PMIC	Power Management Integrated Circuit
ROM	Read Only Memory
SAS I/F	Serial Attached SCSI Interface
SED	Self-Encrypting Drive
SICOC	Self-Initiated Cryptographic Output Capability
SSC	Security Subsystem Class
SSP	Sensitive Security Parameter
TCG	Trusted Computing Group

Table 1. Acronyms

1.3. Security Levels

The cryptographic module is intended to meet requirements of FIPS 140-3 Security Level 2 overall. The following table lists the module's FIPS 140-3 Security Level for each ISO/IEC 24759 sections.

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 2. Security Levels

2. Cryptographic module specification

2.1. Hardware and Physical Perimeter

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

The following photographs show the cryptographic module's top and bottom views. The multiple-chip standalone cryptographic module consists of hardware and firmware components that are all enclosed in two aluminum alloy cases, which serve as the physical perimeter of the module.

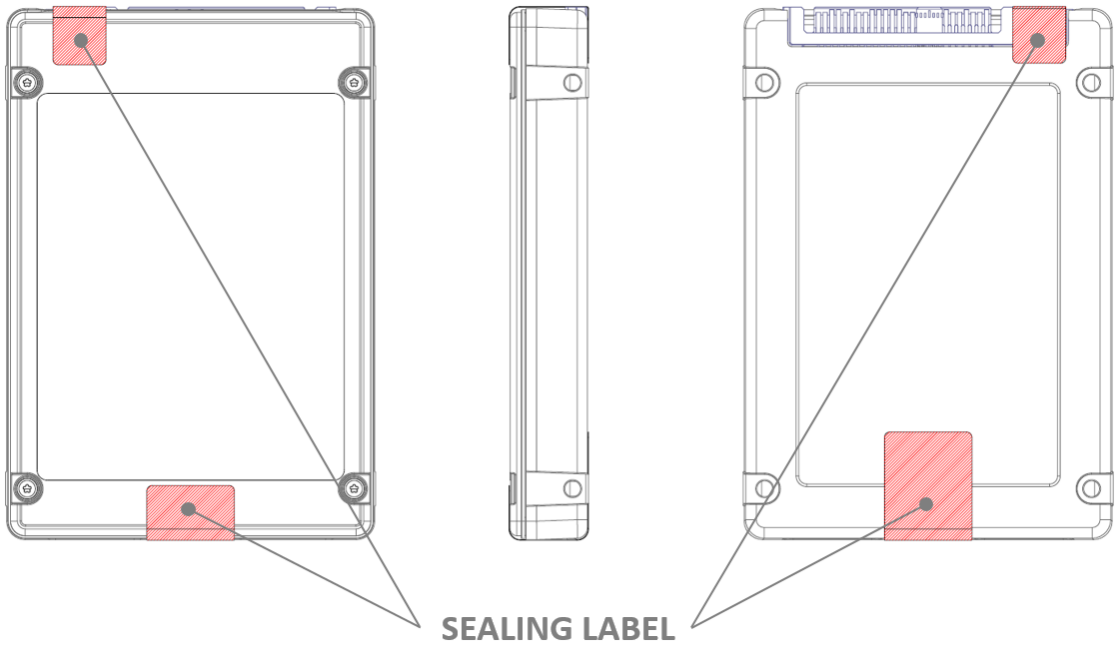

Figure 1. Specification of the Samsung SAS TCG Enterprise SSC SEDs PM1653/PM1655 Series Cryptographic Boundary

2.2. Firmware and Cryptographic Boundary

The PM1653/PM1655 series use a single chip controller with a SAS interface on the system side and Samsung NAND flash internally. The following figure depicts the Module operational environment.

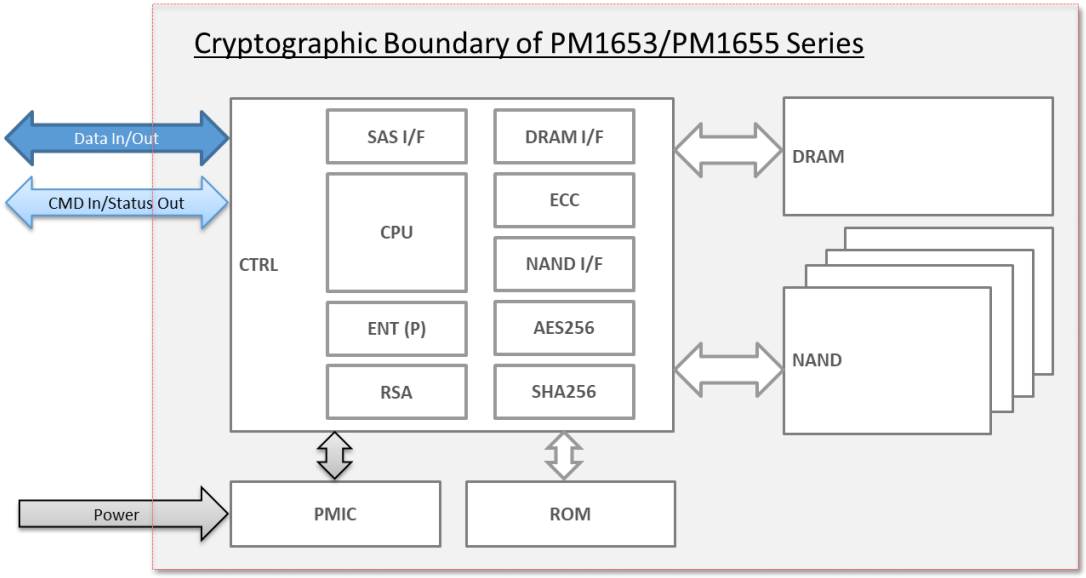

Figure 2. Block Diagram for Samsung SAS TCG Enterprise SSC SEDs PM1653 Series

2.3. Version Information

Model	Hardware Version	Firmware Version	Drive Capacity
PM1653	MZILG960HCHQ-00AC9	EXG0 EXG5 EXG6	960GB
	MZILG1T9HCJR-00AC9		1.9TB
	MZILG3T8HCLS-00AC9		3.8TB
	MZILG7T6HBLA-00AC9		7.6TB
	MZILG15THBLA-00AC9		15TB
	MZILG960HCHQ-00AD9	DXG0 DXG2	960GB
	MZILG1T9HCJR-00AD9		1.9TB
	MZILG3T8HCLS-00AD9		3.8TB
	MZILG7T6HBLA-00AD9		7.6TB
	MZILG3T8HCLS-00AG6	NA50	3.8TB
	MZILG3T8HCLS-00AG7	MS00	3.8TB
	MZILG3T8HCLS-00AVF	LEB0	3.8TB
	MZILG1T9HCJR-00AH9	3P00 3P01	1.9TB
	MZILG3T8HCLS-00AH9		3.8TB
	MZILG7T6HBLA-00AH9		7.6TB
	MZILG15THBLA-00AH9		15TB
PM1655	MZILG800HCHQ-00AC9	EZG0 EZG5 EZG6	800GB
	MZILG1T6HCJR-00AC9		1.6TB
	MZILG3T2HCLS-00AC9		3.2TB
	MZILG800HCHQ-00AD9	DZG0 DZG2	800GB
	MZILG1T6HCJR-00AD9		1.6TB
	MZILG3T2HCLS-00AD9		3.2TB

Table 3. Cryptographic Module Tested Configuration

2.4. Cryptographic Functionality

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
A1767[1]	AES / FIPS 197, SP 800-38E	XTS	256-bits	Data Encryption / Decryption
Vendor Affirmed	CKG[2]/ SP800-133 Rev 2	Section 4 Section 6.1 Section 6.3	N/A	Symmetric Cryptographic Key Generation
DRBG 2186	DRBG / SP 800-90A Rev. 1	CTR_DRBG (AES-256)	N/A	Deterministic Random Bit Generation
A1765	RSA / FIPS 186-4	PKCS PSS	3072-bits	Digital Signature Verification
A1766	SHS / FIPS 180-4	SHA-256	N/A	Message Digest
E43	ENT (P) / SP800-90B	N/A	N/A	ENT (P) provides a minimum of 256 bits of entropy for DRBG seed

Table 4. Approved Algorithms

2.4.2. Non-Approved Algorithm

Following algorithms are not intended to be used as a security function, and not used whatsoever to meet any FIPS 140-3 requirements. 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 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 (SHS Cert.# A1766)		Key Derivation

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

2.5. Approved Mode of Operation

The cryptographic module has only one mode of operation, which is the approved mode of operation. The operator is responsible for following the guidance outlined in section 12. The module shows the approved mode through validated version status by Show Status Service and in Table 8 via SCSI Inquiry command.

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

[2] *CKG is applied to generate the MEK in compliance with sections 4, 6.1 and 6.3 of SP800-133.*

3. Cryptographic module interfaces

Physical Port	Logical Interface Type	Data that Passes Over Port/Interface
SAS Connector	Data Input	plaintext data; signed data; authentication data
	Data Output	plaintext data;
	Control Input	commands input logically via an API (e.g. for the software and firmware components of the cryptographic module); signals input logically or physically via one or more physical ports (e.g. for the hardware components of the cryptographic module);
	Status Output	status information output logically via an API; signal outputs logically or physically via one or more physical ports;
	Power Input	Power input

Table 6. Ports and Interfaces

Note: The module does not implement the Control Output

4. Roles, services, and authentication

4.1. Role

The following table defines the roles, type of authentication, and associated authenticated data types supported by the cryptographic module.

Role	Service	Input	Output
Crypto Officer (CO)	Change the Password.	CO Password	Status
User	Set User Password	User Password	Status
CO and User	Lock/Unlock an LBA Range	LBA Range	Status
	Erase an LBA Range's Data	LBA Range	Status
Firmware Loader (FL)[3]	Update the firmware	Firmware Image	Status

Table 7. Roles, Service Commands, Input and Output

4.2. Approved service

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

Service	Description	Approved Security Functions	SSPs	Role	Type(s) of Access[4]				Indicator[5]
					E	W	G	Z	
Change the Password.	Change CO password	SHA-256	CO Password	CO	O	O		O	UID: AdminSP_SID_C_PIN / AdminSP_Admin1_C_PIN TCG Method: Set Result: TCG status code
Set User Password	Set User Password	SHA-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
Lock/Unlock an LBA Range	Block or allow read (decrypt) / write (encrypt) of user data.	AES-XTS	MEK	CO, User	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.	CTR_ DRBG (AES-256)	DRBG Internal State		O	O	O	O	UID: K_AES_256_GlobalRange_Key / K_AES_256_RangeNNNN_Key TCG Method: Erase Result: TCG status code
			MEK			O	O	O	
Update the firmware	Update the firmware	RSA	Firmware Verification Key	FL	O				WRITE BUFFER Command Result : Status Code

Table 8. Authenticated Services

[3] Firmware Loader role is classified as a Cryptographic Officer.

[4] It means that "Write" and "Zeroise" perform in each storage of SSPs that is described in Table 13. The (R)ead column, which is specified in NIST SP 800-140B, is not applicable to the module.

[5] The result of SCSI or TCG command is used as an indicator.

- The following table shows unauthenticated services. It is initially possible to use the services in following table without authentication. The operator can configure the setting that complied with Samsung SAS, TCG spec.

Service	Description	Approved Security Functions	SSPs	Role	Type(s) of Access[6]				Indicator[7]
					E	W	G	Z	
Show Status[8]	Show the module status - FIPS fail mode	N/A	N/A	N/A					INQUIRY Command Result : Status Code
Show Version[9]	Show module version	N/A	N/A						SECURITY PROTOCOL IN 00h, 02h, 02h, 01h Result: Status Code
Authentication	Authenticate the module	SHA-256	CO Password		O				UID: AdminSP_SID / AdminSP_Admin1 / LockingSP_Admin1~4 / LockingSP_User1~9 TCG Method: Authenticate Result: TCG status code
			User Password		O				
Get Random Number	Provide a random number generated by the CM.	CTR_ DRBG (AES-256)	DRBG Internal State		O		O		UID: ThisSP TCG Method: Random Result: TCG status code
IO Command[10]	Read/Write user data	AES-XTS	MEK		O				WRITE / READ Command Result : Status Code
Revert	Erase user data in all Range by changing the data	CTR_ DRBG (AES-256)	DRBG Internal State		O		O		UID: SPObj(AdminSP) TCG Method: Revert Result: TCG status code
			MEK			O	O	O	
Sanitize	Erase user data by changing the data encryption key.	CTR_ DRBG (AES-256)	DRBG Internal State		O	O	O	O	SANITIZE Command Result : Status Code
			MEK			O	O	O	

Table 9. Unauthenticated Services

[6] It means that “Write” and “Zeroise” perform in each storage of SSPs that is described in Table 13. The (R)ead column, which is specified in NIST SP 800-140B, is not applicable to the module.

[7] The module only supports approved services in an approved manner. The module uses implicit indicators through the result of the SCSI or TCG commands.

[8] If the module enters the FIPS Fail Mode, this command return fail.

[9] The cryptographic module shows the hardware version and firmware version through the ‘COMPLIANCE DESCRIPTOR HARDWARE VERSION’ and ‘COMPLIANCE DESCRIPTOR VERSION’ of FIPS 140 compliance descriptor Structure.

[10] Through Step3 to Step4 in the Section 12.1, the procedure handled by EraseMaster (CO) enforces to configure SICOC functionality which utilizes IO command from the beginning of module operational state.

4.3. Authentication

The module supports role-based authentication that requires authentication to assume for the authorization of each role.

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		
FL	RSA signature verification	Probability of $1/2^{128}$ in a single random attempt. Probability of $6000/2^{128}$ in multiple random attempts in a minute.

Table 10. Roles and Authentication

The CO and User role requires password-based authentication, where each byte can be any of 0x00 to 0xFF. Each password authentication failure holds the cryptographic module for 750ms. This restricts the maximum attempts for a one-minute to less than 80 attempts (60,000ms/750ms) no matter how large Trylimit[11] is set.

The FL role is implemented by RSA signature verification. The firmware signed by Samsung is authenticated by verifying the 3072-bit RSA signature which has 128 security strength in every power-on. Each signature verification attempt takes at least 10ms. This can be enforced with up to 6,000 attempts in a minute.

[11] Trylmit is maximum number of failed authentication attempts that are able to be made using password for each role.

5. Software/Firmware security

- The cryptographic module implements the 482 bytes per 4KB error detection code and SHA-256 hash verification for firmware integrity test.

- The firmware integrity test is performed every power on reset.

6. Operational environment

- The cryptographic module operates in a limited operational environment that is consist of the module's firmware. This 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.

- 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 the cryptographic module:

- The module consists of production-grade components enclosed in an aluminum alloy enclosure, which is opaque within the visible spectrum.
- Even if the top panel of the enclosure can be removed by unscrewing screws, the module is sealed with tamper-evident labels in accordance with FIPS 140-3 Level 2 physical security requirements so that tampering evidence can be easily detected when the top and bottom cases are detached.
- 2 tamper-evident labels are applied over both top and bottom cases of the module at the Samsung manufacturing. The tamper-evident labels cannot be removed and reapplied without remaining tamper evidence.

The following table summarizes the actions required by the Crypto 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 labels		Inspect the sealing labels for scratches, gouges, cuts and other signs of tampering. Remove from service if tampering found.

Table 11. Inspection/Testing of Physical Security Mechanisms

Figure 3. Module Seal Application Location

8. Non-invasive security

- Non-invasive security has not applicable for this cryptographic module.

9. Sensitive security parameter management

- Temporary SSPs are zeroised when power on reset.
- Firmware integrity temporary values are zeroised after the firmware integrity test is complete.
- The zeroisation is performed before overwriting to the target SSP with random value which is generated from the DRBG.
- SSP's are not exported outside the module.

Key / SSP Name/ Type	Strength	Security Function and Cert. Number	Generation	Import / Export	Establish ment	Storage	Zeroisation	Use & related keys
DRBG Internal State[12]	256-bit	CTR_ DRBG (AES-256) / DRBG 2186	SP 800-90A CTR_DRBG (AES-256)	N/A	N/A	N/A (HW IP internal)	Power on Reset	MEK
DRBG Seed	256-bit Nonce: 128-bit	CTR_ DRBG (AES-256) / DRBG 2186	ENT (P)	N/A	N/A	N/A (HW IP internal)	Power on Reset	MEK
DRBG Entropy Input String	256-bit	CTR_ DRBG (AES-256) / DRBG 2186	ENT (P)	N/A	N/A	N/A (HW IP internal)	Power on Reset	MEK
CO Password	Min. 64-bit	N/A	N/A	MD/EE	N/A	RAM	Power on Reset	N/A
User Password	Min. 64-bit	N/A	N/A	MD/EE	N/A	RAM	Power on Reset	N/A
Hashed CO Authentication Data	128-bit	SHA-256 / A1766	Hashed from Password as per SHA-256	N/A	N/A	Flash	Via "Change the Password" and Revert" service	N/A
Hashed User Authentication Data	128-bit	SHA-256 / A1766	Hashed from Password as per SHA-256	N/A	N/A	Flash	Via "Set User Password" and Revert" service	N/A
MEK	256-bit	CKG / AES-XTS / A1767	SP800-133Rev2/ SP 800-90A CTR_DRBG (AES-256)	N/A	N/A	Plain Text in RAM, Flash	Via "Lock an LBA Range", "Erase an LBA Range's Data", "Revert" and "Sanitize" service	N/A
Firmware Verification Key	128-bit	RSA / A1765	N/A	Entered during manufact uring	N/A	HW SFR	Right after FW load test	Firmware load test
						Flash	N/A	

Table 12. SSPs

[12] The values of V and Key are the critical value of the internal state

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
Cert #E43 ENT (P)	- 0.2262 entropy per bit - Minimum of 256 bits of entropy for DRBG seed (total seed length of 384 bits).	Provides entropy input and Nonce to construct Entropy source seed for CTR_DRBG The number of bits input/output to the derivation function are n_{in}=3072 and n_{out}=384.

Table 13. Non-Deterministic Random Number Generation Specification

10. Self-tests

While executing the following self-tests, all data output is inhibited until the self-test is completed. To execute the pre-operational tests on-demand, the operator may run the power-cycle of the module. If the self-test fails, the module enters an error state. All data output is inhibited during self-tests or in an error state.

10.1. Pre-operational Test

- Firmware integrity test
  - SHA-256 hash-based verification is performed at power-on.
  - 482-byte error detection code is performed at power-on.

10.2. Conditional Test

- Cryptographic Algorithm Tests
  - The cryptographic algorithm test can be executed on-demand during the pre-operational test at power-on.

Algorithm	Type	Description
SHS	KAT	SHA-256 hash digest
DRBG	KATs	SP 800-90A Section 11.3 Health Tests of CTR_DRBG (AES-256)
AES	KAT	AES-256 XTS mode encryption and decryption
SHS	KAT	SHA-256 hash digest
RSA	KAT	RSA-3072 signature verification

Table 14. Self-tests

- Firmware load test
  - Firmware load test is performed using RSA-3072 with SHA-256.
  - The firmware load test can be executed on-demand by executing the Update the firmware service.

- TRNG Health tests

  The cryptographic module has performed the below 2 types of tests and each test includes the Repetition Count Test and Adaptive Proportion Test described in SP800-90B.
  - Start-up test is performed for Entropy Source every power on reset.
  - Continuous test is performed for Entropy Source while the module is operating.

11. Life-cycle assurance

The cryptographic module can operate in approved mode once shipped from the vendor's manufacturing site. The followings describe the security rules for secure installation and operation which the cryptographic module and Crypto Officer shall be enforced under FIPS 140-3 security level 2 compliant manner:

11.1. C.Secure Installation

- [Step1] User should examine the tamper evidence.
  - Inspect the entire perimeter for cracks, gouges, lack of 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.
- [Step2] Identify the firmware version in the device.
  - Confirm that the firmware version is equivalent to the version(s) listed in this document via SCSI Inquiry command.
- [Step3] Take the drive's ownership.
  - Change the PIN of SID/EraseMaster to new PIN.
  - Run Erase Method on each Band.

  Note: If required to use the additional Band in Locking SP, new PINs must be set after setting a Band by the Crypto Officer.
  - Configure the Band(s) by setting ReadLockEnabled and WriteLockEnabled columns to True.
  - Don't change LockOnReset column in Locking Table.
- [Step4] Power cycle the module.
- [Step5] Periodically examine the tamper evidence.
  - If there is any sign of tampering, stop using the product to avoid a potential security hazard or information leakage.

11.2. Operational Description of Module

- The cryptographic module shall maintain logical separation of data input, data output, control input, control 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 role-based authentication for security relevant services.
- The cryptographic module shall enforce a limited operational environment by the secure firmware load test using RSA PSS-3072 with SHA-256.
- The cryptographic module shall provide a production-grade, opaque, and tamper-evident cryptographic boundary.
- The cryptographic module enters the error state upon failure of Self-tests. All 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 a sense key (0x4) via the status output. Cryptographic services and data output are explicitly inhibited when in the error state. The module enforces to enter the power on reset if DRBG or NDRBG health test fails.
- The cryptographic module satisfies the requirements of FIPS 140-3 IG C.I (i.e. key_1 ≠ key_2)
- The RSA signature verification satisfies the requirements of FIPS 140-3 IG C.F
- The module generates at a minimum 256 bits of entropy for use in key generation.
- Bypass capability is not applicable to the cryptographic module.
- Critical functions are not applicable to the cryptographic module.
- The module generates symmetric keys which are unmodified outputs from the DRBG.

12. Mitigation of other attacks

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

Other Attacks	Mitigation Mechanism	Specific Limitations
N/A	N/A	N/A

Table 15. Mitigation of Other Attacks