

## Samsung NVMe TCG Opal SSC SEDs PM1733a/PM1735a Series FIPS 140-3 Non-Proprietary Security Policy

**Document Version: 1.0** 

 H/W Version: MZWLR1T6HCJR-00AD9, MZWLR1T9HCJR-00AC9, MZWLR1T9HCJR-00AD9, MZWLR3T2HCLS-00AD9, MZWLR3T8HCLS-00AC9, MZWLR3T8HCLS-00AD9, MZWLR3T8HCLS-00AV8, MZWLR3T8HCLS-00AG6, MZWLR15THBLA-00AG6, MZWLR6T4HBLA-00AD9, MZWLR7T6HBLA-00AC9, MZWLR7T6HBLA-00AD9, MZWLR12THBLA-00AD9, MZWLR15THBLA-00AC9, MZWLR30THBLA-00AC9, MZWLR15THBLA-00AD9, MZWLR30THBLA-00AD9
 F/W Version: MPP90D3Q, MPP92E5Q, MPP92D3Q, MPP93D3Q, MPP95E5Q, NA50

### **Revision History**

Version	Changes
1.0	Initial version

### **Table of Contents**

<u>1.</u>	GENERAL	4
	1.1. SCOPE	4
	1.2. ACRONYMS	4
<u>2.</u>	CRYPTOGRAPHIC MODULE SPECIFICATION	5
	2.1. Cryptographic Boundary	5
	2.2. VERSION INFORMATION	6
	2.3. CRYPTOGRAPHIC FUNCTIONALITY	7
	2.3.1. Approved Algorithm	7
	2.3.2. NON-APPROVED ALGORITHM	7
	2.4. APPROVED MODE OF OPERATION	7
<u>3.</u>	CRYPTOGRAPHIC MODULE INTERFACES	8
<u>4.</u>	ROLES, SERVICES, AND AUTHENTICATION	9
	4.1. ROLE	9
	4.2. APPROVED SERVICE	9
	4.3. AUTHENTICATION	10
<u>5.</u>	SOFTWARE/FIRMWARE SECURITY	11
<u>6.</u>	OPERATIONAL ENVIRONMENT	12
<u>7.</u>	PHYSICAL SECURITY	13
<u>8.</u>	NON-INVASIVE SECURITY	14
<u>9.</u>	SENSITIVE SECURITY PARAMETER MANAGEMENT	15
<u>10.</u>	SELF-TESTS	17
	10.1. PRE-OPERATIONAL TEST	17
	<b>10.2.</b> CONDITIONAL TEST	17
	10.3. Error States	17
<u>11.</u>	LIFE-CYCLE ASSURANCE	18
	11.1. Secure Installation	18
	11.2. OPERATIONAL DESCRIPTION OF MODULE	18
<u>12.</u>	MITIGATION OF OTHER ATTACKS	19

### 1. General

### 1.1. Scope

This document specifies the security policy for Samsung Electronics Co., Ltd. ("Samsung") **SSD NVMe TCG Opal SSC SEDs PM1733a/PM1735a 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 of a hardware module, supporting TCG Opal 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.

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					
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					
КАТ	Known Answer Test					
LBA	Logical Block Address					
MD/EE	Manual Distribution/Electronic Entry					
MEK	Media Encryption Key					
NAND	NAND Flash Memory					
NAND I/F	NAND Flash Interface					
NVMe	Non-Volatile Memory Host Controller Interface Specification					
ROM	Read-only Memory					
SFR	Special Function Register					

#### Table 2. Acronyms

### 2. Cryptographic Module Specification

### 2.1. Cryptographic Boundary

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 cryptographic boundary of the module.



Figure 1. Specification of the Samsung SSD NVMe TCG Opal SSC SEDs PM1733a/PM1735a Series Cryptographic Boundary

The firmware utilizes a single chip controller with an NVMe interface on the system side as well as Samsung NAND flash. The following figure depicts the module operational environment. The firmware 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. Any firmware loaded into 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 NVMe TCG Opal SSC SEDs PM1733a/PM1735a Series

### 2.2. Version information

Model	Hardware Version	Drive Capacity	
	MZWLR3T8HCLS-00AG6		3.84TB
	MZWLR3T8HCLS-00AV8	NA50	3.84TB
	MZWLR15THBLA-00AG6		15.36TB
	MZWLR1T9HCJR-00AC9		1.92TB
	MZWLR3T8HCLS-00AC9		3.84TB
	MZWLR7T6HBLA-00AC9 MPP92E5Q,	MPP92E5Q,	7.68TB
PM1733a	MZWLR15THBLA-00AC9	IVIFF 95L5Q	15.36TB
	MZWLR30THBLA-00AC9		30.72TB
	MZWLR30THBLA-00AD9	MPP93D3Q	30.72TB
	MZWLR1T9HCJR-00AD9		1.92TB
	MZWLR3T8HCLS-00AD9		3.84TB
	MZWLR7T6HBLA-00AD9		7.68TB
	MZWLR15THBLA-00AD9	MPP90D3Q,	15.36TB
	MZWLR1T6HCJR-00AD9 MPP92D3		1.6TB
	MZWLR3T2HCLS-00AD9		3.2TB
PIVI1/35d	MZWLR6T4HBLA-00AD9	]	6.4TB
	MZWLR12THBLA-00AD9		12.8TB

Table 3. Cryptographic Module Tested Configuration

### 2.3. Cryptographic Functionality

#### 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
C1271 <sup>1</sup>	AES /	XTS	256 bits	Data Encryption / Decryption
	FIPS 197, SP 800-38E			(only used for storage)
A1720	DRBG /	Hash_DRBG	N/A	Deterministic Random Bit
	SP 800-90A Rev. 1	(SHA-256)		Generation
A940	RSA / FIPS 186-4	PSS SigVer	3072 bits	Digital Signature Verification
		(SHA-256)		
C1272	SHS / FIPS 180-4	SHA-256	N/A	Message Digest
Vendor	CKG / SP 800-133 Rev2	Section 4 and	N/A	Cryptographic Key Generation
Affirmed		Section 6.1		(Symmetric Keys)
N/A	ENT (P) / SP800-90B	N/A	N/A	Non-deterministic Random
				Number Generator
				(only used for generating seed
				materials for the Approved
				DRBG)
				ENT (P) provides a minimum
				of 256 bits of entropy for
				DRBG seed

Table 4. Approved Algorithms

#### 2.3.2. 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 removal of obfuscation during ROM initialized. (IG 2.4.A Scenario #2)	Firmware Removal of obfuscation
AES-CCM / FIPS 197, SP 800-38C	No Security Claimed; Non-approved	Key obfuscation and Removal of obfuscation
PBKDF2	algorithms here are only used for	Non-SSP Derivation
HMAC / SHA-256 (SHS Cert.# C1272)	obfuscation the CSP. (IG 2.4.A Scenario #1)	Non-SSP Derivation

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 has a single approved mode of operation and does not have a non-approved mode of operation. The cryptographic module shows the approved mode through validated version status by Show Status Service in Table 9 via NVM express Identify Controller command.

The non-approved algorithms are allowed in the approved mode of operation with no security claimed in the module.

<sup>&</sup>lt;sup>1</sup> AES-ECB is the pre-requisite for AES-XTS; AES-ECB alone is NOT supported by the cryptographic module in Approved Mode.

## 3. Cryptographic Module Interfaces

Physical Port	Logical Interface Type	Data that Passes Over Port/Interface
	Data Input	plaintext data; signed data; authentication data
	Data Output	plaintext data;
NVMe Connector	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, and associated services supported by the each role:

Role	Service	Input	Output
Cryptographic Officer(CO)	Lock/Unlock an LBA Range	LBA Range	Status
and User	Erase an LBA Range's Data	LBA Range	Status
СО	Change the Password.	CO Password	Status
User	Set User Password	User Password	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	SSPs	Role	т	Type(s) of Access <sup>2</sup>			Indicator <sup>3</sup>		
		Functions			E	w	G	z			
Change the	Change CO		CO Password	60	0	0		0	UID: AdminSP_SID_C_PIN / AdminSP_Admin1_C_PIN		
Password. pass	password	3HA-230	Hashed CO Authentication Data			0	0	0	0		TCG Method: Set Result: TCG status code
Set User Password	Set User Password	SHA-256	User Password	User	0	0		0	UID: LockingSP_Admin1~4_C_PIN /		
			Hashed User Authentication Data		о	0	0		TCG Method: Set Result: TCG status code		
Lock/Unlock an LBA Range⁴	Block or allow read (decrypt) / write (encrypt) of user data.	N/A	МЕК			0		0	UID: Locking_GlobalRange / Locking_RangeNNNN TCG Method: Set Result: TCG status code		
Erase an LBA Range's Data	Erase user data by	Hash_ DRBG (SHA-256)	DRBG Internal State	CO, User	0	0	0	0	UID: K_AES_256_GlobalRange_Key /		
	changing the data encryption key.		МЕК			0	0	0	K_AES_256_RangeNNNN_Key TCG Method: GenKey Result: TCG status code		

**Table 8. Authenticated Services** 

<sup>&</sup>lt;sup>2</sup> 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.

<sup>&</sup>lt;sup>3</sup> The result of NVMe or TCG command is used as an indicator.

<sup>&</sup>lt;sup>4</sup> The CO can grant Users the authority to utilize this service via updating the "Locking SP ACE Table", in accordance with the TCG specification (included in the Lock/Unlock an LBA Range service). Initially, only the CO can perform this service. This module provides an indicator which shows when Self-Initiated Cryptographic Output Capability is activated or inactivated. The operator can check whether the target range is locked or unlocked through the 'getLockingTable' query per the TCG specification.

- Following table shows unauthenticated services. It is initially possible to use the services in following table without authentication. The operator can be configured setting that complied with NVM, TCG spec.

Comine	Description	Approved	CCD-	Dele	Type(s)			of	In diasta 15
Service	Description	Functions	5585	Role	E	W	G	z	Indicator
Show Status <sup>6</sup>	Show approved version status of the module / FIPS fail mode	N/A	N/A						NVM Command: Identify Controller command Result : Status Code
	Authenticate to the		CO Password		0			0	UID: AdminSP_SID / AdminSP_Admin1 / LockingSP_Admin1~4 /
Authentication	module	SHA-256	User Password		0			0	LockingSP_User1~9 TCG Method: Authenticate Result: TCG status code
Get Random Number	Provide a random number generated by the CM.	Hash_ DRBG (SHA-256)	DRBG Internal State		о		0		UID: ThisSP TCG Method: Random Result: TCG status code
IO Command <sup>7</sup>	Read/Write user data	AES-XTS	МЕК		0				NVM Command: Write / Read Result : Status Code
			DRBG Internal State	N/A	0		0		
	Erase user data in all		MEK			0	0	0	
Revert	Range by changing the data encryption key and clearing the	Hash_ DRBG (SHA-256)	Hashed CO Authentication Data					0	UID: SPObj(AdminSP) TCG Method: Revert Result: TCG status code
	authentication data		Hashed User Authentication Data					0	
FormatNVM /	Erase user data by	Hash_ DRBG	DRBG Internal State		0	0	0	0	Admin Command: Format NVM / Sanitize /
DeleteNS	encryption key.	(SHA-256)	MEK			0	0	0	Namespace Management Result : Status Code
Update the firmware <sup>8</sup>	Update the firmware	RSA	Firmware Verification Key		0			0	Admin Command: Firmware Commit Result : Status Code
Perform Self-tests	Power cycling the module to perform self-tests	N/A	N/A						N/A

Table 9. Unauthenticated Services

#### 4.3. Authentication

This module provides the role-based authentication. The authentication mechanism allows a minimum 8-byte length or longer (up to 32-byte) Password, where each byte can be any of 0x00 to 0xFF, for every Cryptographic Officer and User role supported by the module, which means a single random attempt can succeed with the probability of  $1/2^{64}$  or lower. Each Password authentication attempt takes at least 750ms. It means, the number of attempts possible in a minute period is maximum 80 attempts (60000ms/750ms).

Role	Authentication Method	Authentication Strength			
CO	Password	Probability of 1/2 <sup>64</sup> in a single random attempt			
User	(Min: 8 bytes, Max: 32 bytes)	Probability of 80/2 <sup>64</sup> in multiple random attempts in a minute			
Table 10 Balas and Authoritisation					

Table 10. Roles and Authentication

<sup>&</sup>lt;sup>5</sup> The module only supports approved services in an approved manner. The module uses implicit indicators through the result of the NVMe or TCG commands.

<sup>&</sup>lt;sup>6</sup> The cryptographic module shows the hardware version and firmware version through the 'Model Number (MN)' and 'Firmware Revision (FR)' of Identify Controller Data Structure. If the module enters the FIPS Fail Mode, this service indicates "ERRORMOD" in Firmware Revision (FR).

<sup>&</sup>lt;sup>7</sup> The I/O command itself is the approved service where Self-Initiated Cryptographic Output Capability occurs, while the unlock request (via Lock/Unlock an LBA range" service) is the authorized enablement of this capability.

<sup>&</sup>lt;sup>8</sup> This service is exempted from being authenticated by exception clause (c) of IG 4.1.A.

### 5. Software/Firmware Security

- The cryptographic module employs the 428-byte parity for firmware integrity test.
- The firmware integrity test is performed when 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 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.
- 2 tamper-evident labels are applied over both top and bottom cases of the module at the factory. The tamper-evident labels are not removed and reapplied without tamper evidence.
- The tamper-evident labels are 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 Labels	As often as reasible	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. Tamper Evident Label Placement



Figure 4. Example of Signs of Tamper

## 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	Establis hment	Storage	Zeroisation	Use & Related Keys
DRBG Internal State <sup>9</sup>	256-bit	A1720 Hash_ DRBG (SHA-256)	SP 800-90A HASH_DRBG (SHA-256)	N/A	N/A	Plaintext in RAM	Power on Reset	MEK
DRBG Seed	256-bit	A1720 Hash_ DRBG (SHA-256)	ENT (P)	N/A	N/A	Plaintext in RAM	Power on Reset	MEK
DRBG Entropy Input String	256-bit	A1720 Hash_ DRBG (SHA-256)	ENT (P)	N/A	N/A	Plaintext in RAM	Power on Reset	MEK
CO Password	Min. 64- bit	N/A	N/A	MD/EE	N/A	Plaintext in RAM	Via "Authentication " service	N/A
User Password	Min. 64- bit	N/A	N/A	MD/EE	N/A	Plaintext in RAM	Via "Authentication " service	N/A
Hashed CO Authenticati on Data	128-bit	C1272 SHA-256	Hashed from Password as per SHA-256	N/A	N/A	Plaintext in Flash	Via "Change the Password" and Revert" service	N/A
Hashed User Authenticati on Data	128-bit	C1272 SHA-256	Hashed from Password as per SHA-256	N/A	N/A	Plaintext in Flash	Via "Set User Password" and Revert" service	N/A
МЕК	256-bit	C1271 AES-XTS	SP 800-90A HASH_DRBG (SHA-256)	N/A	N/A	Plain Text in RAM, Flash	Via "Unlock an LBA Range", "Erase an LBA Range's Data", "Revert" and "FormatNVM / Sanitize / DeleteNS" service	N/A
Firmware Verification Key	128-bit	A940 RSA	N/A	Entered during manufacturi ng	N/A	Plaintext in Hardware SFR Plaintext in Flash	Right after FW load test N/A	Firmwa re load test

Table 12. SSPs

<sup>&</sup>lt;sup>9</sup> The values of V and C are the "secret values" 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
ENT (P)	<ul> <li>- 0.5 entropy per bit</li> <li>- Minimum of 256 bits of entropy for DRBG seed</li> <li>(total seed size of 512 bits).</li> </ul>	Entropy source for Hash_DRBG

Table 13. Non-Deterministic Random Number Generation Specification

### 10. Self-Tests

While executing the following self-tests, all data output is inhibited until self-test completion. To execute the preoperational tests on-demand, the operator may 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.

#### 10.1. Pre-operational Test

- Firmware integrity check
  - Firmware integrity check is performed by using 428-byte parity at power-on.

#### 10.2. Conditional Test

Cryptographic Algorithm Tests

Algorithm	Туре	Description		
DRBG	Cryptographic algorithm self-test	KATs for Hash_DRBG (SHA-256) described in SP 800-90A Section 11.3.1, 11.3.2, 11.3.3, 11.3.4 KAT performed with 512-bit entropy input		
AES-XTS	Cryptographic algorithm self-test	Encrypt and Decrypt KAT performed with 512-bit key size		
SHA	Cryptographic algorithm self-test	Hash Digest KAT performed with 256-bit message size		
RSA	Cryptographic algorithm self-test	Verify KAT performed with 3072 Modulus (3072-bit key size) and SHA-256.		
RSA	Firmware load test	Perform using RSA-3072 with SHA-256 when new firmware is downloaded.		
ENT (P)	Cryptographic algorithm self-test	<ul> <li>Perform the below 2 types of tests and each test includes the Repetition Count test and Adaptive Proportion test described in SP800-90B.</li> <li>Start-up test is performed for Entropy Source after power on reset.</li> <li>Continuous test is performed for Entropy Source while the module is operating</li> </ul>		

Table 14. Self-tests

### 10.3. Error States

Name	Description	Conditions	Recovery Method	Indicator
Error state in Boot	The module does not provide any crypto operation.	Integrity test or SP 800-90B start-up failure during boot	Power cycle	Hang state. No action
Error State		Any other self-test failure		If the module enters the FIPS Fail Mode, Show Status service indicates "ERRORMOD" in Firmware Revision (FR).

Table 15. Error States

### 11. Life-Cycle Assurance

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

- The cryptographic module operates always in Approved Mode once shipped from the vendor's manufacturing site.
- The steps necessary 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

- [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 NVM express Identify Controller command.
- [Step3] 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.

- [Step4] 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 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 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 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 firmware integrity checks 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.  $key_1 \neq key_2$ ).
- The module generates at a minimum 256 bits of entropy for use in key generation.
- Bypass capability is not applicable to the cryptographic module.
- Critical functions are not applicable to the cryptographic module.
- 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.

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

Table 16. Mitigation of Other Attacks