Samsung NVMe TCG Opal SSC SEDs BM1733a Series

FIPS 140-3 Non-Proprietary Security Policy

Document Version: 1.0

H/W Version: **MZEM515THALC-00AMV**

F/W Version: **MPOA3A5Q**

Revision History

Version	Change
1.0	Initial Version

Table of Contents

1. General

1.1. Scope

This document specifies the security policy for Samsung Electronics Co., Ltd. ("Samsung") **NVMe TCG Opal SSC SEDs BM1733a Series**, herein after referred to as a "cryptographic module" or "module", SSD (Solid State Drive), satisfies all applicable FIPS 140-3 Security Level 1 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 HW 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	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 Correcting Code
KAT	Known Answer Test
LBA	Logical Block Address
MEK	Media Encryption Key
MSID	Manufactured 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. Cryptographic Boundary

The following photograph shows the cryptographic module's top and bottom views. The multiple-chip standalone cryptographic module consists of hardware and firmware components specified version in the Table 3 that are all enclosed in two aluminum alloy cases, which serve as the cryptographic boundary of the module.

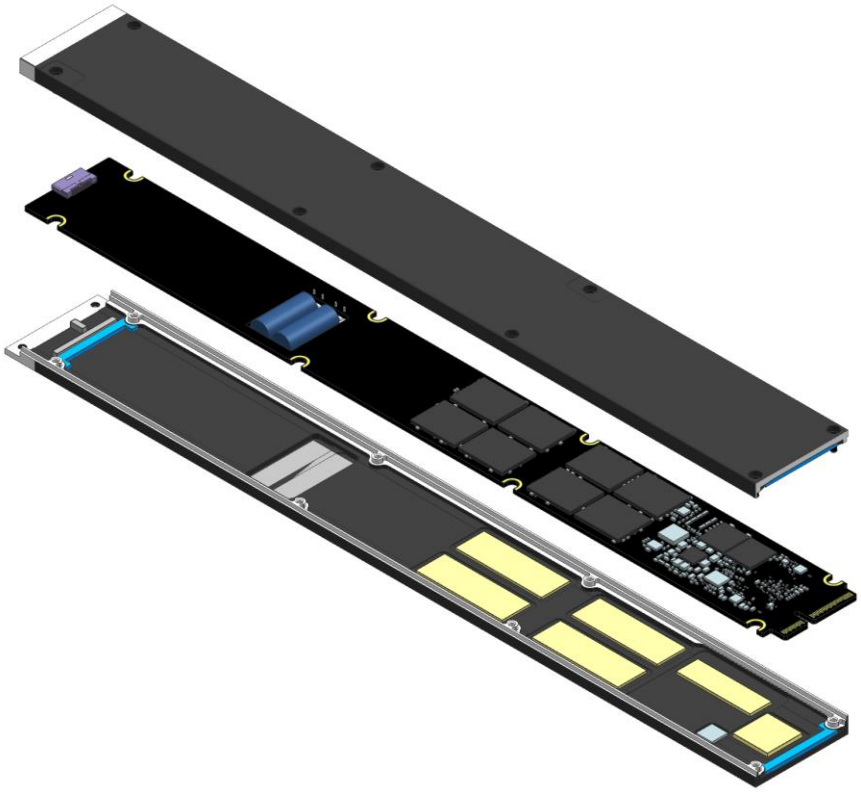

Figure 1. Specification of the Samsung SSD NVMe TCG Opal SSC SEDs BM1733a Series Cryptographic Boundary

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.

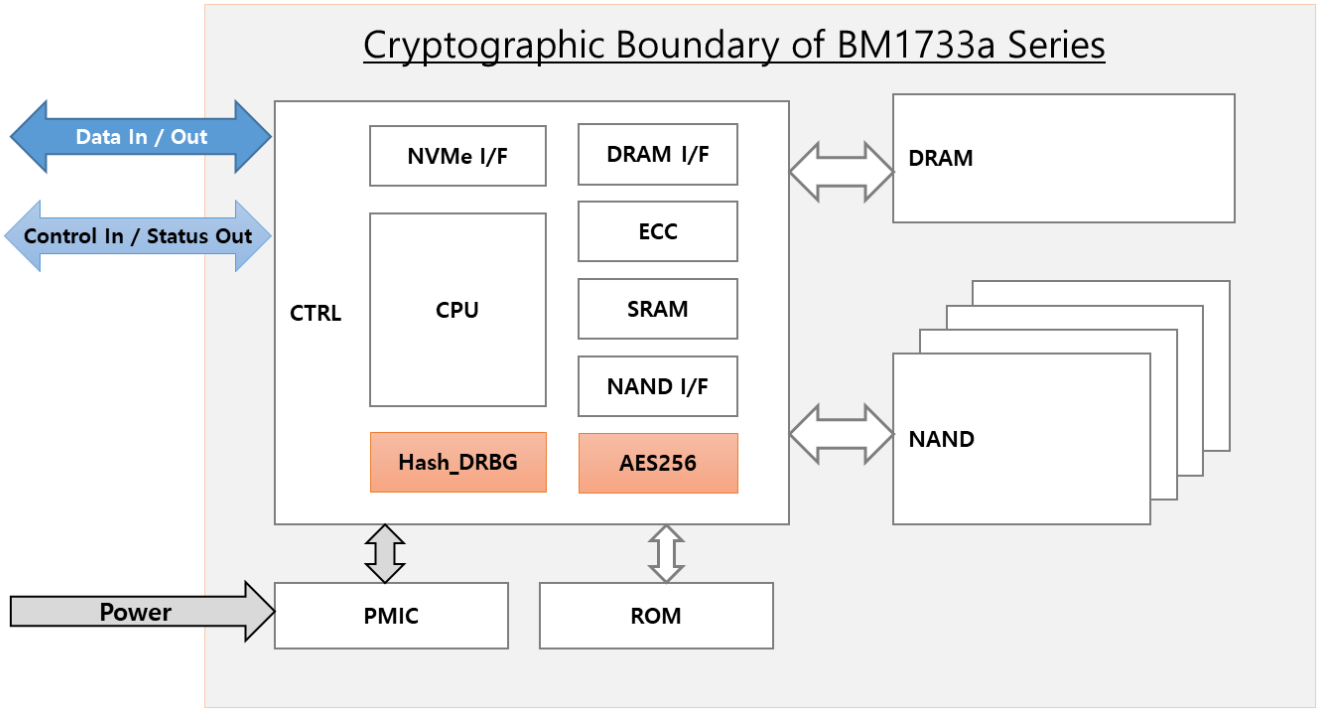

Figure 2. Block Diagram for Samsung SSD NVMe TCG Opal SSC SEDs BM1733a Series

2.2. Version information

Model	Hardware Version	Firmware Version	Drive Capacity
BM1733a	MZEM515THALC-00AMV	MPOA3A5Q	15.36TB

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[1]	AES / FIPS 197, SP 800-38E	XTS,	256 bits	Data Encryption / Decryption
A1720	DRBG / SP 800-90A Rev. 1	Hash_ DRBG (SHA-256)	N/A	Deterministic Random Bit Generation
A940	RSA / FIPS 186-4	PSS SigVer (SHA-256)	3072 bits	Digital Signature Verification
C1272	SHS / FIPS 180-4	SHA-256	N/A	Message Digest
Vendor Affirmed	CKG / SP 800-133 rev2	Section 4 and Section 6.1	N/A	Cryptographic Key Generation (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)

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 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.# C1272)		Key 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 8 via NVM express Identify Controller command.

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

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

3. Cryptographic module interfaces

Physical port	Logical interface Type	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;
	Power Input	Power input
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)	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
	Perform Self-Tests	N/A	N/A
Maintenance[2]	Diagnostics	N/A	N/A

Table 7. Roles, Service Commands, Input and Output

4.2. Service

4.2.1. Approved Services

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

Service	Description	Approved Security Functions	SSPs	Roles	Type(s) of Access[3]				Indicator[4]
					E	W	G	Z	
Show Status[5]	Show approved version status of the module / FIPS fail mode	N/A	N/A	CO					NVM Command: Identify Controller command Result : Status Code
Lock/Unlock an LBA Range	Block or allow read (decrypt) / write (encrypt) of user data.	AES-XTS	MEK		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 (SHA-256)	DRBG Internal State		O		O		UID: K_AES_256_GlobalRange_Key / K_AES_256_RangeNNNN_Key TCG Method: GenKey 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)	DRBG Internal State		O		O		UID: ThisSP TCG Method: Random Result: TCG status code
			DRBG Seed		O		O		
			DRBG Entropy		O		O		

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

[3] It means that "Write" and "Zeroise" perform in each storage of SSPs that is described in Table 10. The (R)ead column, which is specified in NIST SP 800-140B, is not applicable to the module.

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

[5] 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).

			Input String						
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)	DRBG Internal State		O		O		Admin Command: Format NVM / Sanitize / Namespace Management Result : Status Code
			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 (SHA-256)	DRBG Internal State		O		O		UID: SPObj(AdminSP) TCG Method: Revert Result: TCG status code
Perform Self-tests	Power cycling the module to perform self-tests	N/A	N/A					O	N/A
Diagnostics	Perform Maintenance	N/A	N/A	Maintenance					N/A

Table 8. Approved Services

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.
- The masked ROM embedded in this module is guaranteed for a minimum 10 years after manufactured date under effective lifetime.
- If this cryptographic module is no longer deployed, secure sanitization can be fulfilled by carrying out the following NVM Express commands; FormatNVM, Sanitize

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.

- 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 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 a maintenance role. The maintenance access interface is defined as the JTAG port. In compliance with maintenance role requirements, the operator shall perform the following procedures.

- The Cryptographic module must be zeroised by operator via Revert service when entering or exiting the maintenance role.
- The operator should perform the power-on reset the module after exiting the maintenance role. Operator should confirm the original Firmware revision of the module has not changed.
- The operator should inspect the JTAG port as often as feasible since the operator is responsible to manage for JTAG port of the module.

8. Non-invasive security

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

9. Sensitive security parameter management

- Temporary SSPs, stored in RAM are zeroised when power on reset.
- Firmware integrity temporary values are zeroised after the firmware integrity test is complete
- The zeroisation is performed overwriting the target SSP with random value which is creating through the DRBG.
- SSPs are not exported to outside.

Key/SSP Name/ Type	Strength	Security Function and Cert. Number	Generation	Import /Export	Establish ment	Storage	Zeroisation	Use & related keys
DRBG Internal State[6]	256-bit	A1720 Hash_ DRBG (SHA-256)	SP 800-90A HASH_DRBG (SHA-256)	N/A	N/A	RAM	Power on Reset	MEK
DRBG Seed	256-bit	A1720 Hash_ DRBG (SHA-256)	ENT (P)	N/A	N/A	RAM	Power on Reset	MEK
DRBG Entropy Input String	256-bit	A1720 Hash_ DRBG (SHA-256)	ENT (P)	N/A	N/A	RAM	Power on Reset	MEK
MEK	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-bits	A940 RSA	N/A	Entered during manufact uring	N/A	HW SFR	Right after FW load test	Firmware Load Test
						Flash	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 - Minimum of 256 bits of entropy for DRBG seed (total seed size of 512 bits).	Entropy source for Hash_DRBG

Table 11. Non-Deterministic Random Number Generation Specification

[6] *The values of V and C are the “secret values” of the internal state*

10. Self-tests

While executing the following self-tests, all data output is inhibited until self-test completion. To execute the pre-operational 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

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

10.2. Conditional test

- Cryptographic Algorithm Tests

Algorithm	Description
Hash_DRBG	KATs for Hash_DRBG (SHA-256) described in SP 800-90A Section 11.3.1, 11.3.2, 11.3.3, 11.3.4
AES-XTS	AES256 XTS mode Encrypt and Decrypt KAT performed
SHA-256	Hash Digest KAT performed (SHA-256)
RSA, 2048 modulus with SHA-256	Signature verification KAT are performed (RSA 2048 PSS with SHA-256)

Table 12. Self-tests

- Firmware load test
  - Firmware load test is performed using RSA-3072 with SHA-256 when new FW is downloaded.

- Health test

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 after power on reset.
- Continuous test is performed for Entropy Source while the module is operating

11. Life-cycle assurance

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 NVM express Identify Controller command.

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 FW 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 ≠ 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.
- To enter or exit the maintenance role, the operator shall perform zeroisation via Revert Service, and should perform power-on reset the module after exiting the maintenance role. Operator should confirm the firmware version of the module specified in the Table 3 has not been changed.
- If you require the TCG Opal SSC SED Product Manual, kindly contact the Samsung security certification team via email at security_cert@samsung.com.

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 13. Mitigation of Other Attacks