FIPS 140-2 Level 2 Security Policy

For

SAMSUNG SSD PM810 SED FIPS 140 Module

Document Version 0.6

Acronyms....3
1 Module Description....4
2 Cryptographic Boundary....4
3 Ports and Interfaces....5
4 Roles, Services and Authentication....5
5 Security Functions....7
6 Key Management....7
7 Self Tests....7
8 Physical Security....8
9 Secure Operation....9

Acronyms

ATA	Advanced Technology Attachment
ISV	Independent Software Vendor
SATA	Serial Advanced Technology Attachment
SSC	Security Subsystem Class
SSD	Solid-State Drive
TCG	Trusted Computing Group

1 Module Description

The SAMSUNG SSD PM810 SED FIPS 140 Module provides high-performance AES-256 cryptographic encryption and decryption of the data stored in NAND Flash via the SATA interface. The PM810 encryption/decryption creates no degradation in performance compared to a non-encrypted SSD. The PM810 supports both the ATA Security Feature Set and TCG Opal SSC. Security Functionalities include user authentication for access control via ISV TCG Opal support, user data encryption for data protection, and near-instantaneous sanitization of user drive data via cryptographic erase for repurposing or disposal.

Module Name and Hardware Version	**Firmware versions**	**Drive Capacity**
SAMSUNG SSD PM810 SED FIPS 140 Module MZ5PA128HMCD-010D9	AXM96D1Q	128GB
SAMSUNG SSD PM810 SED FIPS 140 Module MZ5PA256HMDR-010D9	AXM96D1Q	256GB

2 Cryptographic Boundary

The Module consists of hardware and firmware components that are all enclosed in two plastic cases, which serve as the cryptographic boundary of the Module. The top and bottom cases are assembled by screws and the tamper-evident labels are applied for the detection of any opening of the cases. No internal component can be seen within the visible spectrum through the opaque enclosure.

3 Ports and Interfaces

The Module includes the following physical ports and logical interfaces.

Port Name	Count	Interface(s) (Data Input, Data Output, Control Input, Status Output)
SATA Port	**1**	Data Input, Data Output, Control Input, Status Output
Power Connector	**1**	Power Input

4 Roles, Services and Authentication

Role	Authentication Mechanism
User	Password (Min: 6bytes, Max:32bytes). The user authenticates using passwords of at least 6 bytes length. The probability of false acceptance is therefore significantly less than one in 1,000,000. Reboot is performed after five unsuccessful authentication attempts. The reboot time is at least 3 seconds; therefore, the user can only make 100 or less consecutive attempts in a minute. Therefore, the probability of randomly guessing authentication data in 60 seconds is less than 1 in 100,000.
Crypto Officer	Password (Min: 6bytes, Max:32bytes). The Crypto Officer authenticates using passwords of at least 6 bytes length. The probability of false acceptance is therefore significantly less than one in 1,000,000. Reboot is performed after five unsuccessful authentication attempts. The reboot time is at least 3 seconds; therefore, the Crypto Officer can only make 100 or less consecutive attempts in a minute. Therefore, the probability of randomly guessing authentication data in 60 seconds is less than 1 in 100,000.

The Module provides the following services to the operators:

Service	**Role**	**Access to Cryptographic Keys and CSPs** **R- read; W – write or generate; E-execute**
Take Ownership	Crypto Officer	PIN(W/E), KEK(R/W)
Unlock the user data	Crypto Officer User	PIN(R/E), MEK(R), KEK(R/E)
Set PIN	Crypto Officer User	PIN(W/E), KEK(R/W)
Crypto Erase	Crypto Officer	PIN(R/W/E), MEK(W), KEK(W)
Disable Locking	Crypto Officer	PIN(R/W/E), KEK(R/W)
Change Data Access Role	Crypto Officer	PIN(R/E), KEK(R/W)
Enable Locking	Crypto Officer	PIN(R/E), KEK(R/W)
User Data Read/Write	Crypto Officer User	MEK(E)
Installation of the Module	Crypto Officer	PIN(W), KEK (R,W)
Run self-test	Crypto Officer User	N/A
Show status	Crypto Officer User	N/A
Reboot	Crypto Officer User	N/A
Update firmware	Crypto Officer	HMAC Key (R,E)
Zeroize	Crypto Officer	All (W)
Disable ATA Security	Crypto Officer User	N/A
Enable ATA Security	Crypto Officer User	N/A
Level 0 Discovery	Crypto Officer User	N/A
Get MSID	Crypto Officer User	N/A

5 Security Functions

The table below lists approved cryptographic algorithms employed by the Module.

Algorithm	Certificate Number
SHS	1442
HMAC	963
AES	1637
ANSI X9.31 PRNG	878

6 Key Management

The following cryptographic keys and CSPs are supported by the Module.

Name and type	Usage	NV Storage	Volatile Storage
Master/User/SID/Admin1-4/User1-4 Passwords (PINs)	Authentication of each role	Flash Memory (Hashed by SHA256)	N/A
KEK(AES Key)	Enc/Dec of MEK	Flash Memory	SRAM in Controller (Plaintext)
MEK(AES Key)	Enc/Dec of User Data	Flash Memory	SRAM in Controller (Plaintext)
HMAC Key(HMAC Key)	FW Image Authentication	Flash Memory	SRAM in Controller (Plaintext)
RNG Seed Key(X9.31 Seed Key)	RNG	Flash Memory	SRAM in Controller (Plaintext)
RNG Seed(X9.31 Seed)	RNG	Flash Memory	SRAM in Controller (Plaintext)

7 Self Tests

The Module runs a set of self-tests on power-up. If one of the self-tests fails, the Module transitions into an error state where all data output and cryptographic operations are disabled.

The Module runs power-up self-tests for the following algorithms:

Algorithm	Test
Firmware integrity	HMAC-SHA256 of the firmware image
AES	KAT for AES
HMAC	KAT for HMAC-SHA256
SHA	KAT for SHA256
ANSI X9.31 PRNG	X9.31 using AES

During the Module operation the following conditional self-tests are performed:

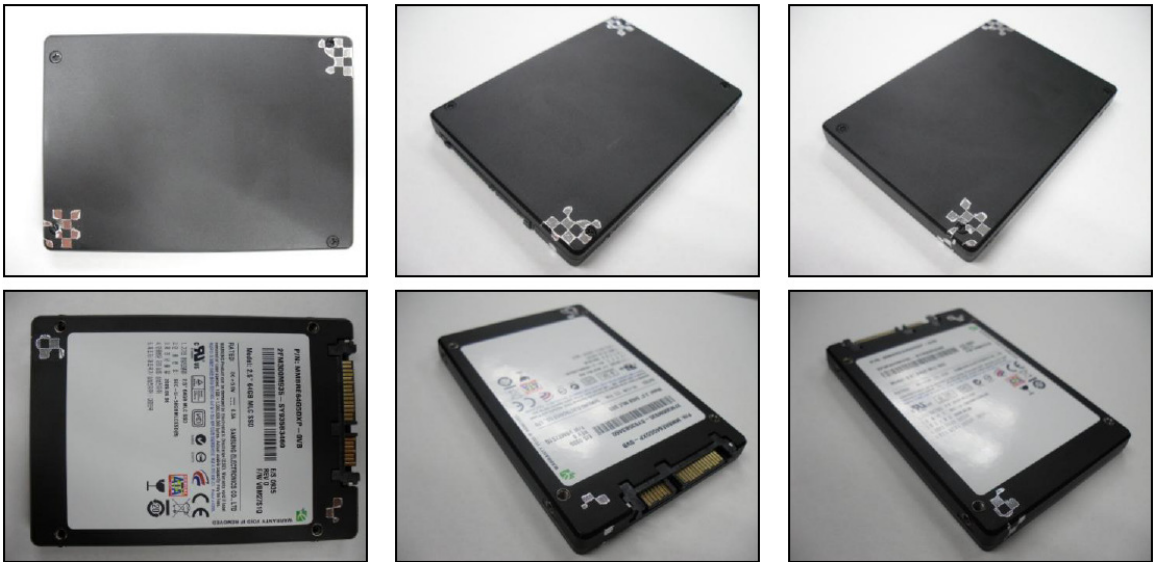
Condition	Test
Random number generation	Continuous PRNG Test
Firmware Update	Firmware update test using HMAC-SHA256

8 Physical Security

The Module consists of production-grade components enclosed in a hard plastic 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 140-2 Level 2 Physical Security requirements so that tampering is easily detected when the top panel is removed. The tamper-evident labels are applied over both top and bottom panels of the Module at the factory. The tamper-evident labels are not removed and reapplied without tamper evidence.

An image of the Module with tamper-evident labels applied is provided below:

An image of the Module with tamper-evident labels detached is provided below:



9 Secure Operation

The Module operates in the Approved Mode of Operation until zeroization is performed. Upon completion of zeroization the module must be returned to the factory for further use. The Module documentation provides detailed guidance for the Module users and administrators.

The Module and the tamper-evident labels must be inspected periodically. If evidence of tampering is detected, the Module must be disabled immediately and returned to the factory.

All authentication data shall be kept confidential and the Module shall not be assessed by unauthorized persons.

The Module is installed as follows:

ATA Interface initialization:
- Set the Master Password by using SET PASSWORD command
- Set the User Password by using SET PASSWORD command

Opal Interface initialization:
- Open a session to the Admin SP as the Anybody authority
- Get the MSID's PIN value from Admin SP for taking ownership of the Module
- Open a session to the Admin SP as the SID authority
- Set a new password value in the SID's credential PIN column
- Activate the Locking SP by using the Activate method
- Open a session to the Locking SP as the admin1 authority
- Set the Locking Table to be locked