MEMKOR MKD-O2F 2.5”/M.2/U.2 SSD

FIPS 140-2 NON-PROPRIETARY SECURITY POLICY

Document Revision: V 1.0

REVISION HISTORY

Version	Date	Change Description
1.0	Dec 13, 2019	First Release

TABLE OF CONTENT

LIST OF TABLES

LIST OF FIGURES

1 INTRODUCTION

1.1 OVERVIEW

This document defines the non-proprietary FIPS 140-2 Security Policy for Memkor, Inc. (Memkor) *Secure*+ MKD-O2F multi-chip standalone cryptographic modules, referred hereinafter as cryptographic module(s) or MKD-O2F module(s) or Solid State Drive(s) (SSD) and fully satisfying FIPS 140-2 Security Level 2 requirements.

The MKD-O2F modules consist of both hardware and firmware components, and come in either SFF-8201 compliant 2.5” SATA/ U.2 (NVMe/PCIe) or M.2 2280 form factor with SATA interface.

The *Secure*+ MKD-O2F module uses an AES-256 hardware engine with XTS encryption mode and ATA command based key management, with architecture enabling low effort and host computer environment agnostic integration into a broad range of applications such as boot drive or data recording. In addition, each module supports hardware and/or software triggered cryptographic erase, zeroization and write protect functions.

With capacities ranging between 250GB and 4TB, SATA or PCIe/NVMe interface and ruggedization for up to 30gRMS, Memkor MKD-O2F Series of cryptographic module SSD’s are aimed at the most challenging environment deployments.

1.2 REFERENCES

(1) Security Requirements for Cryptographic Modules, NIST (FIPS 140-2), May 25, 2001
(2) Advanced Encryption Standard, NIST (FIPS 197), FIPS Publication 197, Nov 26, 2001
(3) Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices, SP 800-38E, 2010
(4) Secure Hash Standard, NIST, FIPS Publication 180-4, 2012
(5) Recommendation for Random Number Generation Using Deterministic Random Bit Generator, NIST, SP 800-90A, 2012

1.3 FIPS 140-2 VALIDATED MODULES

FIPS 140-2 validated module locked BOM Model Numbers are depicted in table below:

Locked BOM Model Number	Hardware Version	Firmware Source/Version	Description
MKD25ST250IN-O2FA	677180474240	05.M54 / 05.M54BO	2.5” SATA, 9.5mm, 250GB, MKD-O2F *BLACK* Series
MKD25ST250IN-O2FB	677190474240	05.M54 / 05.M54BQ	2.5” SATA, 9.5mm, 250GB, MKD-O2F *BLACK* Series
MKD25ST500IN-O2FA	677190474240	05.M54 / 05.M54CO	2.5” SATA, 9.5mm, 500GB, MKD-O2F *BLACK* Series
MKD25ST1T0IN-O2FA	677191474240	05.M54 / 05.M54DO	2.5” SATA, 9.5mm, 1TB, MKD-O2F *BLACK* Series
MKD25ST4T0IO-O2FA	670396422280	05.M54 / 05.M54FP	2.5” SATA, 9.5mm, 4TB, MKD-O2F *ORANGE* Series
MKDM8ST500IO-O2FA	672390474250	05.M54 / 05.M54CR	M.2 2280, 500GB, MKD-O2F *ORANGE* Series
MKD25P41T0IO-O2FA	675391474280	05.M54 / 05.P54DS	U.2/2.5” PCIe/NVMe, 1TB, MKD-O2F *ORANGE* Series
MKD25P44T0IO-O2FA	675496422290	05.M54 / 05.P54FT	U.2/2.5” PCIe/NVMe, 4TB, MKD-O2F *ORANGE* Series

Table 1 FIPS 140-2 Validated Cryptographic Modules

2 CRYPTOGRAPHIC BOUNDARY

2.1 BLOCK DIAGRAM

Figure below depicts MKD-O2F cryptographic module block diagram.

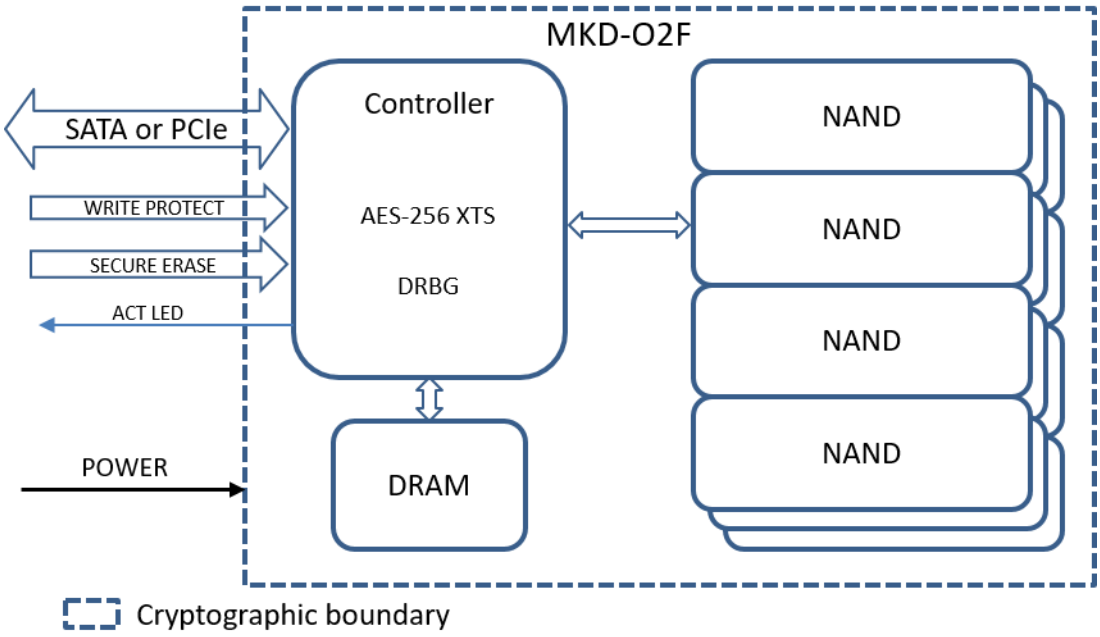

Figure 1 Cryptographic Module Block Diagram

2.2 PHYSICAL BOUNDARY

2.2.1 U.2 PCIE/NVME MODULES

The physical cryptographic boundary for U.2/2.5” PCIe/NVMe modules is defined by the aluminum case that contains the integrated circuits, U.2 host computer connector and 5-pin I/O header used as 1-bit zeroization and 1-bit write protect ports. Figure 2 depicts the physical cryptographic boundary.

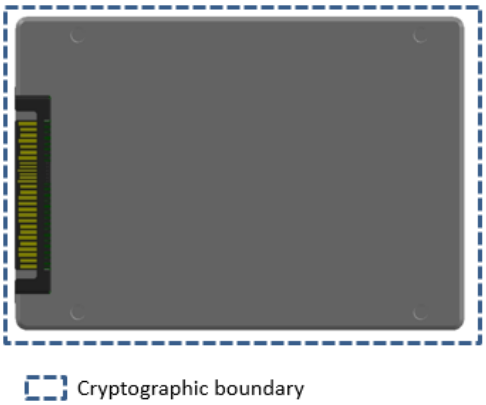

Figure 2 Physical Cryptographic Boundary for U.2 PCIe/NVMe modules

2.2.2 2.5” SATA MODULES

The physical cryptographic boundary for all 2.5” SATA modules is defined by the aluminum case that contains the integrated circuits, 5-pin or 8-pin header but it excludes SATA host computer connector. Figure 3 shows physical cryptographic boundary for 2.5” SATA modules.

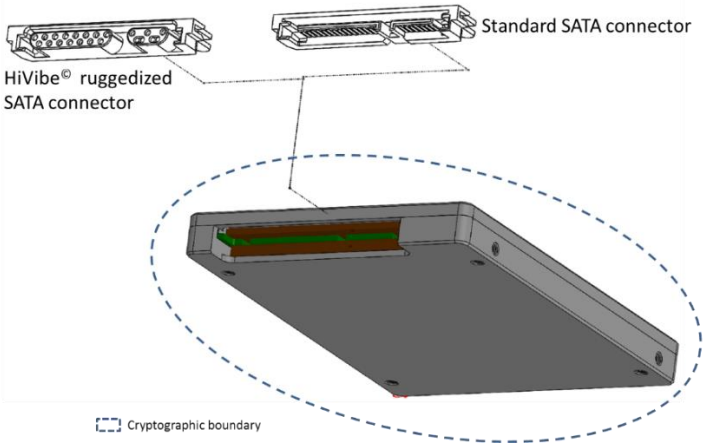

Figure 3: 2.5” SATA Physical Cryptographic Boundary

Note: 2.5” SATA cryptographic modules “do not” include a multi-pin host connector on the cryptographic module boundary itself; such external connectors are considered as external peripheral equipment as far as the validated cryptographic module is concerned. However, please note that all units are delivered to the Cryptographic Officer by Memkor with either standard 15+7 pin SATA (or) HiVibe© ruggedized SATA connector which “are not” part of the cryptographic module.

2.2.3 M.2 2280 SATA MODULE

The physical cryptographic boundaries for M.2 2280 SATA module is defined by the opaque tamper-evident epoxy resins that covers the PCB Assembly, and M.2 SATA port. The cryptographic boundaries are depicted in Figure 4 below. See also Figure 12 for additional images of the cryptographic module.

Figure 4 Physical Cryptographic Boundary for M.2 2280 SATA Module

2.3 MODULE DEPICTION

Memkor’s MKD-O2F cryptographic modules span across Memkor’s ORANGE and BLACK Series SSD families and Figures 5 through 12 illustrate each module type.

2.3.1 HIGHLY RUGGEDIZED 2.5” SATA BLACK SERIES

- Up to 30gRMS and -40degC to 85degC operations
- Standard SATA or HiVibe SATA connectors
- 250/500/1000 GB capacity
- Hardware triggered Zeroization and Write Protect via SATA connector pins

Figure 5 MKD25ST250IN-O2FA 2.5” 250GB SATA 9.5mm SSD Module

Figure 6 MKD25ST250IN-O2FB 2.5” 250GB High Endurance SATA 9.5mm SSD Module

Figure 7 MKD25ST500IN-O2FA 2.5” 500 GB SATA 9.5mm SSD Module

Figure 8 MKD25ST1T0IN-O2FA 2.5” 1 TB SATA 9.5mm SSD Module

2.3.2 HIGH PERFORMANCE 2.5” SATA ORANGE SERIES

- Up to 16.3 gRMS and -40degC to 85degC operations, standard SATA or HiVibe SATA connectors, 4 TB capacity
- Hardware triggered Zeroization and Write Protect via 8-pin header and SATA connector pins

Figure 9 MKD25ST4T0IO-O2FA 2.5” 4 TB SATA 9.5mm SSD Module

2.3.3 HIGH PERFORMANCE U.2/2.5” PCIE/NVME ORANGE SERIES

- Up to 16.3 gRMS and -40degC to 85degC operations, 1 or 4 TB capacity
- Hardware triggered Zeroization and Write Protect via 5-pin header and SATA connector pins

Figure 10 MKD25P41T0IO-O2FA U.2/2.5” PCIe 9.5mm 1 TB SSD Module

Figure 11 MKD25P44T0IO-O2FA 2.5” PCIe 9.5mm 4TB SSD Module

2.3.4 HIGH PERFORMANCE M.2 2280 SATA ORANGE SERIES

- -40degC to 85degC operations
- 500 GB capacity
- Hardware triggered Zeroization and Write Protect via SATA connector pins

Figure 12 MKDM8ST500IO-O2FA M.2 SATA 500 GB SSD Module

3 SECURITY LEVEL SPECIFICATION

The cryptographic modules support the following FIPS 140-2 security levels:

Security Requirements	Level
Cryptographic Module Specification	2
Cryptographic Module Ports and Interfaces	2
Roles, Services, and Authentication	2
Finite State Model	2
Physical Security	2
Operational Environment	N/A
Cryptographic Key Management	2
EMI/EMC	2
Self-tests	2
Design Assurance	2
Mitigation of Other Attacks	N/A

Table 2 Security Requirement Levels

4 PHYSICAL PORTS AND LOGICAL INTERFACES

4.1 HIGHLY RUGGEDIZED 2.5” SATA BLACK SERIES

For MKD25ST250IN-O2FA, MKD25ST250IN-O2FB, MKD25ST500IN-O2FA and MKD25ST1T0IN-O2FA SATA modules, the applicable ports include SATA Power and SATA Signal ports as detailed in Table 3 and Figure 133.

Physical Port	Logical Interface
SATA Power	Control input, Status output, and Power Input
SATA Signal	Control Input, Status output, Data input, Data output

Table 3 2.5” SATA Black Series Modules Physical Ports and Logical Interfaces

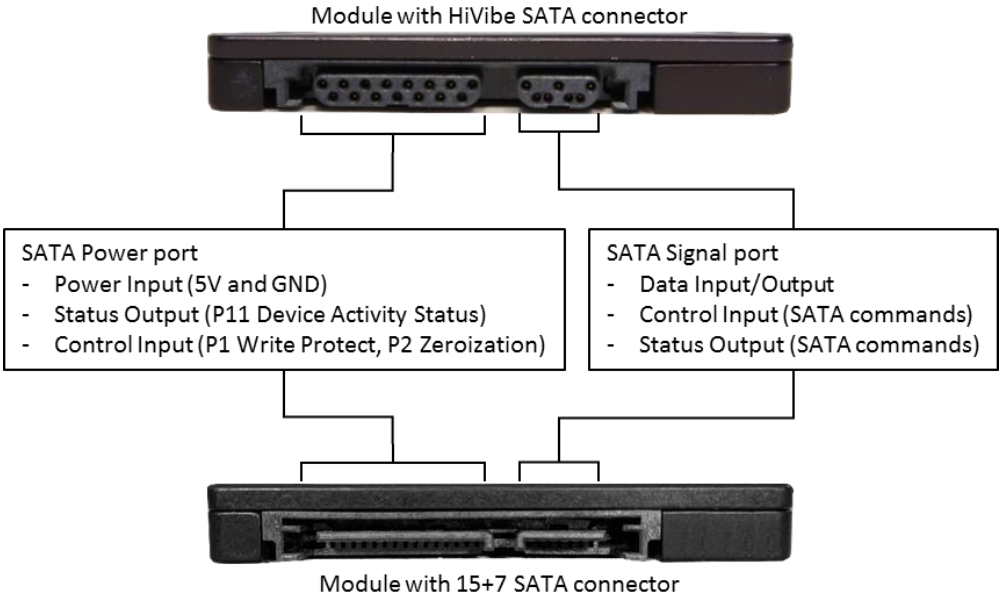

Figure 13 2.5” SATA Black Series Modules Physical Ports and Logical Interfaces

4.2 HIGH PERFORMANCE 2.5” SATA ORANGE SERIES

For MKD25ST4T0IO-O2FA SATA module, the applicable ports include SATA Power, SATA Signal and Write Protect/Zeroization ports as detailed in Table 4 and Figure 134.

Physical Port	Logical Interface
SATA Signal	Data input, Data output, Control input, Status output
SATA Power	Control input, Status output, and Power Input
Write Protect	Control Input
Zeroization	Control Input

Table 4 2.5” SATA Orange Series Modules Physical Ports and Logical Interfaces

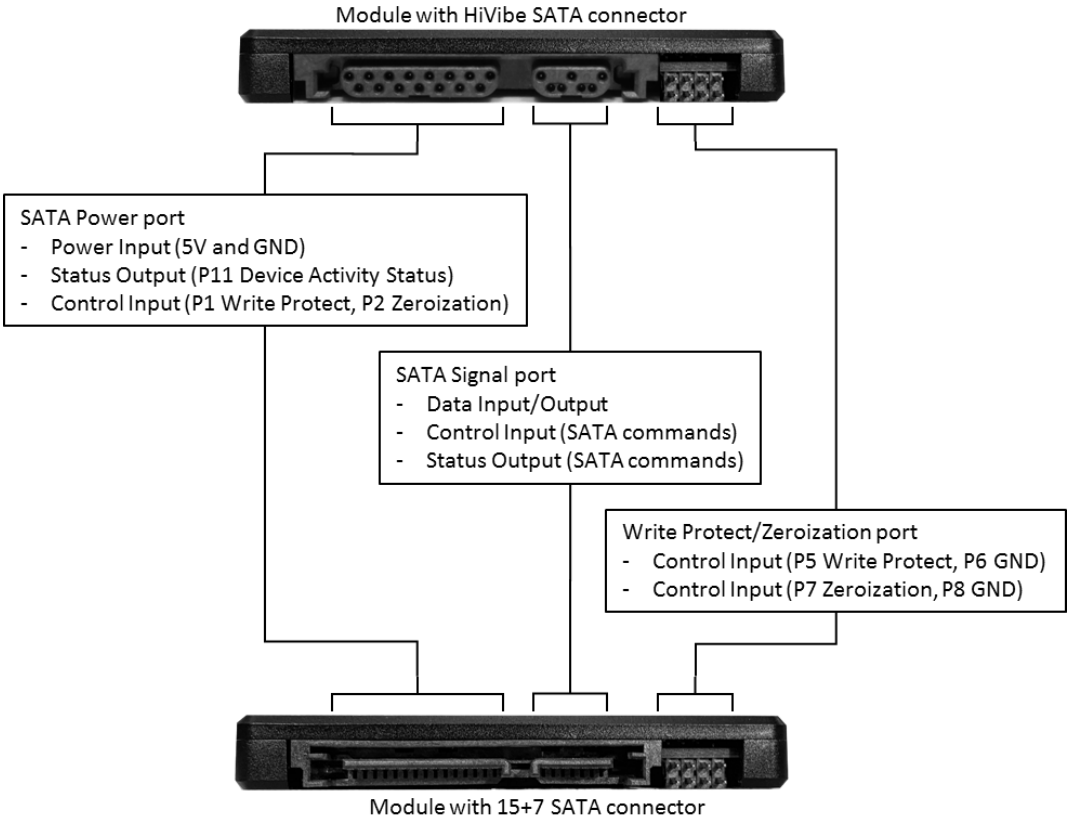

Figure 14 2.5” SATA Orange Series Modules Physical Ports and Logical Interfaces

4.3 HIGH PERFORMANCE M.2 2280 SATA ORANGE SERIES

For MKDM8ST500IO-O2FA SATA module, the applicable port is M.2 SATA port as detailed in Table 5 and Figure 15.

Physical Port	Logical Interface
M.2 SATA	Data input, Data output, Control input, Status output, and Power Input

Table 5 M.2 2280 SATA Orange Series Modules Physical Ports and Logical Interfaces

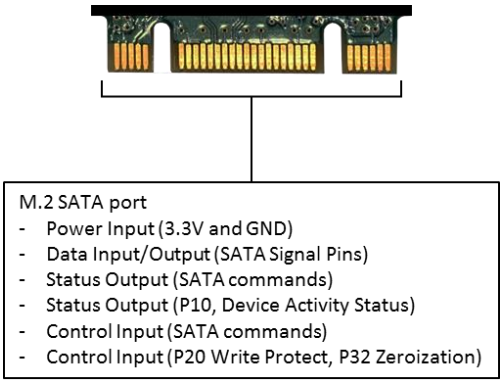

Figure 15 M.2 2280 SATA Orange Series Modules Physical Ports and Logical Interfaces

4.4 HIGH PERFORMANCE U.2/2.5” PCIE/NVME ORANGE SERIES

For MKD25P41T0IO-O2FA PCIe module, the applicable ports are PCIe and Write Protect/Zeroization ports as depicted in Table 6 and Figure 16

Physical Port	Logical Interface
PCIe	Data input, Data output, Control input, Status output, and Power Input
Write Protect	Control Input
Zeroization	Control Input

Table 6 U.2 PCIe Orange Series Modules Physical Ports and Logical Interfaces

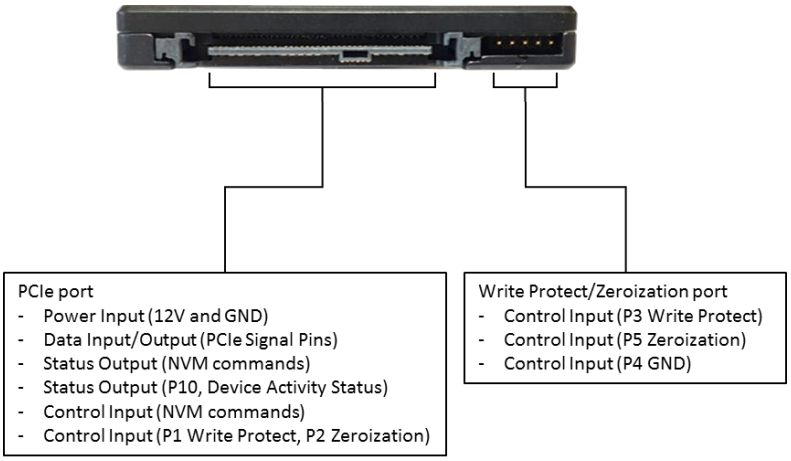

Figure 16 U.2 PCIe Orange Series Modules Physical Ports and Logical Interfaces

5 APPROVED MODES OF OPERATION DESCRIPTION

The module only supports a FIPS Approved Mode of Operation.

Mode	State	Description
Security Mode Disabled	**Uninitialized**	SSD Security is not activated by Crypto Officer. No authentication required to access user data SSD area.
Security Mode Enabled	**Crypto-Officer**	Crypto-Officer verifies physical security of cryptographic module and activates module security by entering inital Host Key
	Self-Test	SSD is in the process of executing self-test sequence
	Login	SSD allowes user access to 256MB Shadow LBA area only and is awaiting Host Key authentication from the Host
	Authenticated User	SSD received correct Host Key from the Host, and enables full access to user data SSD area
Exception Mode	**Error State**	When error is detected, SSD enters into Exception mode and aborts Host requests

Table 7 Cryptographic Module Modes of Operation

6 SECURITY RULES

The following specifies the security rules under which the cryptographic module shall operate:

- The module only supports a FIPS Approved Mode of Operation.
- The module supports the following power-up self-tests:
  - Firmware image verified by SHA-256 hash tag
  - SHA-256 KAT
  - SP800-90A HASH DRBG KAT
  - SP800-90A HASH DRBG Section 11.3 Health Test
  - AES-XTS Encrypt KAT
  - AES-XTS Decrypt KAT
  - NDRNG Repetition Count Test
  - NDRNG Adaptive Proportion Test
- The module supports the following conditional self-tests:
  - Continuous RNG test on Approved SP800-90A HASH DRBG
  - Continuous RNG test on non-Approved NDRNG
  - NDRNG Repetition Count Test
  - NDRNG Adaptive Proportion Test
- The module will be in Uninitialized State when shipped from the factory.
- Crypto Officer can initialize and activate the FIPS Approved Mode of Operation by following the next procedures:
  1. Inspect module per section Physical Security Policy.
  2. Power-on the module.
  3. Module shall appear to the host as uninitialized; this confirms all power-up self-tests successfully passed.
  4. Execute service “**Show Status**” ATA command Identify Device. Confirm the module Hardware Part Number and Firmware Version is an approved configuration as listed in section Cryptographic Boundary.
  5. Execute service “**Set Host Key (PIN)”** to set a Host Key (PIN). This is a one-time operation.
  6. Module will automatically reboot, and run power-up self-tests again.
     If all power-up self-tests pass, the module SSD capacity will appear to the host as 256MB, which means that security is enabled.
  7. Module is now in a Login State.
  8. Execute service “**Show Status**” (ATA command Identify Device) and verify module status specifies (FIPS-compliant, Security Enabled). (See below for more information on FIPS Approved Mode indicator)
  9. Module is now in the FIPS Approved Mode of Operation.
- The FIPS Approved Mode indicator can be obtained by executing “**Show Status**” ATA command Identify Device. Identify Device Command FIPS Descriptor Word 137 data 0x0023 (FIPS-compliant, Security Enabled) for SATA / AHCI. Identify Device Command FIPS Descriptor Word 3092 data 0x0023 (FIPS-compliant, Security Enabled) for PCIe / NVMe.
- If the module fails any power-up tests or conditional tests, then the module will enter a hard error state. During a hard error state, the module is not available for any services, and it inhibits all data output. Error indicator is:
  - Module will not show up to host.

- Module will output constant toggle signal via Activity signal pin, ACT LED. Pin location identified below per part number:

Model Number	Pin
MKD25ST250IN-O2FA	SATA P11
MKD25ST500IN-O2FA	SATA P11
MKD25ST250IN-O2FB	SATA P11
MKD25ST1T0IN-O2FA	SATA P11
MKD25ST4T0IO-O2FA	SATA P11
MKD25P41T0IO-O2FA	PCIe P11
MKD25P44T0IO-O2FA	PCIe P11
MKDM8ST500IO-O2FA	M.2 Pin 10

Table 8 Activity Signal on Host Connector

- If the module passed all self-test items, then the module will show up to the host and it is available to start servicing commands.
- The module inhibits all data output during self-tests.
- At Login State, authentication is always required.
- Any invalid attempts to authenticate to the module will result in status output “Password Failure” (Fail=1h, key retry count value). Module does not provide any other feedback to the operator and mitigates brute force attacks as described in section Identification and Authentication Policy.
- The module does not support manual key entry or any other type of key entry/output.
- The module supports zeroization to destroy all critical security parameters.
- The module logically inhibits the data output interface when performing key generation and zeroization processes.

The module supports one Host Key for a single user.

7 CRITICAL SECURITY PARAMETERS, AND PRIVATE KEYS

The cryptographic module comprises the following Keys and CSPs:

CSP & Key	Description / Usage	Storage
AES Master Key	Cryptographic module uses an AES 256-bit XTS key to encrypt/decrypt User LBA data. • Generation: Internally via FIPS approved SP800-90 HASH DRBG • Entry: N/A • Output: N/A • Zeroization : Zeroization command or exceeding PIN attempt limit	Controller/NAND
Host Key (PIN)	User send 10-32 bytes Host Key (PIN). Cryptographic module supports one PIN code. • Generation: Crypto Officer/User generates PIN • Entry: Sent to cryptographic module in plaintext • Output: N/A • Zeroization : Zeroization command or exceeding PIN attempt limit	Controller/NAND
DRBG Internal State	The SSD module contains a non-deterministic hardware random number generator (NDRNG) that uses an internal, unpredictable physical source of entropy that is outside of human control. The NDRNG generates random numbers that serve as seeding values for the FIPS Approved Deterministic Random Bit Generator (SP800-90A HASH DRBG). Continuous RNG tests are performed on the outputs of the NDRNG and on the outputs of the Approved SP800-90A DRBG. Note: the minimum number of bits of entropy generated by the module for use in key generation is 256. Values of V and C of HASH DRBG mechanism • Generation: Internally using the SP800-90 HASH DRBG • Entry: N/A • Output: N/A • Zeroization : Zeroization command or exceeding PIN attempt limit	Controller/NAND

Table 9 Critical Security Parameters

8 IDENTIFICATION AND AUTHENTICATION POLICY

The module supports Crypto Officer (CO) and User roles. The CO role is to conduct an initial inspection and initialize the security of the module. The User role is to define user authentication to perform module security services. Please refer to Table 10.

Role	Role Description	Authentication Type	Authentication data
Crypto Officer (CO)	The CO receives the Cryptographic module when first received from the manufacturer and conducts the following procedures • The CO shall inspect the module per Section Physical Security Policy. • The CO shall initialize the FIPS 140-2 security mode by entering the initial Host Key PIN • The CO shall be responsible for the proper handling of the module during its usage, including routine physical inspections as recommended in this document • The CO shall be responsible for module handling when in hard Error State. It is recommended to contact Memkor should such situation occurs.	Role-based	PIN
User	The User becomes responsible for the module, once Crypto Officer initializes the FIPS 140-2 Security. The User shall follow the following security procedures: • The User shall change the Host Key before an initial use. • The User shall contact Crypto Officer upon any suspicion of physical security violation or any evidence of tamper. • The user shall contact Crypto Officer when the module entered the Error State.	Role-based	PIN

Table 10 Roles and Required Identification and Authentication

Authentication Method	Probability	Strenght of Mechanism
Host Key (PIN) based authentication	Minimum PIN length is 10 bytes with a maximum length of 32 bytes, and Key Retry count is persistent during power-cycle.	The probability of randomly authenticating a Host Key (PIN) in a single attempt with a 10 characters password is 1/2^80, considering single byte is 2^8 and 10 bytes length is total (2^8)^10 different possible input. This probability is less than FIPS 140-2 authentication strength requirements 1/1,000,000. To protect the module from brute-force attack, module implements a Key Retry count (“N”). The Key Retry count will increase, whenever Host Key verification fails. This Key Retry count record is non-volatile even after power cycling. When key retry count is greater than 5, the module will start zeroization process automatically. Key Retry count is reset to zero when correct Host Key is entered and verified. Hence, in a one-minute period, the probability that a random attempt will succeed, or false acceptance will occur, is 5/(2^80) which is less than 1 in 100,000.

Table 11 Strength of Authentication Mechanisms

9 ACCESS CONTROL POLICY

The cryptographic module supports two roles: Crypto Officer (CO) and User. The type of services corresponding to each of the supported roles is described as below.

(U/A = Unauthenticated, R = Read, W = Write, Z = Zeroize, N/A = Not applicable,)

Service	Description	CO	User	U/A	Type of Access	Cryptographic Kyes and CSP’s
Write Data (to Shadow LBA)	Receive plaintext data from host. Write data to non-secured range of internal memory.	✓	✓	✓	N/A	N/A
Read Data (from Shadow LBA)	Output plaintext data to host. Read data from non-secured range of internal memory.	✓	✓	✓	N/A	N/A
Write Data (to User LBA)	Receive plaintext data from host, outside of the cryptographic boundary, AES encrypt data and program into secured range of internal memory.	✓	✓		R	AES Master Key
Read Data (from User LBA)	AES decrypt data from secured range of internal memory. Output plaintext to host, outside of the cryptographic boundary.	✓	✓		R	AES Master Key
Set Host Key (PIN)	Set or Change Host Key (PIN).	✓	✓		W W W	Host Key AES Master Key DRBG Internal State
Login/Unlock	Unlock secured range of internal memory.	✓	✓		R R	Host Key AES Master Key
Logout/Lock	Lock-up secured range of internal memory.	✓	✓	✓	N/A	N/A
Show Status	Status Outputs. (ATA command Identify Device and other status information)	✓	✓	✓	N/A	N/A
Self-Test	Module automatically performs required self-tests of the module after power-on.	✓	✓	✓	N/A	N/A
Set Write Protect	Set the device to read-only using GPIO.	✓	✓	✓	N/A	N/A
Zeroize	Destroy all CSPs. This service can be triggered by one of below methods: • ATA CRYPTOSCRAMBLE • ATA SET SECURITY ERASE • GPIO External trigger	✓	✓	✓	Z Z Z	Host Key AES Master Key DRBG Internal State

Table 12 Roles, Services, CSPs, and Types of Access

10 ALGORITHMS

10.1 APPROVED ALGORITHMS

CAVP Cert.	Algorithm	Standard	Mode/Method	Key Lengths, Curves, or Moduli	Use
C1408[1]	AES	FIPS 197 SP 800-38A	AES ECB	256	Prerequisite only for AES XTS
C1414	AES	FIPS 197 SP 800-38E	XTS	256	Data Encryption/ Decryption for storage applications only
Vendor Affirmed	CKG	SP 100-133			Cryptographic Key Generation
C1415	DRBG	SP 800-90A	HASH_DRBG SHA-256		Deterministic Random Bit Generation
C1409	SHS	FIPS 180-4	SHA-256		Message Digest

Table 13 Table of Approved Algorithms

10.2 ALLOWED ALGORITHMS

The module supports the following non-approved but allowed algorithms:

Algorithm	Caveat	Use
NDRNG	Only used for generating seed materials for the Approved HASH_DRBG. Minimum security strength is 256 bits.	Non-deterministic Random Number Generator
PBKDF	No Security Claimed as per FIPS-140-2 IG section 1.23	Used for obfuscation of PIN, considered as plaintext

Table 14 Table of Allowed Algorithms

[1] Module does not implement AES-CBC; Latent Functionality.

11 PHYSICAL SECURITY POLICY

2.5” SATA and U.2/PCIe SSD’s comprise the integrated circuits enclosed in the two-part CNC/aluminum enclosure connected with screws and making the cryptographic module. The enclosure screws are sealed by tamper evident labels applied in the factory. Furthermore, the PCBA is encapsulated with a hard, opaque, tamper-evident Urethane/Epoxy Coating and covered with tamper evident filler. The module is opaque within the visible spectrum.

M.2 SSD is encapsulated with a hard, opaque, and tamper evident Urethane/Epoxy Coating.

Table below lists the actions required by the Cryptographic Officer Role to ensure physical security integrity of the cryptographic module:

Physical Security Mechanisms	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
CNC/Aluminum enclosure	On initial receipt of the device and in accordance with Crypto Officer organizational security policy. It is recommended to inspect the enclosure once a year.	Inspect for evidence of prying or removal such as: - Bending of enclosure - Marks from attempts to separate top and bottom parts of enclosure - Removal of tamper evident label
Tamper Evident Labels	On initial receipt of the device and in accordance with Crypto Officer organizational security policy. It is recommended to inspect the seals once a year.	Inspect labels for evidence of a removal attempt. - Label removal or an attempt to remove will result in a broken label pattern and/or a residue on the enclosure. - Solvent attacks will result in the tamper evident label being physically disfigured - Temperature attacks will result in the tamper evident label being disfigured - It is impossible to reapply the label
Urethane/Epoxy Coating	On initial receipt of the device and in accordance with Crypto Officer organizational security policy. It is recommended to inspect the Epoxy Coating once a year.	Inspect for scratches, gouges, scrapes, deformations, and any other suspicious signs of malice and tampering.
Tamper Evident Filler	On initial receipt of the device and in accordance with Crypto Officer organizational security policy. It is recommended to inspect the Tamper Evident Filler once a year.	Inspect for scratches, gouges, scrapes, deformations, and any other suspicious signs of malice and tampering.

Table 15 Inspection/Testing of Physical Security Mechanisms

If any evidence of tampering exists, the Crypto Officer is required to cease use of the cryptographic module immediately.

Figure 17 Enclosure and Tamper-evident labels before and after removal

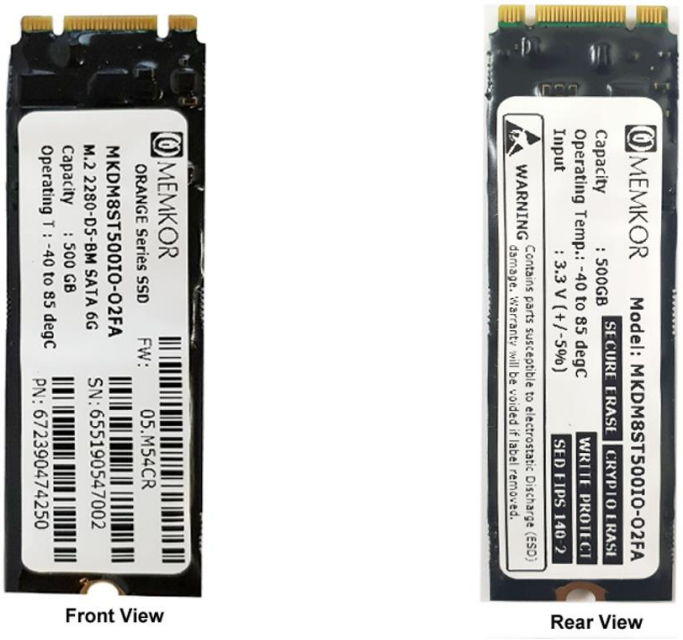

Figure 18 M.2 Tamper Evident Urethane/Epoxy Coating

12 ELECTROMAGNETIC INTERFERENCE AND COMPATIBILITY (EMI/EMC)

The Cryptographic modules successfully completed compliance testing in accordance with FCC Part 15 Subpart B.

13 MITIGATION OF OTHER ATTACKS POLICY

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

Table 16 Table of Mitigation of Other Attacks

The Module has not been designed to mitigate attacks outside of the scope of FIPS 140-2.

14 ACRONYMS

Term	Description
2.5”	2.5 inch Form Factor (SFF-8201)
AES	Advanced Encryption Standard (FIPS-197)
CMVP	Cryptographic Module Validation Program
CO	Crypto Officer
CPU	Central Processing Unit
CSP	Critical Security Parameter
CSP	Critical Security Parameters
DRAM	Dynamic Random-Access Memory
DRBG	Deterministic Random Bit Generator
FIPS	Federal Information Processing Standard Publication
GPIO	General Purpose Input Output
KAT	Known Answer Test
LBA	Logical Block Addressing
M.2	Computer Expansion Card Disk form factor
NAND	NAND flash memory
NDRNG	Non-Deterministic Random Number Generator
NVMe	NVM Express or Non-Volatile Memory Host Controller Interface Specification
PCIe	PCI Express
PIN	Personal Identification Number (Host Key)
RNG	Random Number Generator
SATA	Serial Advanced Technology Attachment
SFF	Small Form Factor
SHA	Secure Hash Algorithms
SHS	Secure Hash Standard
SSD	Solid State Drive
U.2	PCIe Computer Interface typically used on 2.5” Form Factor

Table 17 Acronyms