We turn on ideas

Seagate® Momentus® Thin Self-Encrypting Drives TCG Opal FIPS 140 Module Security Policy

Security Level 2

Rev. 0.9 – Aug 30, 2010

Seagate Technology, LLC

Table of Contents

1 Introduction

1.1 Scope

This security policy applies to the FIPS 140-2 Cryptographic Module (CM) embedded in **Seagate® Momentus® Thin TCG Opal Self-Encrypting Drive** products.

This document meets the requirements of the FIPS 140-2 standard (Appendix C) and Implementation Guidance (section 14.1). It does not provide interface details needed to develop a compliant application.

This document is non-proprietary and may be reproduced in its original entirety.

1.2 Security Levels

Requirement Area	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
Electromagnetic Interface / Electromagnetic Compatibility (EMI / EMC)	3
Self – tests	2
Design Assurance	2
Mitigation of Other Attacks	N/A

1.3 References

1. FIPS PUB 140-2
2. Derived Test Requirements for FIPS PUB 140-2
3. Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program
4. TCG Storage Security Subsystem Class: Opal, Specification Version 1.00, Revision 3.00, February 4, 2010
5. TCG Storage Architecture Core Specification, Specification Version 2.00 Final, Revision 1.0, April 20, 2009
6. TCG Storage Interface Interactions Specification, Specification Version 1.0, January 14, 2009
7. ATA-8 ACS
8. Serial ATA Rev 2.6 (SATA)

1.4 Acronyms

AES	Advanced Encryption Standard (FIPS 197)
CBC	Cipher Block Chaining, an operational mode of AES
CM	Cryptographic Module
CO	Crypto-officer
CSP	Critical Security Parameter
MEK	Media Encryption Key
FIPS 140	FIPS 140-2
HDA	Head and Disk Assembly
HDD	Hard Disk Drive
IV	Initialization Vector for encryption operation
LBA	Logical Block Address
KAT	Known Answer Test
MBR	Master Boot Record
MSID	Manufactured SID, public drive-unique value that is used as default PIN, TCG term
POR	Power-on Reset (power cycle)
POST	Power on Self-Test

PSID	Physical SID, public drive-unique value
RNG	Random Number Generator
SED	Self-Encrypting Drive, Seagate HDD products that provide HW data encryption.
SID	Security ID, PIN for Drive Owner CO role, TCG term
SoC	System-on-a-Chip
SOM	Security Operating Mode
SP	Security Provider or Security Partition (TCG), also Security Policy (FIPS 140)

2 Cryptographic Module Description

2.1 Overview

The Seagate Momentus Thin Self-Encrypting Drive (SED) TCG Opal FIPS 140 Module is embedded in Seagate Momentus Thin SED model disk drives. The cryptographic module (CM) provides a wide range of cryptographic services using FIPS approved algorithms. Services include hardware-based data encryption, instantaneous user data disposal with cryptographic erase, independently controlled and protected user data LBA ranges, and authenticated FW download. The services are provided through an industry-standard TCG Opal SSC interface.

The CM is a multiple-chip embedded physical embodiment. The physical interface to the CM is the SATA connector and jumper block pins. The logical interface is the industry-standard ATA (7), TCG SWG (5), and Opal SSC (4) protocols, carried on the SATA transport interface (8). The primary function of the module is to provide data encryption, access control and cryptographic erase of the data stored on the hard drive media. The human operator of the drive product interfaces with the CM through a "host" application on a host system.

The CM functionality is implemented in the ASIC, Serial Flash, SDRAM and firmware. Each of these components additionally provides non-security functionality that is logically isolated from the security functions. The drive media provides the non-volatile storage of the keys, CSPs and FW. This storage is in the "system area" of the media which is not logically accessible / addressable by the host application.

The ASIC is an SoC which has the following major logical functions: host interface using an industry standard SATA interface, a RW Channel interface to the HDA, interface to media motor controller, data encryption engine, and processing services which execute the firmware. An Approved Security Function, AES-128, is implemented in the data encryption engine.

During drive operation, the SDRAM hosts the firmware and the encrypted user data being transferred between the media and the ASIC.

The firmware is logically separated into four groups: ATA interface, Security, Servo, and Read/Write. The FIPS 140 services are isolated in the Security section of the firmware.

Security functions fall into two categories. At-rest data is transferred to/from the drive's media and encrypted/decrypted using ATA write/read commands respectively. Other security operations, including authentication and management of cryptographic secrets, are accessed using ATA Trusted Send/Receive commands. These commands are actually wrappers for another industry standard protocol: TCG Opal. The security services provided by the CM through the TCG protocol correspond to the methods of the following TCG SP Templates: Base, Admin, Locking, and Crypto. Some of the TCG-based services are specific to the Seagate implementation and are described in detail in product documentation.

2.2 Logical to Physical Port Mapping

FIPS 140-2 Interface	Module Ports
Data Input	SATA Connector
Data Output	SATA Connector
Control Input	SATA Connector
Status Output	SATA Connector
Power Input	Power Connector

2.3 Hardware and Firmware Versions

The Momentus® SED Drives, FIPS 140 Module has been validated in six configurations:

1. Model ST320LT009: HW ver 9WC142, FW ver 1003HPMA
2. Model ST320LT009: HW ver 9WC142, FW ver 1002HPBA
3. Model ST320LT009: HW ver 9WC142, FW ver 1001DEMA
4. Model ST250LT009: HW ver 9WC14C, FW ver 1001DEMA
5. Model ST320LT009: HW ver 9WC142, FW ver 1001SDMA
6. Model ST250LT009: HW ver 9WC14C, FW ver 1001SDMA

The configurations vary by storage capacity and customer-unique FW differences which do not involve FIPS services.

2.4 FIPS Approved Algorithms

Algorithm	Certificate Number
ASIC AES	#1392
Firmware AES	#1341
RSA	#648
SHA	#1223
FIPS 186-2 PRNG	#737

2.5 Self-Tests

Function Tested	Self-Test Type	Implementation	Failure Behaviour
ASIC AES	Power-On	Encrypt and Decrypt KAT performed	Enters FIPS Self Test Fail State
Firmware AES	Power-On	Encrypt and Decrypt KAT performed	Enters FIPS Self Test Fail State
RSA	Power-On	Verify KAT performed.	Enters FIPS Self Test Fail State
SHA-1	Power-On	Digest KAT performed	Enters FIPS Self Test Fail State
SHA-256	Power-On	Digest KAT performed	Enters FIPS Self Test Fail State
FIPS 186-2 PRNG	Power-On	PRNG KAT performed	Enters FIPS Self Test Fail State
Firmware Integrity Check	Power-On	16-bit CRC and ECC	Enters FW Integrity Error State
Firmware Load Check	Conditional: When new firmware is downloaded	RSA PKCS#1 signature verification of new firmware image is done before it can be loaded.	Firmware download is aborted.
FIPS 186-2 PRNG	Conditional: When a random number is generated	Newly generated random number is compared to the previously generated random number. Test fails if they are equal.	Enters FIPS Self Test Fail State.

2.6 FIPS 140 Approved Modes of Operation

Before the operator performs the Secure Initialization steps detailed in Section 7.1, the drive will operate in a non FIPS compliant mode (Security Operating Mode 0, i.e. SOM0). From this mode, the operator may choose to initialize the CM to operate in either the ATA Enhanced Security Mode (SOM1) or TCG Opal Security Mode (SOM2). Both of these modes are FIPS compliant modes and after setting up (configuring) the module per the Security Rules of this policy, an operator can switch between the modes. Details on these SOM modes and how they can transition from one to the other can be found in the product documentation.

The module's FIPS modes of operation are enforced through configuration and policy. Violating these ongoing policy restrictions (detailed in Section 7.2) would mean that one is no longer using the drive in a FIPS compliant mode of operation. The operator can determine if the CM is operating in a FIPS approved mode by invoking the Show Status service(refer to Section 4.1)

2.6.1 ATA Enhanced Security Mode (SOM1)

This mode provides services through industry-standard ATA commands, and TCG Opal commands addressed to the TCG Admin SP. Some of the services are based on the ATA Security Feature set but with vendor-unique extensions (e.g. encryption of user data on media). Other services are based on the TCG Opal commands. To operate in SOM1, the ATA User must do a Set PIN from SOM0 mode. This mode corresponds to having a deactivated TCG Opal Locking SP.

SOM1 implements the Master and User roles as defined in ATA. The ATA security lock / unlock states correspond to operator authentication for the Read / Write data services (which use an internal AES 128-bit key for encryption and decryption of data written to and read from the drive media respectively). In addition, a "Drive Owner" CO role is provided, which can enable or disable access to the FW download service for FW upgrade. Additionally, a cryptographic erase service is provided to the Master and User roles through the ATA Security Erase Unit commands. The FW download service (ATA Download

Microcode command) provides a FIPS-compliant FW load test by verifying the code's embedded 2048-bit RSA signature.

2.6.2 TCG Opal Security Mode (SOM2)

This mode provides services through industry-standard ATA commands, TCG Opal commands addressed to the TCG Admin SP, and TCG Opal commands addressed to the TCG Locking SP. It provides all of the services of the ATA Enhanced Security Mode as well as additional features through TCG Opal commands. Some ATA Security commands are disabled in this mode and their functionality is provided through the TCG Opal commands. To operate in SOM2, the Drive Owner must invoke the Activate method on the Locking SP from SOM0 mode.

One of the fundamental differences in this Mode is the capability to have multiple Users with independent access control to read/write/erase independent data areas (LBA ranges). Note that by default there is a single "Global Range" that encompasses the whole user data area.

In addition to the Drive Owner and User(s) roles, this mode implements a CO role (Admins) to administer the additional features. These features include:

- Enable/disable additional Users
- Create and configure multiple LBA Ranges
- Assign access control of Users to LBA Ranges
- Lock/unlock LBA Ranges
- Erase LBA Ranges using Cryptographic Erase
- MBR Shadowing

2.7 User Data Cryptographic Erase Methods

Since all user data is encrypted / decrypted by the CM for storage / retrieval on the drive media, the data can be erased using a cryptographic method. The data is effectively erased by changing the encryption key (MEK). Thus, the FIPS 140 key management capability "zeroization" of the key erases all the user data. This capability is available through both FIPS modes. Of course the user data can also be erased by overwriting, but this can be a long operation on high capacity drives.
Other FIPS services can be used to erase all the other private keys and CSPs (see Section 2.8).

2.8 Revert SP Methods

In either SOM1 or SOM2 modes, the TCG Revert SP method may be invoked to transition the CM into SOM0 (non-FIPS compliant) mode. This corresponds to the Exit FIPS Mode service and is akin to a "restore to factory defaults" operation. This operation also provides a means to zeroize keys and CSPs. Subsequently, the CM has to be re-initialized before it can return to a FIPS compliant mode of operation (i.e. SOM1 or SOM2). This Revert SP method may be invoked by the Drive Owner, Admins or an unauthenticated role using the public PSID value.

2.9 Shadow MBR (in SOM2 Only)

In SOM2, the CM provides a means for the host to remap a User Data LBA range to a "Shadow" area; this is called "Shadow MBR". The data in this area is not encrypted, thus read/write operations to this band do not use the User Data Read/Write service.

To enable this feature, the host application issues a TCG Set Method to the MBRControl Table in the Locking SP.

Further details on this feature can be found in the TCG Opal documentation (4).

3 Identification and Authentication (I&A) Policy

3.1 Operator Roles

Note: The following identifies the CO and User roles with a *general* description of the purposes. For further details of the services performed by each role in each FIPS mode, see section 4.1.

3.1.1 Crypto Officer Roles

3.1.1.1 Drive Owner

This CO role corresponds to the SID (Secure ID) Authority on the Admin SP as defined in Opal SSC [4]. This role is used to transition the CM to TCG Opal Security Mode or to download a new FW image. Note: only a FIPS validated firmware version can be loaded to the module. Otherwise, the module is not operating in FIPS mode.

3.1.1.2 Admins (1-4) (TCG Opal Security Mode (SOM2) Only)

This CO role for TCG Opal Security Mode corresponds to the same named Authority on the Locking SP as defined in Opal SSC [4]. This role is used to enable/disable Users, create and delete data regions (LBA Ranges), set LBA Range attributes, lock/unlock LBA Ranges and erase LBA Ranges (by zeroizing the MEK with the Cryptographic Erase service).

3.1.2 User Roles

3.1.2.1 User (1) – SOM1, Users (1-16) – SOM2

This role can unlock (and also lock) the drive so that an operator can read and write data to the drive. This role can also call the Cryptographic Erase service.

When operating in TCG Opal Security Mode, there can be up to 16 separate Users (User IDs) and the role corresponds to the same named TCG Authority on the Locking SP. The Admin role enables Users and assigns them read/write/erase access to LBA ranges.

3.1.2.2 Master (ATA Enhanced Security Mode (SOM1) Only)

This role corresponds to the same named role as defined in ATA [7]. This role only provides a backup authentication to the ATA User and does not have access to administration services beyond those of the ATA User role.

3.1.3 Unauthenticated Role

This role can perform the Show Status service.

If the operator has physical access to the drive, this role can also reset the module with a power cycle (which results in POSTs) as well as configure the jumper block to control the interface speed between the host and drive (a non-security relevant service). This role can also use the public PSID value to invoke the Exit FIPS Mode service.

3.2 Authentication

3.2.1 Authentication Types

Some operator roles have role-based authentication and others have identity-based authentication. For example, the Drive Owner role uses role-based authentication as there is only one ID and one PIN. In TCG Opal Security Mode, the CM has up to 4 Admin and 16 User operators. Each of these operators is assigned a unique ID to which a PIN is associated, thus this provides identity-based authentication.

For some services the authentication is performed in a separate associated service; e.g. the Read Unlock service is the authentication for subsequent User Data Read service. If the User Data Read service is attempted without prior authentication then the command will fail.

For authentication using the TCG interface, the operator and PIN can be provided in the StartSession method itself. Alternatively, an operator may use the Authenticate method to authenticate to a role after a Session has been started. Authentications will persist until the session is closed.

3.2.2 Authentication in ATA Enhanced Security Mode

In ATA Enhanced Security Mode, Master and User operator authentication is provided through a PIN provided in the ATA Security command [7]. In the event of authentication failure, the ATA command will abort, and subsequent read/write services will abort. A password attempt counter is implemented as specified in ATA, which when reached, blocks Master/User service authentication (with command abort), until the module is reset (Unblock PIN service).

Depending on a parameter of the Set PIN service for the User password, the User services may or may not be fully extended to the Master role. If the Master Password Capability is set to “High”, then either role can access the same services. Otherwise the Master role only has access to the erase service.

Drive Owner authentication for the Set PIN and Enable/Disable FW Download services is provided through the TCG StartSession or Authenticate to Admin SP.

3.2.3 Authentication in TCG Opal Security Mode

Operator authentication is provided via the TCG StartSession or Authenticate methods. The host application can have only a single session open at a time. During a session the application can invoke services for which the authenticated operator has access control. Note that a security rule of the CM is that the host must not authenticate to more than one operator (TCG authority) in a session.

For some services the host application will authenticate to the “Anybody” authority which does not have a private credential. Therefore these operations are effectively unauthenticated services.

3.2.4 Authentication Mechanism, Data and Strength

Operator authentication with PINs is implemented by hashing the operator input value and comparing it to the stored hash of the assigned PIN. The PINs have a retry attribute (“TryLimit”) that controls the number of unsuccessful attempts before the authentication is blocked until a module reset. The PINs have a maximum length of 32 bytes.
Per the policy security rules, the minimum PIN length is 4 bytes (Rule 4 in Section 7.1). This gives a probability of $1/2^{32}$ of guessing the PIN in a single random attempt. This easily meets the FIPS 140 authentication strength requirements of less than 1/1,000,000.
Each authentication attempt takes 30ms on average to complete. This means that approximately {(60*1000)/30} attempts can be made in one minute. Thus the probability of multiple random attempts to succeed in one minute is $2000/2^{32}$. This is significantly lower than the FIPS requirement of 1/100,000.

3.2.5 Personalizing Authentication Data

The initial value for SID is a manufactured value (mSID). This is a device-unique, 32-byte, public value. The Security Rules (Section 7) for the CM requires that the PIN values must be “personalized” to private values using the “Set PIN” service. Note that for SOM1, setting the User PIN also sets the Drive Owner PIN to the same value; the Drive Owner PIN can be set to a different value with the TCG Set Method.

4 Access Control Policy

4.1 Services

The following tables represent the FIPS 140 services for each FIPS Approved Mode in terms of the Approved Security Functions and operator access control. Note the following:

- Use of the services described below is only compliant if the module is in the noted Approved mode.
- Underlying security functions used by higher level algorithms are not represented (e.g. hashing as part of asymmetric key)
- Operator authentication is not represented in this table.
- Some security functions listed are used solely to protect / encrypt keys and CSPs.
- Service input and output details are defined by the TCG and ATA standards.
- Unauthenticated services (e.g. Show Status) do not provide access to private keys or CSPs.
- * Some services have indirect access control provided through enable / disable or lock / unlock services used by an authenticated operator; e.g. User data read / write.
- If the Operator value contains “opt” then the access is dependent on the module setup (see 3.2.2).

Table 1.1 - FIPS 140 Authenticated Services – SOM1

Service Name	Description	Operator Access Control	Security Function	Command(s)/Event(s)
Set PIN	Change operator authentication data. Note: Setting the User PIN also sets the Drive Owner PIN.	Master*, User*, Drive Owner	Hashing	ATA SECURITY SET PASSWORD, TCG Set Method
Lock / Unlock FW Download	Enable / Disable FW Download Service	Drive Owner	None	TCG Set Method
Firmware Download	Load complete firmware image. If the self-test of the code load passes then the device will run with the new code.	None**	Asymmetric Key	ATA DOWNLOAD MICROCODE
Unlock User Data	Enable user data read/write and Set PIN services.	User (opt. Master)	Symmetric Key (to unwrap MEK)	ATA SECURITY UNLOCK
User Data Read / Write	Encryption / decryption of user data.	None*	Symmetric Key	ATA Read / Write Commands
Cryptographic Erase	Erase user data through cryptographic means: by zeroizing the encryption key and the User PIN. Note: FIPS mode is exited.	Master, User	RNG	ATA SECURITY ERASE PREPARE + ATA SECURITY ERASE UNIT
Exit FIPS Mode	Exit ATA Enhanced Security Mode (SOM1). Note: CM will enter SOM0.	User* (opt. Master*), Drive Owner	RNG, Hashing, Symmetric Key	• ATA SECURITY DISABLE PASSWORD • ATA SECURITY ERASE PREPARE + SECURITY ERASE UNIT • TCG AdminSPObj.Revert()

Table 1.2 - FIPS 140 Unauthenticated Services – SOM1

Service Name	Description	Operator Access Control	Security Function	Command(s)/Event(s)
Unblock PIN	Reset Master and User password attempt counter.	None	None	POR
Show Status	Reports if CM is in a FIPS approved mode.	None	None	ATA IDENTIFY DEVICE Word 128 Bit 1 = 1 (Security Enabled)
Reset Module	Runs POSTs and zeroizes key & CSP RAM storage.	None	None	POR
Disable Services	Disables ATA Security commands until POR	None	None	ATA SECURITY FREEZE LOCK
Exit FIPS Mode	Exit ATA Enhanced Security Mode (SOM1). Note: CM will enter SOM0.	None (using PSID)	None	• TCG AdminSP.RevertSP()

*Security has to be Unlocked
**FW Download has to be Unlocked

Table 2.1 - FIPS 140 Authenticated Services – SOM2

Service Name	Description	Operator Access Control	Security Function	Command(s)/Event(s)
Set PIN	Change operator authentication data. Note: Admins can set PINs for any User or Admin.	Admin1-4, User1-16, Drive Owner	Hashing	TCG Set Method
Lock / Unlock FW Download Port	Enable / Disable FW Download Service	Drive Owner	None	TCG Set Method
Firmware Download	Load complete firmware image. If the self-test of the code load passes then the device will run with the new code.	None**	Asymmetric Key	ATA DOWNLOAD MICROCODE
Enable / Disable Admin(2-4), User(s)	Enable / Disable an Admin or User Authority.	Admin1-4	None	TCG Set Method
Set Range Attributes	Set the location, size, locking and User access rights of the LBA range.	Admin1-4	None	TCG Set Method
Lock / Unlock User Data Range for Read and/or Write	Block or allow read (decrypt) / write (encrypt) of user data in a range.	Admin1-4, User1-16	None	TCG Set Method, ATA SECURITY UNLOCK
User Data Read / Write	Encryption / decryption of user data to/from a LBA range. Access control to this service is provided through Lock / Unlock User Data Range.	None*	Symmetric Key	ATA Read / Write Commands
Cryptographic Erase	Erase user data in an LBA range by cryptographic means: changing the encryption key.	Admin1-4, User1-16	RNG, Symmetric Key	TCG GenKey Method
Exit FIPS Mode	Exit TCG Opal Security Mode (SOM2). Note: CM will enter SOM0.	Drive Owner, Admin1-4	RNG, Hashing, Symmetric Key	• TCG AdminSP.RevertSP() • TCG AdminSPObj.Revert() • TCG LockingSPObj.Revert()

Table 2.2 - FIPS 140 Unauthenticated Services – SOM2

Service Name	Description	Operator Access Control	Security Function	Command(s)/Event(s)
Unblock PIN	Resets password attempt counters.	None	None	POR
Show Status	Reports if CM is in a FIPS approved mode.	None	None	TCG Level 0 Discovery. Drive Security Life Cycle State = 0x80 (Use State) **AND** SecurityOperatingMode in Admin SP = 0x02 (SOM2)
Reset Module	Runs POSTs and zeroizes keys & CSPs in RAM	None	None	POR
Exit FIPS Mode	Exit TCG Opal Security Mode (SOM2). Note: CM will enter SOM0.	None (using PSID)	None	• LockingSP.RevertSP()

*Data Range has to be Unlocked
**FW Download has to be Unlocked

4.2 Cryptographic Keys and CSPs

The following table defines the keys / CSPs and the operators / services which use them. It also describes the lifecycle of these data items in terms of initial value, input / output, storage and zeroization. Note the following:

- Lifecycle – Initial Value represents the value before the required Security Rules for module setup have been completed. An initial value of "undefined" means that there is no way to authenticate to the associated operator until it has been set by the operator.
- The use of PIN CSPs for authentication is implied by the operator access control.
- The Set PIN service is represented in this table even though generally it is only used at module setup.
- All non-volatile storage of keys and CSPs is in the system area of the drive media to which there is no logical or physical access from outside of the module.
- Non-critical security parameters are not represented in this table.
- Read access of private values are internal only to the CM and are thus not represented in this table.
- There is no security-relevant audit feature.

Name	Mode (ATA / TCG / Both)	Description	Type (Pub / Priv, key / CSP (e.g. PIN)), size	Operator Role	Services Used In	Access (W, X)	Lifecycle				
							Initial Value	Storage	Storage Form (Plaintext / Encrypted)	Entry / Output	Zeroization
SID (Secure ID), aka Drive Owner PIN	Both	Auth. Data	Private, PIN, 32 bytes	Drive Owner	Set PIN	W	MSID	Media (System Area)	SHA Digest	Electronic Input from Host No output	Revert Admin SP
Master, User Passwords	ATA	Auth. Data	Private, PIN, 32 bytes	None (subject to unlocked)	Set PIN	W	MSID (Master), Undefined (User)	Media (System Area)	SHA Digest	Electronic Input from Host No output	Revert Admin SP, Cryptographic Erase (User)
				Master, User	Unlock User Data	X					
				Master, User	Cryptographic Erase	X					
				Master, User	Exit FIPS Mode	X					
Master, User MEK	ATA	MEK mixed with PINs	Private, AES Key, 128 bits	Master, User	Unlock User Data	X	RNG generated during manufacturing	Media (System Area)	Obfuscated (considered plaintext for FIPS purposes)	None	Revert Admin SP, Cryptographic Erase
Admin1-4 Passwords	TCG	Admins Auth. Data	Private, PIN, 32 bytes	Admins	Set PIN	W	SID (Admin1), Undefined (Admin2-4)	Media (System Area)	SHA Digest	Electronic Input from Host No output	Revert
User1-16 Passwords	TCG	Users Auth. Data	Private, PIN, 32 bytes	Admins, Users	Set PIN	W	Undefined	Media (System Area)	SHA Digest	Electronic Input from Host No output	Revert
LBA Range MEKs	TCG	MEK mixed with MEKEK	Private, AES Key, 128 bits	Admins, Users	Unlock User Data	X	RNG generated during manufacturing	Media (System Area)	Encrypted	None	Revert, Cryptographic Erase
Seed Key (XKEY)	Both	RNG Key	Private, Hash Key, 64 bytes	None	Services which use the RNG (e.g. cryptographic erase)	X, W	Set to RNG state at each RNG usage	RAM	None	None	Reset
Seed	Both	RNG seed (entropy)	Private, Hash seed, 520 bytes	None	1st RNG use after POST	X	Entropy collected at power up	RAM	None	None	Reset
ORG0-0 - ORG0-3	Both	Firmware Load Test Signature Verify Key	Public, RSA Key, 2048 bits	Drive Owner (enable FW download)	FW Download	X	Public keys generated during manufacturing	Media (System Area)	Plaintext	None	None (Public)
MEKEK	TCG	Media Encryption Key Encryption Key	Private, AES Key, 128 bits	Admins, Users	Unlock User Data	X	RNG generated during manufacturing	Media (System Area)	Encrypted	None	Revert

4.3 Non-Critical Security Parameters

This section lists the security-related information which do not compromise the security of the module.

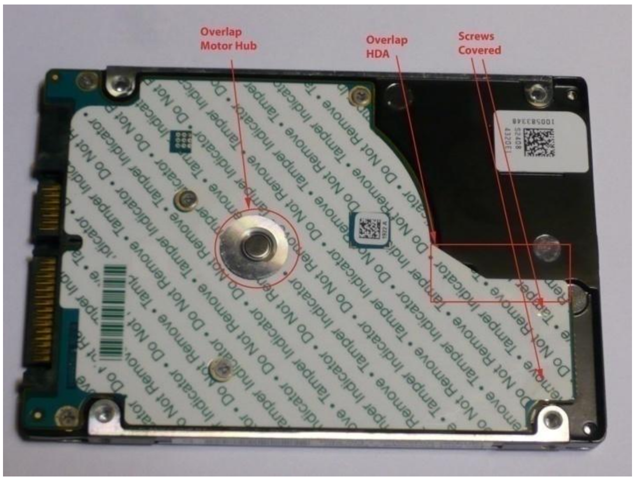
- AES IV (i.e. Initialization Vector)
  The CM HW AES IV (CBC mode) is derived for each read/write operation.
- PIN Retry Attributes – Tries, TryLimit and Persistence
  These parameters affect the handling of failed authentication attempts.
- PSID (Physical SID)
  This public drive-unique value is only used for the TCG Revert Admin SP method (i.e. Exit FIPS Mode service). This method will leave the CM in a non FIPS compliant "factory default" mode (SOM0) and will require a re-initialization for the CM to resume operation in a FIPS compliant mode.
- MSID (Manufactured SID)
  This drive-unique value is the manufactured default value for Drive Owner and Master roles.

5 Physical Security

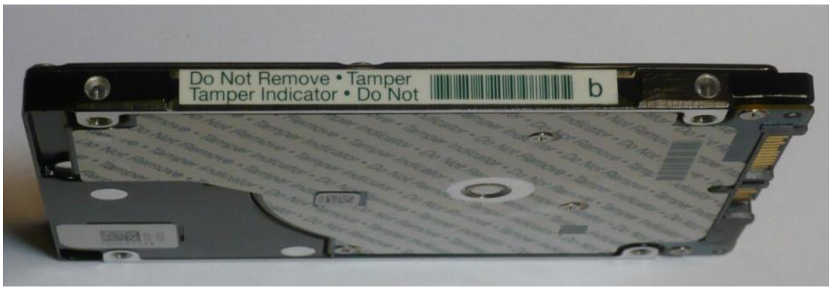
5.1 Mechanisms

The CM has the following physical security:

- Production-grade components with standard passivation
- Opaque, tamper-evident, security label on the exposed (back) side of the PCBA which prevents electronic design visibility and protects physical access to the electronics by board removal
- Tamper-evident security labels that prevent HDA cover removal for access or visibility to the media
- Exterior of the drive is opaque
- The tamper-evident labels cannot be penetrated or removed and reapplied without tamper-evidence
- The tamper-evident labels cannot be easily replicated with a low attack time



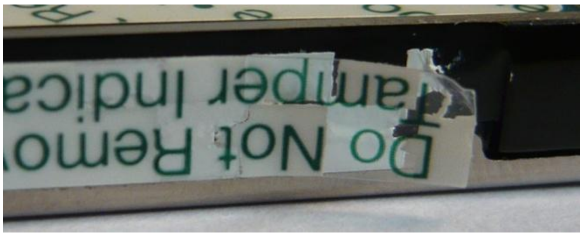
- Security labels on side of drive to provide tamper-evidence of HDA cover removal,

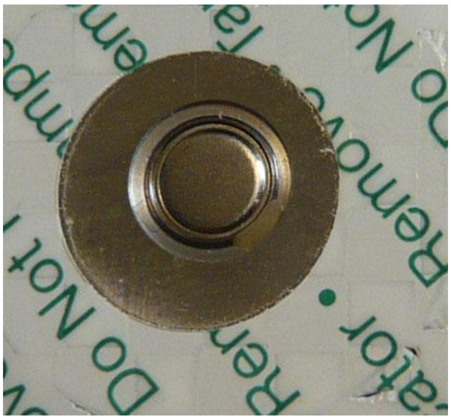


5.2 Operator Requirements

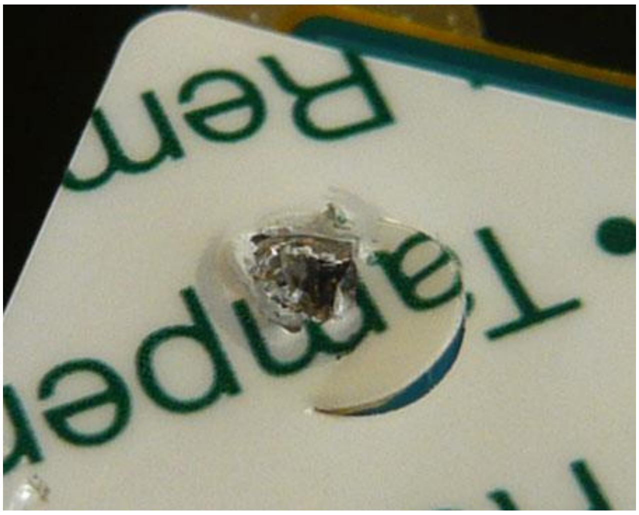
The operator is required to inspect the CM periodically for one or more of the following tamper evidence:

- Checkerboard pattern on security label or substrate





- Security label over screws at indicated locations is missing or penetrated,



- Text (including size, font, orientation) on security label does not match original,
- Security label cutouts do not match original.

Upon discovery of tamper evidence, the module should be removed from service.

6 Operational Environment

The FIPS 140-2 Area 6 Operational Environment requirements are not applicable because the CM operates in a "non-modifiable operational environment". That is, while the module is in operation the operational environment cannot be modified and no code can be added or deleted. FW can be upgraded (replaced) with a signed FW download operation. If the code download is successfully authenticated then the module will begin operating with the new code image.

7 Security Rules

7.1 Secure Initialization

The CM does not change mode across module resets. However, certain operations can result in exiting the FIPS Approved mode. In some of these exit scenarios (e.g. POST failure), the drive cannot be restored to FIPS mode and does not provide any FIPS services.

The following are the security rules for initialization and operation of the CM in a FIPS 140 compliant manner. Reference the appropriate sections of this document for details.

1. COs: At receipt of the product examine the shipping packaging and the product packaging to ensure it has not been accessed during shipping by the trusted courier.
2. COs and Users (either mode): At installation and periodically examine the physical security mechanisms for tamper evidence.
3. Transition the CM to one of the FIPS approved modes by doing one of the following:
   - ATA Mode (SOM1): User Set PIN.
   - TCG Opal (SOM2): Drive Owner executes Activate method on Locking SP
4. COs and Users: At installation, set all operator PINs applicable for the FIPS mode to private values of at least 4 bytes length:
   - ATA Mode (SOM1): Master and User. Drive Owner (optional).
   - TCG Opal (SOM2): Drive Owner, Admins and Users
5. Users: At installation and periodically confirm drive is in FIPS approved mode with the Show Status service.
6. Drive Owner: At installation, disable the "Makers" authority (using SID_Set_Makers ACE to the Admin SP). To query this setting, perform the Get method for the Makers authority on the Admin SP, specifying the "enabled" column.
7. At installation, the value of LockOnReset for FW Download must be set to "Power Cycle" and it must not be modified.

7.2 Ongoing Policy Restrictions

1. Prior to assuming a new role, close the current Session and start a new Session, or do a power-on reset, so that the previous authentication is cleared.
2. COs (Admins) for SOM2: If it is intended to have a band lock on module reset then set ReadLockEnabled and WriteLockEnabled to "True"; the default value is "False". If a band is configured with a value of False then the band is to be considered excluded from the module boundary.

8 Mitigation of Other Attacks Policy

The CM does not make claims to mitigate against other attacks beyond the scope of FIPS 140-2.