



# Seagate Secure® TCG Enterprise SSC Self-Encrypting Drives FIPS 140 Module

## Security Policy

### Security Level 2

Rev. 0.6 – January 09, 2015

Seagate Technology, LLC

## Table of Contents

1	Introduction .....	4
1.1	Scope .....	4
1.2	Security Levels.....	4
1.3	References .....	4
1.4	Acronyms .....	4
2	Cryptographic Module Description .....	6
2.1	Overview .....	6
2.2	Logical to Physical Port Mapping .....	6
2.3	Product Versions .....	6
2.4	FIPS Approved Algorithms .....	7
2.5	Self-Tests.....	7
2.6	FIPS 140 Approved Modes of Operation.....	8
2.6.1	TCG Security Mode.....	8
2.6.2	ATA Enhanced Security Mode.....	8
2.7	User Data Cryptographic Erase/Sanitize Methods.....	9
2.8	RevertSP Method .....	9
2.9	Show Status .....	9
3	Identification and Authentication (I&A) Policy.....	10
3.1	Operator Roles .....	10
3.1.1	Crypto Officer Roles.....	10
3.1.2	User Roles .....	10
3.1.3	Unauthenticated Role.....	10
3.2	Authentication .....	10
3.2.1	Authentication Types .....	10
3.2.2	Authentication in ATA Enhanced Security Mode .....	11
3.2.3	Authentication in TCG Security Mode .....	11
3.2.4	Authentication Mechanism, Data and Strength .....	11
3.2.5	Personalizing Authentication Data .....	11
4	Access Control Policy .....	12
4.1	Services .....	12
4.2	Cryptographic Keys and CSPs.....	15
5	Physical Security .....	17
5.1	Mechanisms.....	17
5.2	Operator Requirements .....	18
6	Operational Environment.....	20
7	Security Rules .....	20
7.1	Secure Initialization .....	20
7.2	Ongoing Policy Restrictions .....	20
8	Mitigation of Other Attacks Policy.....	20

---

## Table of Figures

Figure 1: Enterprise Capacity® 3.5,HDD v4 (SAS Interface).....	17
Figure 2: Enterprise Capacity® 3.5, HDD v4(SATA) .....	17
Figure 3: Enterprise Capacity® 3.5, HDD v4 (SAS/SATA interface) .....	18
Figure 4: Enterprise Capacity® 3.5, HDD v4 (SAS/SATA) Top Cover Temper Evidence .....	18
Figure 5: Enterprise Capacity® 3.5, HDD v4 (SAS/SATA) PCBA Temper Evidence .....	19
Figure 6: Enterprise Capacity® 3.5, HDD v4 (SAS/SATA) Screw covered by Security label.....	19

# 1 Introduction

## 1.1 Scope

This security policy applies to the FIPS 140-2 Cryptographic Module (CM) embedded in **Seagate Secure® TCG Enterprise SSC Self-Encrypting Drives**.

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

FIPS 140-2 Requirement Area	Security 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

The overall security level pursued for the cryptographic modules is Security Level 2.

## 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: Enterprise, Specification Version 1.0, Revision 3.00, January 10, 2011
5. TCG Storage Architecture Core Specification, Specification Version 1.0, Revision 0.9, May 24, 2007
6. TCG Storage Interface Interactions Specification, Specification Version 1.0
7. ATA-8 ACS
8. Serial ATA Rev 2.6 (SATA )
9. SCSI Primary Commands-4 Rev 15 (SPC-4)
10. SCSI Block Commands Rev15 (SBC-3)
11. Serial Attached SCSI-2 Rev 13 (SAS-2)

## 1.4 Acronyms

AES	Advanced Encryption Standard (FIPS 197)
ASIC	Application Specific Integrated Circuit
CBC	Cipher Block Chaining, an operational mode of AES
CM	Cryptographic Module
CO	Crypto-officer
CSP	Critical Security Parameter
DRBG	Deterministic Random Bit Generator
GCM	Galois/Counter Mode (SP800-38D)
HDA	Head and Disk Assembly
HDD	Hard Disk Drive
HMAC	Hash-based message authentication code

---

IV	Initialization Vector for encryption operation
LBA	Logical Block Address
KAT	Known Answer Test
MEK	Media Encryption Key
MSID	Manufactured SID, public drive-unique value that is used as default PIN, TCG term
POR	Power-on Reset (power cycle)
PN	Part Number(s)
POST	Power on Self-Test
PSID	Physical SID, public drive-unique value
RNG	Random Number Generator
SHA	Secure Hash Algorithm
SID	Security ID, PIN for Drive Owner CO role, TCG term
SoC	System-on-a-Chip
SP	Security Provider or Security Partition (TCG), also Security Policy (FIPS 140)

## 2 Cryptographic Module Description

### 2.1 Overview

The Seagate Secure® TCG Enterprise SSC Self-Encrypting Drives FIPS 140 Module is embodied in Seagate **Enterprise Capacity® HDD v4** Self-Encrypting Drives model disk drives. These products meet the performance requirements of the most demanding Enterprise applications. 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 bands and authenticated FW download. The services are provided through industry-standard TCG Enterprise SSC, SCSI and ATA protocols.

The CM has a multiple-chip embedded physical embodiment. The physical interface to the CM is a SATA or SAS connector. The logical interfaces are the industry-standard ATA (refer to Section 1.3, item 7), SCSI (refer to Section 1.3, items 9 & 10), TCG SWG (refer to Section 1.3, item 4), and Enterprise (refer to Section 1.3, item 4) protocols, carried on the SATA (refer to Section 1.3, item 8) or SAS (refer to Section 1.3, item 11) transport interface. 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 cryptographic boundary of the CM surrounds the entire drive unit, including all of its hardware, firmware, and electronics.

### 2.2 Logical to Physical Port Mapping

For HW versions that support ATA protocol (defined in Section 2.3):

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

For HW versions that support SCSI protocol (defined in Section 2.3):

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

### 2.3 Product Versions

The following models and hardware versions (PNs) are validated with the following FW versions:

- Enterprise Capacity® HDD v4, 3.5-Inch, 7K-RPM, SAS Interface, 6000 GB,
  - 6000 GB: ST6000NM0104 [1]
  - 6000 GB: ST6000NM0114 [1]
  - FW Versions: 0001 [1]
- Enterprise Capacity® HDD v4, 3.5-Inch, 7K-RPM, SATA Interface, 6000 GB,
  - 6000 GB: ST6000NM0084 [2]
  - FW Versions: ZZZZ [2]

HW versions that support SCSI protocol are:

- Enterprise Capacity® HDD v4, 3.5 inch, 7K-RPM, SAS Interface, 6000GB

HW version that supports ATA protocol is:

- Enterprise Capacity® HDD v4, 3.5 inch, 7K-RPM, SATA Interface, 6000GB

The photographs on the title page consist of representative HW versions of both models mentioned in this section.

## 2.4 FIPS Approved Algorithms

Algorithm	Certificate Number
ASIC AES	#2842 , #2803
ASIC SHA-256	#2383 , #2352
Firmware AES	#1343
Firmware AES-GCM	#2841
RSA	#1021
SHA	#1225
Firmware HMAC	#1597
800-90 DRBG	#62
800-132 PBKDF	Vendor Affirmed
800-38F Key Wrap using AES-256 Cert.# 1343 as the underlying encryption algorithm.	#2947
NDRNG	Non-Approved but Allowed

ASIC AES Certificate #2842 is applicable for HW version that supports SCSI protocol (defined in Section 2.3).

ASIC AES Certificate #2803 is applicable for HW version that supports ATA protocol (defined in Section 2.3).

ASIC SHA-256 Certificate #2383 is applicable for HW versions that support SCSI protocol (defined in Section 2.3).

ASIC SHA-256 Certificate #2352 is applicable for HW versions that support ATA protocol (defined in Section 2.3).

For cryptographic algorithms such as AES, SHA and RSA, the CM only uses AES-256, SHA-256 and RSA-2048.

The remaining certificates are applicable for all HW versions of this Security Policy.

## 2.5 Self-Tests

Function Tested	Self-Test Type	Implementation	Failure Behavior
ASIC AES	Power-On	Encrypt and Decrypt KAT performed	Enters FIPS Self Test Error State and rejects host commands with error code.
ASIC SHA-256	Power-On	Digest KAT performed	Enters FIPS Self Test Error State and rejects host commands with error code.
Firmware AES	Power-On	Encrypt and Decrypt KAT performed	Enters FIPS Self Test Error State and rejects host commands with error code.
Firmware GCM	Power-On	Encrypt and Decrypt KAT performed	Enters FIPS Self Test Error State and rejects host commands with error code.
RSA	Power-On	Sign Verify KAT performed	Enters FIPS Self Test Error State and rejects host commands with error code.

Firmware HMAC	Power-On	Digest KAT performed	Enters FIPS Self Test Error State and rejects host commands with error code.
800-90 DRBG	Power-On	DRBG KAT performed	Enters FIPS Self Test Error State and rejects host commands with error code.
Firmware Integrity Check	Power-On	Signature Verification	Enters FW Integrity Error State and does not become operationally ready.
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.
800-90 DRBG	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 Error State and rejects host commands with error code.
Firmware SP 800-132 PBKDF	Power-On	PBKDF KAT performed	Enters FIPS Self Test Fail State
Non-Approved but Allowed NDRNG	Conditional: When a non-Approved but Allowed 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 Error State and rejects host commands with error code.

## 2.6 FIPS 140 Approved Modes of Operation

Before the operator performs Secure Initialization steps detailed in Section 7.1, the drive will operate in a non-FIPS Approved mode (uninitialized state).

For CM that support SCSI protocol on the SAS interface, the operator can only initialize the CM as “TCG Security” mode. For CM that support ATA protocol on the SATA interface, the operator may choose to initialize the CM to operate in either “TCG Security” or “ATA Enhanced Security” mode. After setting up (configuring) the module per the Security Rules of this policy, the CM is always in Approved mode of operation except when a critical failure has been detected, when any ‘Exit FIPS mode’ services are invoked, or when the module is not in ‘Use’ state. For CM that supports both Approved modes, an operator can switch the CM between these Approved modes of operation and to do so, the CM must transition to the uninitialized state (via ‘Exit FIPS mode’ service) which results in zeroization of keys and CSPs.

The module’s FIPS modes of operation are enforced through configuration and policy. Violating the Security rules and ongoing policy restrictions (detailed in Section 7.1 and Section 7.2) would mean that one is no longer using the drive in a FIPS Approved mode of operation.

Sections 2.6.1 and 2.6.2 describe the differences between the 2 modes.

### 2.6.1 TCG Security Mode

This mode has 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 (EraseMaster) to administer the above capability.

### 2.6.2 ATA Enhanced Security Mode

This mode implements the Master and User roles, and lock/unlock/erase as defined in the ATA Security feature set as well as Sanitize feature set in ATA protocol. There is a single user data region which can be read/written/erase with one encryption key.



---

## 2.7 User Data Cryptographic Erase/Sanitize Methods

Since all user data is encrypted / decrypted by the CM for storage / retrieval on the drive media, the data can be erased/sanitized using cryptographic methods. The data is effectively erased/sanitized by changing the media encryption key (MEK). Thus, the FIPS 140 key management capability “zeroization” of the key effectively erases all the user data in that read operations will decrypt with a different key value and thus the data is not returned as it was written.

Other FIPS service can be used to erase all the other private keys and CSPs (see Section 2.8).

## 2.8 RevertSP Method

The TCG RevertSP method may be invoked to transition the CM back to the manufactured state (uninitialized). 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 Approved mode of operation. This RevertSP method is invoked as an unauthenticated service by virtue of the use of a public credential (PSID).

## 2.9 Show Status

Show status service (refer to Section 4.1) can be used to determine if the drive is operational under the security constraints of FIPS. For this purpose TCG Level 0 Discovery mechanism and TCG Get method are utilized.

TCG Level 0 Discovery mechanism maybe invoked by the operator to know if drive in “use” or security “fail” state. If the Drive Security Life Cycle State is 0x80 then drive is in Use State i.e. security is operational. If the Drive Security Life Cycle State is 0xFF the drive is in security Fail State i.e. drive is not operational in terms of FIPS services.

In addition, the TCG Get method can be used to retrieve the approved modes of operation value. The values of 0x01 or 0x02 correspond to ATA Enhanced Security Mode and TCG Security Mode respectively. The value 0x00 indicates the CM is in the uninitialized state.

## 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 Enterprise SSC [refer to Section 1.3, item 4]. This role is used to transition the CM to TCG Security Mode (applicable for SATA command interface) and 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 EraseMaster (TCG Security Mode)

This CO role corresponds to same named role as defined in Enterprise SSC [refer to Section 1.3, item 4]. This role is used to enable/disable User roles, and erase user data region (LBA band). An operator is authenticated to this role with role-based authentication.

#### 3.1.2 User Roles

##### 3.1.2.1 BandMasters (0-15) (TCG Security Mode)

This user role corresponds to the same named role as defined in Enterprise SSC [refer to Section 1.3, item 4]. This role is used to lock/unlock and configure a user data band (“LBA band”) for read/write access.

A CM can be configured to support up to 16 user data bands, which are controlled by their respective BandMaster credentials. By default 2 user bands are enabled. BandMasters are enabled/disabled using the EraseMaster role. An operator is authenticated to the BandMaster role with identity-based authentication. If a user data band is erased (EraseMaster service) then the BandMaster PIN is reset to MSID.

##### 3.1.2.2 User (ATA Enhanced Security Mode)

This role corresponds to the same named role as defined in ATA [refer to Section 1.3, item 7]. It can unlock (and also lock) the drive so that an operator can read and write data to the drive. This role can also use the Cryptographic Erase service.

##### 3.1.2.3 Master (ATA Enhanced Security Mode)

This role corresponds to the same named role as defined in ATA [refer to Section 1.3, item 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). This role can also use the public PSID value to invoke the Exit FIPS Mode service. See section 4.1 for details.

### 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 Security Mode, the CM has up to 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.

### 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 [refer to Section 1.3, item 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 Authenticate to Admin SP.

### 3.2.3 Authentication in TCG Security Mode

Operator authentication is provided within a TCG session. The host application can have only a single session open at a time. Authentication of an operator, using the TCG interface, uses the Authenticate method to authenticate to a role after a session has been started. Authentications will persist until the session is closed.

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 the Show Status the host application will authenticate to the “Anybody” authority which does not have a private credential. Therefore this operation is effectively an unauthenticated service.

### 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 3 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  $1/1,000,000$ .

In TCG interface, each failed authentication attempt takes a minimum of 15ms to complete. Thus a maximum of  $\{(60*1000)/15\}$  attempts can be processed in one minute. Thus the probability of multiple random attempts to succeed in one minute is  $4000/2^{32}$ . This is significantly lower than the FIPS requirement of  $1/100,000$ .

In ATA security interface, the PIN blocking feature limits the number of unsuccessful attempts to 5 (it “unblocks” with module reset) and the minimum time for a module reset is about 15 seconds (about 4/min). Thus the probability of multiple random attempts to succeed is  $4/2^{32}$ . This is significantly lower than the FIPS requirement of  $1/100,000$ .

### 3.2.5 Personalizing Authentication Data

The initial value for SID and various other PINs 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 ATA Enhanced Security Mode, 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.

Hardware versions that support ATA protocol (defined in Section 2.3) provide services indicated in Tables 1.1 and 1.2 (when in TCG Security Mode), Tables 2.1 and 2.2 (when in ATA Enhanced Security Mode).

Hardware versions that support SCSI protocol (defined in Section 2.3) provide services in Tables 1.1 and 1.2 (when in TCG Security Mode).

For cryptographic algorithm certificates and hardware version association, refer to Section 2.4.

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, SCSI 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 “optional” then the access is dependent on the module setup (see Section 3.2.2).

**Table 1.1 - FIPS 140 Authenticated Services  
(TCG Security Mode)**

Service Name	Description	Operator Access Control	Security Function	Command(s)/Event(s)
Set PIN	Change operator authentication data.	EraseMaster BandMasters, Drive Owner	Hashing	TCG Set Method
Firmware Download	Enable/Disable FW download and load complete firmware image. If the self-test of the code load passes then the device will run with the new code.	Drive Owner**	Asymmetric Key	TCG Set Method, SCSI Write Buffer, ATA DOWNLOAD MICROCODE
Enable / Disable BandMasters	Enable / Disable a User Authority.	EraseMaster	None	TCG Set Method
Set Range Attributes	Set the location, size, and locking attributes of the LBA range.	BandMasters	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.	BandMasters	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	SCSI Read, Write Commands ATA Read, Write Commands
Cryptographic Erase	Erase user data in an LBA range by cryptographic means: changing the encryption key. BandMaster PIN is also reset.	EraseMaster,	DRBG, Symmetric Key	TCG Erase Method

**Table 1.2 - FIPS 140 Unauthenticated Services  
(TCG Security Mode)**

Service Name	Description	Operator Access Control	Security Function	Command(s)/Event(s)
Show Status	Reports if the CM is operational in terms of FIPS services and approved mode of operation value.	None	None	TCG Level 0 Discovery, TCG Get Method Drive Security Life Cycle State =0x80(Use State) and, Approved mode of operation value =0x02.
Reset Module	Runs POSTs and zeroizes key & CSP RAM.	None	None	POR
DRBG Generate Bytes	Returns an SP 800-90 DRBG Random Number of 256 bytes	None	None	TCG Random()
Exit FIPS Mode	Exit Approved Mode of Operation. Note: CM will enter non-FIPS mode.	None (using PSID)	None	TCG AdminSP.RevertSP()
FIPS 140 Compliance Descriptor	Reports FIPS 140 Revision, Overall Security Level, Hardware and Firmware revisions and Module name	None	None	SCSI SECURITY PROTOCOL IN – Protocol 0 ATA TRUSTED RECEIVE – Protocol 0

<b>Table 2.1- FIPS 140 Services – Authenticated Services (ATA Enhanced Security Mode)</b>				
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.	User (optional Master), Drive Owner	Hashing	ATA SECURITY SET PASSWORD, TCG Set Method
Firmware Download	Enable / Disable FW Download and load complete firmware image. If the self-test of the code load passes then the device will run with the new code.	Drive Owner**	Asymmetric Key	TCG Set Method, ATA DOWNLOAD MICROCODE
Unlock User Data	Enable user data read/write and Set PIN services.	User (optional 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	DRBG	ATA SECURITY ERASE PREPARE + ATA SECURITY ERASE UNIT
Sanitize	Sanitize user data through cryptographic means: by zeroizing the encryption key.	None*	DRBG	ATA CRYPTO SCRAMBLE
Disable Services	Disables ATA Security commands until POR	None*	None	ATA SECURITY FREEZE LOCK
Exit FIPS Mode	Exit Approved Mode of Operation. Note: CM will enter non-FIPS mode.	User(optional Master)	DRBG, Hashing, Symmetric Key	ATA SECURITY DISABLE PASSWORD, ATA SECURITY ERASE PREPARE + ATA SECURITY ERASE UNIT

<b>Table 2.2 - FIPS 140 Unauthenticated Services (ATA Enhanced Security Mode)</b>				
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 the CM is operational in terms of FIPS services and approved mode of operation value.	None	None	TCG Level 0 Discovery, TCG Get Method Drive Security Life Cycle State=0x80(Use State) and, Approved mode of operation value=0x01.
Reset Module	Runs POSTs and zeroizes key & CSP RAM storage.	None	None	POR
Exit FIPS Mode	Exit Approved Mode of Operation. Note: CM will enter non-FIPS mode.	None (using PSID)	None	TCG AdminSP.RevertSP()
FIPS 140 Compliance Descriptor	Reports FIPS 140 Revision, Overall Security Level, Hardware and Firmware revisions and Module name	None	None	ATA TRUSTED RECEIVE – Protocol 0

\*Security has to be Unlocked

\*\*FW Download Port has to be Unlocked

---

## 4.2 Cryptographic Keys and CSPs

The following table defines the keys / CSPs and the operators / services which use them. Note the following:

- 
- 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.
- The module uses SP 800-90 DRBG and adopts Hash\_DRBG mechanism.
- 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.

Table 3 – “Key Management”						
Name	Mode (ATA / TCG / Both)	Description	Type (Pub / Priv, key / CSP (e.g. PIN)), size	Operator Role	Services Used In	Access **(W, X)
SID (Secure ID), aka Drive Owner PIN	Both	Auth. Data	Private, PIN, 32 bytes	Drive Owner	Set PIN	W
Master, User Passwords	ATA	Auth. Data	Private, PIN, 32 bytes	None (subject to unlocked)	Set PIN	W
				Master, User	Unlock User Data	X
				Master, User	Cryptographic Erase	X
				Master, User	Sanitize	X
				Master, User	Exit FIPS Mode	X
Master, User MEK	ATA	Media Encryption Key	Private, AES Key, 512 bits	Master, User	Unlock User Data	X
EraseMaster	TCG	EraseMaster, Auth Data	Private, PIN, 32 bytes	EraseMaster	SetPIN	W
					Cryptographic Erase	X
BandMasters (0-15) Passwords	TCG	Users Auth. Data	Private, PIN, 32 bytes	BandMasters	Set PIN	W
					Unlock User Data	X
LBA Range MEKs	TCG	MEK (per LBA band)	Private, AES Key, 512 bits	Users	Unlock User Data	X
Entropy Input String	Both	*Input to a DRBG mechanism of a string of bits that contains entropy	Private, 520 bytes	None	Services which use the DRBG (e.g; cryptographic erase, sanitize)	X
Seed	Both	*String of bits that is used as input to a DRBG mechanism	Private, Hash seed, 544 bytes	None	Services which use the DRBG (e.g. cryptographic erase, sanitize)	X
Internal State	Both	*Collection of stored information about DRBG instantiation	Private, V and C	None	Services which uses the DRBG (e.g. cryptographic erase, sanitize)	X
ORG0-0 - ORG0-1	Both	Firmware Load Test Signature Verify Key	Public, RSA Key, 2048 bits	Drive Owner (enable FW download)	FW Download	X
MEKEK (MEK Encryption Key)	Both	This key is used to protect the MEK	Private, AES Key, 32 bytes	Master, User, BandMasters, EraseMaster	Unlock User Data, Cryptographic Erase, Set PIN	W, X
Master Key	Both	This key is used to protect the MEKEK	Private, AES Key, 32 bytes	Master, User, BandMasters, EraseMaster	Unlock User Data, Cryptographic Erase, Set PIN	W,X
CSPSK	Both	Used internally within PBKDF	Private, AES Key, 32 bytes	Master, User, BandMasters, EraseMaster	Unlock User Data, Cryptographic Erase, Set PIN	W, X
HMAC Key	Both	Used internally within PBKDF	Private, HMAC Key, 32 bytes	Master, User, BandMasters, EraseMaster	Unlock User Data, Cryptographic Erase, Set PIN	W, X

\* Source: Section 4 Terms and Definitions of NIST Special Publication 800-90

\*\* W - Write access is allowed, X - Execute access is allowed





## 5 Physical Security

### 5.1 Mechanisms

The CM has the following physical security:

- Production-grade components with standard passivation
  - One opaque, tamper-evident security label (TEL) on the exposed (back) side of the PCBA applied by Seagate manufacturing prevents electronic design visibility and protects physical access to the electronics by board removal
  - Two tamper-evident security labels applied by Seagate manufacturing prevent top and bottom 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 label on PCBA of drive to provide tamper-evidence of PCBA removal



Figure 1: Enterprise Capacity® 3.5,HDD v4 (SAS Interface)



Figure 2: Enterprise Capacity® 3.5, HDD v4(SATA)

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



Figure 3: Enterprise Capacity® 3.5, HDD v4 (SAS/SATA interface)

## 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

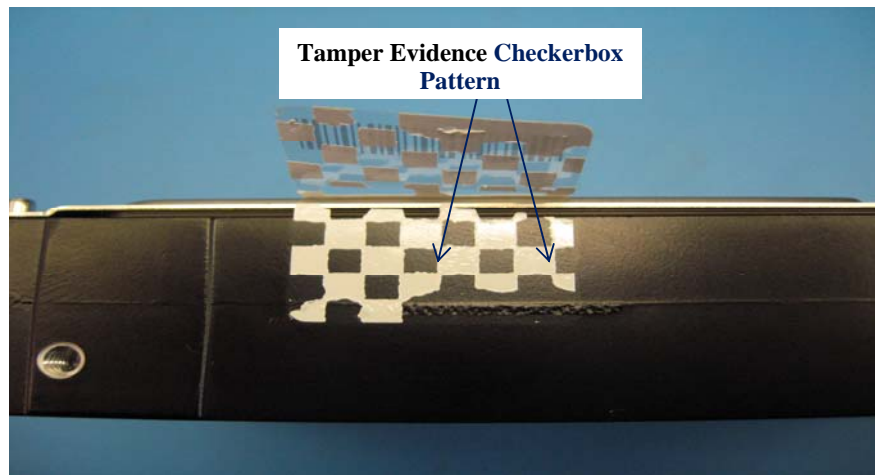


Figure 4: Enterprise Capacity® 3.5, HDD v4 (SAS/SATA) Top Cover Tamper Evidence

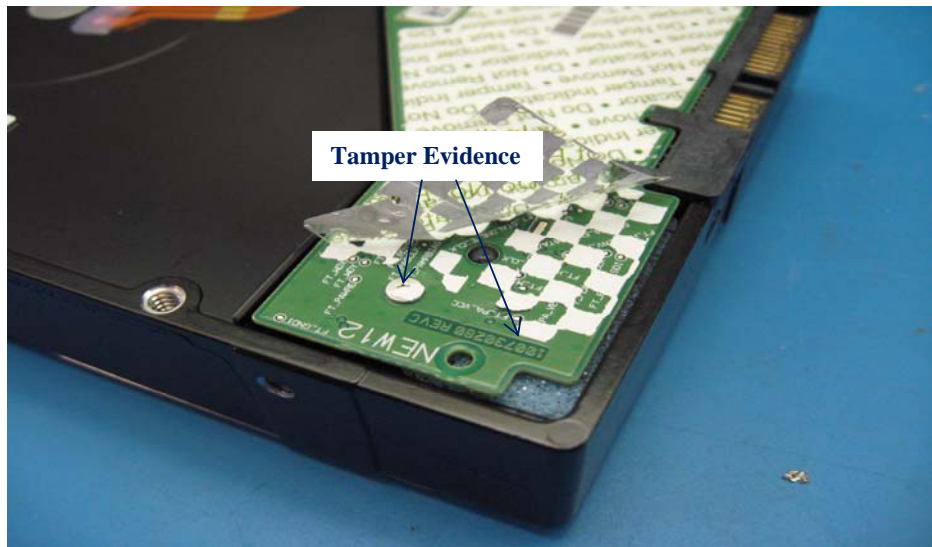


Figure 5: Enterprise Capacity® 3.5, HDD v4 (SAS/SATA) PCBA Tamper Evidence

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

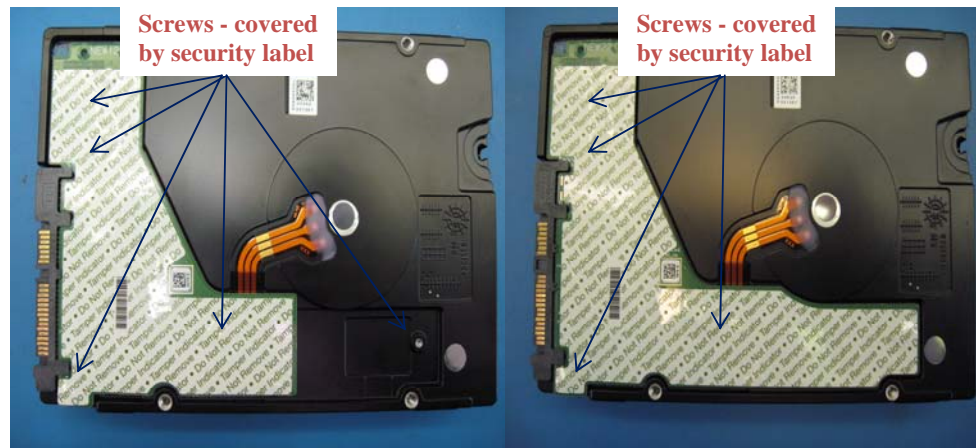


Figure 6: Enterprise Capacity® 3.5, HDD v4 (SAS/SATA) Screw covered by Security label

- 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 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. Users: At installation and periodically examine the physical security mechanisms for tamper evidence.
2. CM that supports ATA protocol on the SATA interface can transition to either of the modes by doing one of the following:
  - ATA Enhanced Security Mode: User Set PIN.
  - TCG Security Mode: authenticates to the Locking SP as BandMaster 0, BandMaster 1 or EraseMaster.

CM that supports SCSI protocol on the SAS interface can only transition to TCG Security Mode.

- Transition to TCG Security Mode is done by authenticating to Locking SP as BandMaster 0, BandMaster 1 or EraseMaster.
3. COs and Users: At installation, set all operator PINs applicable for the FIPS mode to private values of at least 4 bytes length:
    - ATA Enhanced Security Mode: Master and User. Drive Owner (optional).
    - TCG Security: Drive Owner, EraseMaster and BandMasters
  4. Drive Owner: At installation, disable the “Makers” authority<sup>1</sup>.
  5. At installation, the value of LockOnReset1 for FW Download must be set to “Power Cycle” and it must not be modified.
  6. At installation, the value of PortLocked1 for FW Download must be set to “TRUE”.

### 7.2 Ongoing Policy Restrictions

1. Prior to assuming a new role, close the current Session and start a new Session, or do a powercycle, so that the previous authentication is cleared.
2. Users for TCG Security Mode: User Data Read/Writes shall be an authenticated service<sup>2</sup>. Therefore, 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.

<sup>1</sup> Refer to Section 1.3, Item 5.

<sup>2</sup> Refer to Section 4.1, Table 1.1.