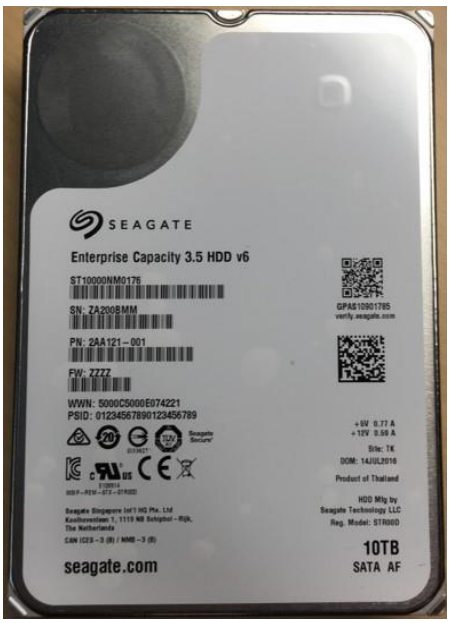

Seagate Secure® TCG Enterprise SSC Self-Encrypting Drive Non-Proprietary FIPS 140-2 Module Security Policy

Security Level 2

Rev. 0.3 – April 18, 2017

Seagate Technology, LLC

Table of Contents

Table of Figures

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 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

FIPS 140-2 Requirement Area	Security Level
Cryptographic Module Specification	3
Cryptographic Module Ports and Interfaces	2
Roles, Services and Authentication	3
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	3
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)

1.4 Acronyms

AES	Advanced Encryption Standard (FIPS 197)
CBC	Cipher Block Chaining, an operational mode of AES
CM	Cryptographic Module
CMAC	Cipher-Based Message Authentication Code algorithm
CO	Crypto-officer
CSP	Critical Security Parameter
CSPSK	Critical Security Parameter Sanitization Key
DRBG	Deterministic Random Bit Generator
MEK	Media Encryption Key
HDD	Hard Disk Drive
HMAC	Hash Message Authentication Code
IV	Initialization Vector for encryption operation
KDF	Key Derivation Function
LBA	Logical Block Address
LED	Light Emitting Device
MSID	Manufactured SID, public drive-unique value that is used as default PIN, TCG term

NDRNG	Non-Deterministic Random Number Generator
POR	Power-on Reset (power cycle)
POST	Power on Self-Test
PSID	Physical SID, public drive-unique value
PSK	Pre-Shared Key
RNG	Random Number Generator
SED	Self-Encrypting Drive, Seagate HDD/SSD products that provide HW data encryption.
SID	Secure 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)
XTS	The XTS-AES algorithm is a mode of operation of the Advanced Encryption Standard (AES)

2 Cryptographic Module Description

2.1 Overview

The Seagate Secure® TCG Enterprise SSC Self-Encrypting Drive FIPS 140-2 Module is embodied in Seagate Enterprise Performance SED 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 (AES-XTS), 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 and ATA protocols.

The CM, whose cryptographic boundary is the full drive enclosure, has a multiple-chip embedded physical embodiment. The physical interface to the CM is a SATA connector. The logical interfaces are the industry-standard ATA (refer to Section 1.3, item 7), TCG SWG (refer to Section 1.3, item 5), and Enterprise (refer to Section 1.3, item 4) protocols, carried on the SATA (refer to Section 1.3, item 8) transport interface. The primary function of the module is to provide data encryption, access control and cryptographic erase of the data stored on the flash drive media. The human operator of the drive product interfaces with the CM through a "host" application on a host system.

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 Product Versions

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

- Enterprise Capacity® HDD, 3.5" v6, 7.2K-RPM, SATA Interface
  - 10000 GB: ST10000NM0176 [1]
  - 10000 GB: ST10000NM0186 [2]
  - FW Versions: SF02 [1], NF02 [2]

2.4 FIPS Approved Algorithms

Algorithm	Certificate Number	Modes/Key Sizes/Etc used	Standard
Hardware AES	#4279	256-bit XTS and CBC	SP800-38E and FIPS 197
Hardware RSA	#2300	Signature verification w/ 2048-bit modulus	FIPS 186-4
Hardware SHA	#3515	256-bit	FIPS 180-4
Hardware HMAC	#2815	256-bit	FIPS 198-1
Firmware AES	#1343	128-bit, 256-bit CBC	FIPS 197
Firmware AES-GCM	#2841	256-bit	SP800-38D
Firmware AES-GCM (TLS)	#3759	128-bit, 256-bit	SP800-38D
Firmware AES CMAC	#3760	128-bit	SP800-38B
Firmware SHA	#3304	256-bit, 384-bit	FIPS 180-4
Firmware RSA	#2056	Signature verification w/ 2048-bit modulus	FIPS 186-4
Firmware DRBG	#1146	Hash based DRBG	SP800-90A
Firmware HMAC	#2613	256-bit	FIPS 198-1
Firmware CVL DHE (TLS)	#852	Ephemeral Mode	SP800-56A
Firmware AES Key Wrap	#2947	256-bit	SP800-38F
Firmware CVL KDF	#828	TLSv1.2 KDF	SP800-135
Firmware PBKDF	Vendor Affirmation	Option 2a	SP800-132
Firmware CKG	Vendor Affirmation	N/A	SP800-133
Hardware NDRNG	Non approved but allowed	N/A	N/A

SP800-132, Section 5.4 Option 2a is used and password length is a minimum of 4 bytes. The Master Key is 256 bits and decryption algorithm is AES-GCM. The keys derived from passwords are used in storage applications.

There are algorithms, modes and keys that have been CAVS tested but not utilized by the module. Only the algorithms, modes and keys shown in this table are utilized by the module.

The module supports the TLS protocol. This protocol has not been reviewed or tested by the CAVP or CMVP.

The length of the data unit for any instance of an implementation of XTS-AES shall not exceed 2^20 AES blocks.

The module meets the XTS-AES IG A.9 requirement.

2.5 Self-Tests

Function Tested	Self-Test Type	Implementation	Failure Behavior
Hardware XTS-AES	Power-On	Encrypt and Decrypt KAT performed.	Enters FIPS Self Test Error State.
Firmware AES	Power-On	Encrypt and Decrypt KAT performed.	Enters FIPS Self Test Error State.
Firmware AES – GCM (800-38D)	Power-On	Encrypt and Decrypt KAT performed.	Enters FIPS Self Test Error State.
Firmware AES-GCM (large block size)	Power-On	Encrypt and Decrypt KAT performed.	Enters FIPS Self Test Error State.
Firmware AES CMAC	Power-On	CMAC KAT performed.	Enters FIPS Self Test Error State.
Hardware RSA	Power-On	Verify KAT performed.	Enters FIPS Self Test Error State.
Hardware SHA-256	Power-On	Digest KAT performed.	Enters FIPS Self Test Error State.
Firmware SHA-512	Power-On	Digest KAT performed.	Enters FIPS Self Test Error State.
Firmware 800-90A DRBG	Power-On	DRBG KAT performed.	Enters FIPS Self Test Error State.
Firmware 800-38F Key Wrap	Power-On	Encrypt and Decrypt KAT performed.	Enters FIPS Self Test Error State.
Firmware 800-132 PBKDF	Power-On	KAT performed.	Enters FIPS Self Test Error State.
Firmware 800-135 KDF	Power-On	KDF KAT performed.	Enters FIPS Self Test Error State.
Firmware FFC Diffie Hellman Ephemeral Mode	Power-On	Diffie-Hellman KAT performed.	Enters FIPS Self Test Error State.
Firmware HMAC	Power-On	Keyed-Hash Message Authentication Code constructed from SHA-256.	Enters FIPS Self Test Error State.
Hardware HMAC	Power-On	Keyed-Hash Message Authentication Code constructed from SHA-256.	Enters FIPS Self Test Error State.
Firmware Integrity Check	Power-On	Signature Verification.	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.	Incoming firmware package is not loaded and is discarded.
Firmware 800-90A 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.
Firmware 800-90A DRBG Health Tests	Conditional: When a random number is generated	Instantiate, Reseed, Generate and Uninstantiate Health Tests defined in SP800-90A.	Enters FIPS Self Test Error State.
Firmware 800-90B DRBG Health Tests	Conditional: When a seed for DRBG is requested	Repetition Count and Adaptive Proportion tests are performed.	Enters FIPS Self Test Error State.
Non-Approved NDRNG	Conditional: When a seed for DRBG is requested	Newly generated random number is compared to the previously generated random	Enters FIPS Self Test Error State.

		number. Test fails if they are equal.	

2.6 FIPS 140-2 Approved Mode of Operation

Before the operator performs Secure Initialization steps detailed in Section 7.1, the drive will operate in a non-FIPS compliant mode.

For this CM that supports 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 mode of operation is 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).

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/crypto erase independent data areas (LBA ranges). Note that by default there is a single "Global Range" that encompasses the whole user data area which is the starting point from which multiple Users request their independent data areas.

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 has the capability to have multiple Users with independent access control to read/write/crypto 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.

2.6.3 Entering FIPS Approved Mode of Operation

After the module is installed and configured per the Security Rules of this policy in Section 7.1, the drive is always in the Approved mode of operation except when a critical failure has been detected, causing a transition to a "Failed" state.

In some of these exit scenarios (e.g. repeated POST failure), the drive cannot be restored to FIPS mode and does not provide any FIPS services.

2.7 User Data Cryptographic Erase Methods

Since all user data is encrypted / decrypted by the CM for storage on / retrieval from the drive media, the data can be erased using cryptographic methods. The data is erased by zeroizing the Media Encryption Key (MEK).

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

2.8 Revert-SP Method

The TCG Revert-SP 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 compliant mode of operation. This Revert-SP method is invoked as an unauthenticated service by virtue of the use of a public credential (PSID).

2.9 Show Status

Show status service can be used to determine if the drive is operational under the security constraints of FIPS. For this purpose TCG Level 0 Discovery mechanism is utilized. TCG Level 0 Discovery mechanism maybe invoked by the operator to know if drive is 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.

The LED indicates the drive is powered on. Drive activity is indicated by blinking of the LED. No other status is indicated through LED.

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 [4]. This role is used 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 the same named role as defined in Enterprise SSC [refer to Section1.3, item 4]. This role is used to enable/disable User roles, and erase the 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 (0-31) (TCG Security Mode)

This user role corresponds to the same named role as defined in Enterprise SSC [refer to Section1.3, 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 32 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

Operator roles have identity-based authentication. For example, the Drive Owner has only one ID and one PIN. In TCG Security Mode, the CM has up to 32 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 3]. 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.

Another method of authentication uses the StartTLS method in order to setup a secure TLS tunnel. Note that this method is only available after the PSKs have been set, which requires the operator to first authenticate using the method described in the preceding paragraph.

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 by means of the respective CO/User roles PIN is implemented. This mechanism also applies to the respective User roles associated with PSKs. The PINs have a maximum length of 32 bytes (256 bits). The PSKs have a maximum length of 64 bytes (512 bits). Per the policy security rules, the minimum PIN/PSK length is 4 bytes (32 bits) (Rule 2 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 140-2 authentication strength requirements of less than 1/1,000,000.

In TCG interface, each failed authentication attempt for PINs takes a minimum of 15ms to complete. Thus a theoretical 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. The PINs have a retry attribute ("TryLimit") that controls the number of unsuccessful attempts before the authentication is blocked. The "TryLimit" has an unmodifiable value of 1024. Since the "TryLimit" is unmodifiable, only 1024 attempts can be processed in one minute before the authorities are locked out.

In TCG interface, each authentication attempt for PSKs takes a minimum of 500ms to complete. Thus a theoretical maximum of {(60*1000)/500} attempts can be processed in one minute. Thus the probability of multiple random attempts to succeed in one minute is $120/2^{32}$. 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.

The initial value for PSKs are empty and disabled. For Drive Owner PSKs, "personalized" to private values by Drive Owner role using the "Set TLS PSK" service. For EraseMaster PSK, "personalized" to private values by EraseMaster role using the "Set TLS PSK" service. For BandMaster PSKs, "personalized" to private values by respective BandMasters role using the "Set TLS PSK" service.

4 Access Control Policy

4.1 Services

The following tables represent the FIPS 140-2 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).

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 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.

Table 1.1 - FIPS 140-2 Authenticated Services - TCG Security Mode			
Service Name	Description	Operator Access Control	Command(s)/Event(s)
Set PIN	Change operator authentication data.	EraseMaster, BandMasters, Drive Owner	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 **	TCG Set Method, ATA DOWNLOAD MICROCODE
Enable / Disable BandMasters	Enable / Disable a User Authority.	EraseMaster	TCG Set Method
Set Range Attributes	Set the location, size, and locking attributes of the LBA range.	BandMasters	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	TCG Set Method
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.	BandMasters	ATA Read, Write Commands
Cryptographic Erase	Erase user data in an LBA range by cryptographic means: changing the Media encryption key (MEK). BandMaster PIN is also reset.	EraseMaster	TCG Erase Method
Set TLS PSK	Set PSK for Secure Messaging.	EraseMaster, BandMasters, Drive Owner	TCG Set Method

Table 1.2 - FIPS 140-2 Unauthenticated Services - TCG Security Mode			
Service Name	Description	Operator Access Control	Command(s)/Event(s)
Enable Secure Messaging	Support host initiated TLS Session.	None	TCG StartTLS Method
Show Status	Reports if the CM is operational in terms of FIPS services and approved mode of operation value.	None	TCG Level 0 Discovery, TCG Get Method FIPS Operating Mode indicator (Byte 30, bit 0) = 1.
Reset Module	Runs POSTs and zeroizes key & CSP in RAM.	None	POR
DRBG Generate Bytes	Returns an SP800-90A DRBG Random Number.	None	TCG Random()
Exit FIPS Mode	Exit Approved Mode of Operation. Note: CM will enter non-FIPS mode.	None (using PSID)	TCG AdminSP.RevertSP()
FIPS 140 Compliance Descriptor	Reports FIPS 140 Revision, Overall Security Level, Hardware and Firmware revisions and Module name.	None	ATA TRUSTED RECEIVE – Protocol 0

**FW Download Port has to be Unlocked

Table 2.1- FIPS 140 Services – Authenticated Services (ATA Enhanced Security Mode)			
Service Name	Description	Operator Access Control	Command(s)/Event(s)
Set PIN	Change operator authentication data.	User (optional Master), Drive Owner	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**	TCG Set Method, ATA DOWNLOAD MICROCODE
Unlock User Data	Enable user data read/write and Set PIN services.	User (optional Master)	ATA SECURITY UNLOCK
User Data Read / Write	Encryption / decryption of user data.	User (optional Master)	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	ATA SECURITY ERASE PREPARE + ATA SECURITY ERASE UNIT
Sanitize	Sanitize user data through cryptographic means: by zeroizing the encryption key.	User (optional Master)	ATA CRYPTO SCRAMBLE
Disable Services	Disables ATA Security commands until POR	User (optional Master)	ATA SECURITY FREEZE LOCK
Exit FIPS Mode	Exit Approved Mode of Operation. Note: CM will enter non-FIPS mode.	User (optional Master)	ATA SECURITY DISABLE PASSWORD, ATA SECURITY ERASE PREPARE + ATA SECURITY ERASE UNIT

Table 2.2 - FIPS 140 Unauthenticated Services (ATA Enhanced Security Mode)			
Service Name	Description	Operator Access Control	Command(s)/Event(s)
Unblock PIN	Reset Master and User password attempt counter.	None	POR
Show Status	Reports if the CM is operational in terms of FIPS services and approved mode of operation value.	None	TCG Level 0 Discovery, TCG Get Method FIPS Operating Mode indicator (Byte 30, bit 0) = 1.
Reset Module	Runs POSTs and zeroizes key & CSP RAM storage.	None	POR
Exit FIPS Mode	Exit Approved Mode of Operation. Note: CM will enter non-FIPS mode.	None (using PSID)	TCG AdminSP.RevertSP()
FIPS 140 Compliance Descriptor	Reports FIPS 140 Revision, Overall Security Level, Hardware and Firmware revisions and Module name	None	ATA TRUSTED RECEIVE – Protocol 0

**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 800-90A DRBG and adopts Hash_DRBG mechanism.
- Symmetric keys and seeds for asymmetric keys are unmodified outputs from the DRBG.
- 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, 32-256 bits	Drive Owner	Set PIN	W
Master, User Passwords	ATA	Auth. Data	Private, PIN, 32-256 bits	Master, User	Set PIN	W
Master, User MEK	ATA	Media Encryption Key	Private, AES Key, 256 bits	Master, User	Unlock User Data	X
EraseMaster	TCG	EraseMaster Auth Data	Private, PIN, 32-256 bits	Master, User	Unlock User Data	X
				Master, User	Cryptographic Erase	X
BandMaster (0-32) Passwords	TCG	Users Auth. Data	Private, PIN, 32-256 bits	Master, User	Sanitize	X
					Lock/Unlock User Data	X
LBA Range MEKs	TCG	MEK (per LBA band)	Private, AES Key, 256 bits	BandMasters	Lock/Unlock User Data	X
Entropy Input String	Both	*Input to a DRBG mechanism of a string of bits that contains entropy	Private, 256 bits	None	Services which use the DRBG (cryptographic erase)	X
Seed	Both	*String of bits that is used as input to a DRBG mechanism	Private, Hash seed, 440 bits	None	Services which use the DRBG (cryptographic erase, SetPIN)	X
Internal State	Both	*Collection of stored information about DRBG instantiation	Private, V and C 440 bits each	None	Services which uses the DRBG (cryptographic erase, SetPIN)	X
ORG 0-0 - ORG 0-1	Both	Firmware Load Test Signature Verify Key	Public, RSA Key, 2048 bits	Drive Owner	FW Download	X
MEKEK	Both	This key is used to wrap the MEK	Private, AES Key, 256 bits	BandMasters, EraseMaster	Lock/Unlock User Data, Cryptographic Erase, Set PIN	W,X
Master Key	Both	This key is used to protect the MEKEK	Private, AES Key, 256 bits	Drive Owner, BandMasters, EraseMaster	Unlock User Data, Cryptographic Erase, Set PIN	W,X
CSPSKs	Both	Critical Security Parameter Sanitization Keys, used within PBKDF	Private, AES Key, 256 bits	BandMasters, EraseMaster	Lock/Unlock User Data, Cryptographic Erase, Set PIN	W, X
Drive Owner PSKs	TCG	Pre-Shared secret value used for TLS handshake (up to 4 are supported)	Private, Pre-Shared Key, 32-512 bits	Drive Owner	Set TLS PSK	W,X
EraseMaster PSK	TCG	Pre-Shared secret value used for TLS handshake	Private, Pre-Shared Key, 32-512 bits	EraseMaster	Set TLS PSK	W,X
BandMaster PSKs	TCG	Pre-Shared secret value used for TLS handshake(32 are supported)	Private, Pre-Shared Key, 32-512 bits	BandMaster	Set TLS PSK	W,X
Secure Messaging Session Key	TCG	Derived session unique key	Private, AES Key, 128 or 256 bits	EraseMaster, BandMasters, Drive Owner	Enable Secure Messaging	X
Secure Messaging Key Pair	TCG	Key pair used for deriving shared secret during handshake	Public and Private, Diffie-Hellman, 2048 and 256 bits	EraseMaster, BandMasters, Drive Owner	Enable Secure Messaging	X

* Source: Section 4 Terms and Definitions of NIST Special Publication 800-90A
** 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
- Access to the interior of the drive is prevented via a weld of the drive top cover to the base deck.
- Exterior of the drive is opaque
- The tamper-evident label cannot be penetrated or removed and reapplied without tamper-evidence
- The tamper-evident label cannot be easily replicated with a low attack time

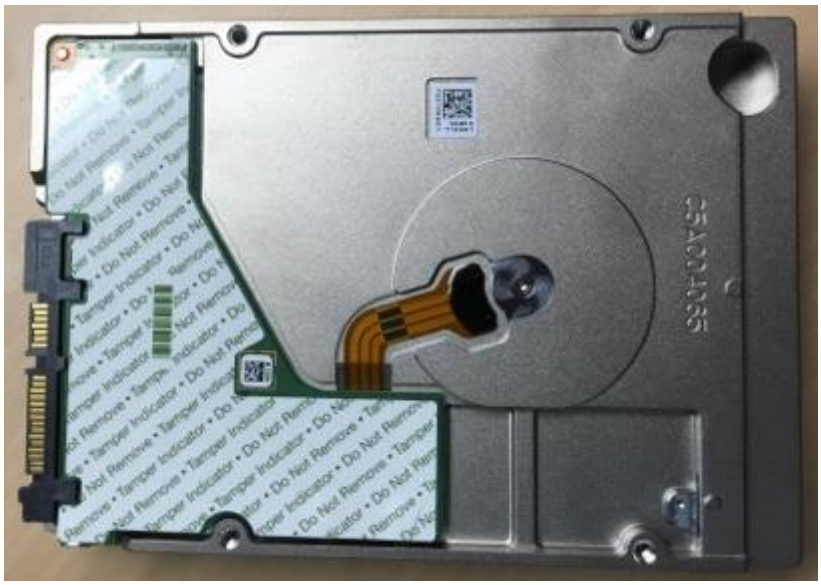

Figure 1: Tamper-Evident Security Label on PCBA to provide evidence of PCBA tampering

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
- Security label cutouts do not match original

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

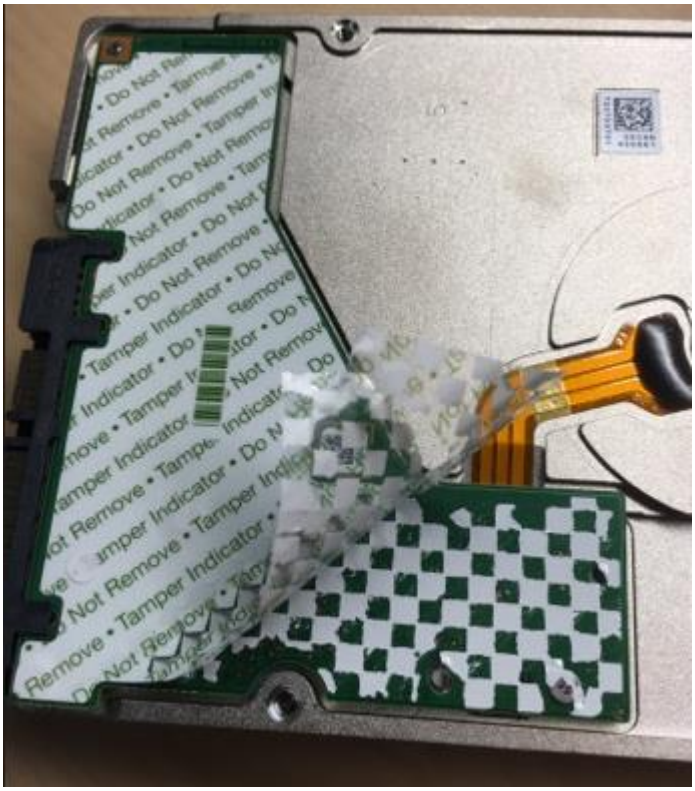

Figure 2: Tamper-Evident Security Label on PCBA showing evidence of tampering

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 140-2 compliant manner. Reference the appropriate sections of this document for details.

1. Users: At installation and at periodic intervals examine the physical security mechanisms for tamper evidence.
2. CM using 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.
3. COs and Users: At installation, set all operator PINs applicable for the FIPS mode to private values of at least 4 bytes (32 bits) 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[1]
5. At installation, the value of LockOnReset[1] for FW Download must be set to "Power Cycle" and it must not be modified.
6. At installation, the value of PortLocked[1] for FW Download must be set to "TRUE".

At the end of these steps, the CM will be in a FIPS Approved Mode of operation. This can be verified with Show Status service (refer to Section 4.1).

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 cycle, so that the previous authentication is cleared.
2. User Data Read/Writes shall be an authenticated service[2]. Therefore, set ReadLockEnabled[1] and WriteLockEnabled[1] 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.
3. Set all PSKs (Drive Owner PSKs, EraseMaster PSK, BandMaster PSKs) applicable for the FIPS mode to private values of at least 4 bytes (32 bits) length.

8 Mitigation of Other Attacks Policy

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

[1] Refer Section 1.3, Item 5
[2] Refer to Section 4.1, Table 1.1