Seagate
Secure Constellation® ES and Constellation®.2 Self-Encrypting Drives
FIPS 140 Module Security Policy

Security Level 2

Rev. 1.9 – November 23, 2012

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 Constellation® ES** and **Constellation®.2 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 Areas	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 2.0, December 21, 2009
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)
CBC	Cipher Block Chaining, an operational mode of AES
CM	Cryptographic Module
CO	Crypto-officer
CSP	Critical Security Parameter
DRBG	Deterministic Random Bit Generator
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
MSID	Manufactured SID, public drive-unique value that is used as default PIN, TCG term
PN	Part Number(s)
POR	Power-on Reset (power cycle)
POST	Power on Self-Test
PSID	Physical SID, public drive-unique value
RNG	Random Number Generator
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 **Constellation® ES** and **Constellation®.2** Self-Encrypting Drives FIPS 140 Module is embodied in Seagate **Constellation® ES** and **Constellation®.2** 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 (7), SCSI (9 & 10), TCG SWG (5), and Enterprise (4) protocols, carried on the SATA (8) or SAS (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 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 ASICs are SoCs which have the following major logical functions: host interface using an industry standard SAS or SATA interface, a RW Channel interface to the HDA, interface to media motor controller, data encryption engines, and processing services which execute the firmware. An Approved Security Function, AES-256, 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/SCSI command set, 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/SCSI write/read commands respectively. Other security operations, including authentication and management of cryptographic secrets, are accessed using ATA Security and Trusted Send/Receive or SCSI SECURITY PROTOCOL IN/OUT commands. The ATA Trusted Send/Receive and SCSI Security commands are actually wrappers for industry standard protocol TCG protocols.

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:

- Constellation®.2, 2.5-Inch, 7K-RPM, SAS Interface, 1000/500 GB,
  - 1000 GB: 9XU268 [1, 6], 9XU268-251 [2, 7, 9, 11], 9XU268-257 [3, 8, 10, 12,13], 9XU268-047 [4], 9XU268-090 [5]
  - 500 GB: 9XU264 [1, 6], 9XU264-251 [2, 7, 9, 11], 9XU264-257 [3, 8, 10, 12,13], 9XU264-047 [4], 9XU264-090 [5]

  FW Versions: A002 [1], ASF2 [2], ANF1 [3], NS01 [4], QF70 [5], 0003 [6], ASF5 [7], AEF3 [8], ASF8 [9], AEF5 [10], ASF9 [11], AEF6 [12], AEF7 [13]

- Constellation®.2, 2.5-Inch, 7K-RPM, SATA Interface, 1000/500/250 GB,
  - 1000 GB: 9XU168 [14, 15]
  - 500 GB: 9XU164 [14, 15]
  - 250 GB: 9XU162 [14, 15]

  FW Versions: 0002 [14], 0003 [15]

- Constellation® ES, 3.5-Inch, 7K-RPM, SAS Interface, 2000/1000/500 GB,
  - 2000 GB: 1AV268 [16, 18]
  - 1000 GB: 1AV264 [16, 18], 1AV264-257 [17, 20, 22], 1AV264-251 [19, 21, 23]
  - 500 GB: 1AV262 [16, 18]

  FW Versions: A001 [16], PNF0 [17], 0002 [18], PSF1 [19], PEF3 [20], PSF4 [21], PEF4 [22], PSF5 [23]

- Constellation® ES, 3.5-Inch, 7K-RPM, SATA Interface, 2000/1000/500 GB,
  - 2000 GB: 1AV168 [24, 25]
  - 1000 GB: 1AV164 [24, 25]
  - 500 GB: 1AV162 [24, 25]

  FW Versions: A001 [24], 0002 [25]

HW versions that support ATA protocols are:

- Constellation®.2, 2.5-Inch, 7K-RPM, SATA Interface, 1000/500/250 GB and
- Constellation® ES, 3.5-Inch, 7K-RPM, SATA Interface, 2000/1000/500 GB.

HW versions that support SAS protocols are:

- Constellation®.2, 2.5-Inch, 7K-RPM, SAS Interface, 1000/500 GB and
- Constellation® ES, 3.5-Inch, 7K-RPM, SAS Interface, 2000/1000/500 GB.

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

2.4 FIPS Approved Algorithms

Algorithm	Certificate Number
ASIC AES	#1416, #1417
Firmware AES	#1343
RSA	#650
SHA	#1225
800-90 DRBG	#62

Certificate #1416 is applicable for HW versions that support ATA protocol (defined in Section 2.3).

Certificate #1417 is applicable for HW versions that support SAS protocol (defined in Section 2.3).

Certificates #1343, 650, 1225 and 62 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.
Firmware AES	Power-On	Encrypt and Decrypt KAT performed	Enters FIPS Self Test Error State and rejects host commands with error code.
RSA	Power-On	Verify KAT performed.	Enters FIPS Self Test Error State and rejects host commands with error code.
SHA-1	Power-On	Digest KAT performed	Enters FIPS Self Test Error State and rejects host commands with error code.
SHA-256	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	16-bit CRC and ECC	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.

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 compliant mode.

There are 2 approved modes of operation, “TCG Security” or “ATA Enhanced Security”. The modes provide the same FIPS services but with different command protocols and minor functional differences e.g. number of user ids. Note that the ATA Enhanced Security mode is only available on hardware versions that support the ATA protocol on the SATA interface.

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).

The following sections 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.

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/crypto-erased with one encryption key.

2.6.3 Entering FIPS Approved Modes of Operation

For models that supports the SCSI protocol (defined in Section 2.3) the CM will only operate in TCG Security mode. 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.

For models that support the ATA protocol (defined in Section 2.3), the operator may choose to initialize the CM to operate in either ATA Enhanced Security or TCG Security modes. After setting up (configuring) the module per the Security Rules of this policy, an operator can switch between the modes. To transition to ATA Enhanced Security Mode from uninitialized state, the Set PIN service is used on the User role. This mode corresponds to having a deactivated TCG Locking SP. To transition to TCG Security Mode, the host authenticates as BandMaster 0 or BandMaster 1 to the Locking SP from uninitialized state. The CM does not change mode across module resets. Note that to switch between the two modes the module must transition to the uninitialized state (exit FIPS mode service) which results in zeroization of keys and CSPs.

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/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 services 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 compliant 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 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 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, for HW versions that support the SATA protocol then the Show Status service can be used to confirm the “SecurityOperatingMode”; i.e. FIPS Approved mode. 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 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 [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 [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 [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 [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 [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 6.8 seconds (about 10/min). Thus the probability of multiple random attempts to succeed is $10/2^{32}$. 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 “opt” then the access is dependent on the module setup (see 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
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	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,	RNG, 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 • current FIPS approved mode***.	None	None	TCG Level 0 Discovery, Drive Security Life Cycle State***
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()

Table 2.1- FIPS 140 Services – Authenticated Services (ATA Enhanced Security Mode)				
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
Sanitize	Sanitize user data through cryptographic means: by zeroizing the encryption key.	None*	RNG	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*(opt. Master*)	RNG, Hashing, Symmetric Key	ATA SECURITY DISABLE PASSWORD ATA SECURITY ERASE PREPARE + SECURITY ERASE UNIT

Table 2.2 - FIPS 140 Unauthenticated Services (ATA Enhanced Security Mode)				
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 • current FIPS approved mode***.	None	None	TCG Level 0 Discovery, Drive Security Life Cycle State***
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()

*Security has to be Unlocked
**FW Download Port has to be Unlocked
*** Applicable for CM that support SATA protocol (refer to Section 2.9)

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.
- The module uses SP 800-90 DRBG and adopts Hash_DRBG mechanism.
- 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.

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)**	**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	RevertSP
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	RevertSP, Cryptographic Erase (User)
				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	MEK mixed with PINs	Private, AES Key, 256 bits	Master, User	Unlock User Data	X	RNG generated during manufacturing	Media (System Area)	Obfuscated (considered plaintext for FIPS purposes)	None	RevertSP, Cryptographic Erase, Sanitize
EraseMaster	TCG	EraseMaster Auth Data	Private, PIN, 32 bytes	EraseMaster	SetPIN	W	MSID	Media (System Area)	SHA Digest	Electronic Input from Host No output	RevertSP
BandMasters (0-15) Passwords	TCG	Users Auth. Data	Private, PIN, 32 bytes	BandMasters	Set PIN	W	MSID	Media (System Area)	SHA Digest	Electronic Input from Host No output	RevertSP
LBA Range MEKs	TCG	MEK (per LBA band)	Private, AES Key, 256 bits	Users	Unlock User Data	X	RNG generated during manufacturing	Media (System Area)	Obfuscated (considered plaintext for FIPS purposes)	None	RevertSP, Cryptographic Erase
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 RNG (e.g; cryptographic erase, sanitize)	X	Entropy value collected at power up or reseeding	RAM	None	None	Reset
Seed	Both	*String of bits that is used as input to a DRBG mechanism	Private, Hash seed, 544 bytes	None	Services which use the RNG (e.g. cryptographic erase, sanitize)	X	Undefined, depends on DRBG instantiation inputs	RAM	None	None	Reset
Internal State	Both	*Collection of stored information about DRBG instantiation	Private, V and C	None	Services which uses the RNG (e.g. cryptographic erase, sanitize)	X	Undefined, updated at each DRBG usage	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)

* Source: Section 4 Terms and Definitions of NIST Special Publication 800-90
** W - Write access is allowed, X - Execute access is allowed

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 RevertSP Admin SP method (i.e. Exit FIPS Mode service). This method will leave the CM in a non FIPS compliant "factory default" mode 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.

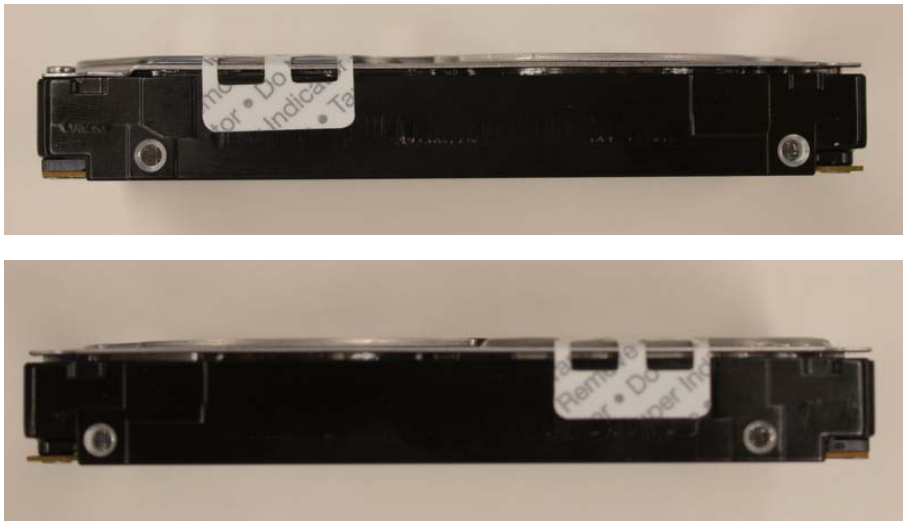
5 Physical Security

5.1 Mechanisms

The CM has the following physical security:

- Production-grade components with standard passivation
- 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
- On each side of the top cover a tamper-evident security label is applied by Seagate manufacturing 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 label on PCBA of drive to provide tamper-evidence of PCBA removal

- 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 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. For ATA CM, transition to a FIPS approved mode is by doing one of the following:
   - ATA Enhanced Security Mode: User Set PIN.
   - TCG Security Mode: authenticates to the Locking SP as BandMaster 0 or BandMaster 1
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 (defined in TCG Core Specification [5]) .
5. At installation, the value of LockOnReset (defined in TCG Core Specification [5]) for FW Download must be set to "Power Cycle" and it must not be modified.
6. After secure initialization is complete, do a power-on reset to clear authentications established during initialization.

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. Users for TCG Security Mode: If it is intended to have a band lock on module reset then set ReadLockEnabled and WriteLockEnabled (defined in TCG Core Specification [5]) 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.