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

**Security Level 2**

**Rev. 1.0 – June 23, 2016**

**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 Secure® TCG Opal SSC Self-Encrypting Drive** products. The module meets all FIPS 140-2 overall Security Level 2 requirements.

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

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

## 1.2 Security Levels

| Requirement Area | Level |
|---|---|
| Cryptographic Module Specification | 2 |
| Cryptographic Module Ports and Interfaces | 2 |
| Roles, Services and Authentication | 2 |
| Finite State Model | 2 |
| Physical Security | 2 |
| Operational Environment | N/A |
| Cryptographic Key Management | 2 |
| Electromagnetic Interface / Electromagnetic Compatibility (EMI / EMC) | 3 |
| Self – Tests | 2 |
| Design Assurance | 2 |
| Mitigation of Other Attacks | N/A |

## 1.3 References

1. FIPS PUB 140-2
2. Derived Test Requirements for FIPS PUB 140-2
3. Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program
4. TCG Storage Security Subsystem Class: Opal, Specification Version 2.00
5. TCG Storage Architecture Core Specification, Specification Version 2.00
6. TCG Storage Interface Interactions Specification, Specification Version 1.0
7. TCG Storage Opal SSC Feature Set: Single User Mode, Specification Version 1.0
8. ATA-8 ACS
9. Serial ATA Rev 3.2 (SATA)

## 1.4 Acronyms

| | |
|---|---|
| AES | Advanced Encryption Standard (FIPS 197) |
| CBC | Cipher Block Chaining, an operational mode of AES |
| CM | Cryptographic Module |
| CO | Crypto-officer |
| CSP | Critical Security Parameter |
| CSPSK | Critical Security Parameter Sanitization Key |
| MEK | Media Encryption Key |
| FIPS 140 | FIPS 140-2 |
| HDA | Head and Disk Assembly |
| HDD | Hard Disk Drive |
| IV | Initialization Vector for encryption operation |
| LBA | Logical Block Address |
| KAT | Known Answer Test |
| MBR | Master Boot Record |
| MSID | Manufactured SID, public drive-unique value that is used as default PIN, TCG term |
| PBKDF | Password-Based Key Derivation Function |
| 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 products that provide HW data encryption. |
| 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) |
| SUDR | Single User Data Range |

# 2 Cryptographic Module Description

## 2.1 Overview

The 'Seagate Secure® TCG Opal SSC Self-Encrypting Drive (SED) FIPS 140-2 Module' is embodied in Seagate Laptop thin and Laptop Self-Encrypting Drive model disk drives. The cryptographic module (CM) provides a wide range of cryptographic services using FIPS approved algorithms. Services include hardware-based data encryption, instantaneous user data disposal with cryptographic erase, independently controlled and protected user data LBA ranges, and authenticated FW download. The services are provided through an industry-standard TCG Opal SSC interface.

The CM is a multiple-chip embedded physical embodiment. The cryptographic boundary is the entire physical drive. The physical interface to the CM is the SATA connector and jumper block pins. The logical interface is the industry-standard ATA (8), TCG SWG (5), and Opal SSC (4) protocols, carried on the SATA transport interface (9). 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.

## 2.2 Logical to Physical Port Mapping

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

## 2.3 Hardware and Firmware Versions

The SED Drives, FIPS 140 Module has been validated in 6 configurations:

| Hardware Versions | Hardware Description | Firmware Versions |
|---|---|---|
| ST1000LM038 - 1RD172 | ST1000LM038 – 1TB | SDM1 |
| ST1000LM038 - 1RD172 | ST1000LM038 – 1TB | RSE1 |
| ST1000LM038 - 1RD172 | ST1000LM038 – 1TB | LSM1 |
| ST2000LM010 - 1RA174 | ST2000LM010 – 2TB | SDM1 |
| ST2000LM010 - 1RA174 | ST2000LM010 – 2TB | RDE1 |
| ST2000LM010 - 1RA174 | ST2000LM010 – 2TB | LSM1 |

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

## 2.4 FIPS Approved Algorithms

| Algorithm | Supported Modes | Certificate No. |
|---|---|---|
| ASIC AES<br>Note: The largest data unit length supported is 2^5 blocks. | ECB (e/d; 128, 256);<br>CBC (e/d; 128, 256);<br>XTS (KS: XTS_256 ((e/d) (f/p)) | #3758 |
| ASIC SHA | SHA-256 (BYTE-only) | #3128 |
| ASIC RSA | ALG[RSASSA-PKCS1_V1_5]<br>SIG (gen) (2048 SHA (256))<br>SIG (ver) (2048 SHA (256)) | #1933 |
| ASIC HMAC using ASIC SHA | HMAC-SHA256 (Key Size Ranges Tested: KS<BS, KS>BS) | #2460 |
| Firmware AES | ECB (e/d; 128, 256);<br>CBC (e/d; 128, 256) | #1343 |
| Firmware AES GCM | GCM (KS: AES_128 (e/d) Tag Length(s): 128) (KS: AES_256 (e/d) Tag Length(s): 128) PT Lengths Tested: (0, 128, 256, 8, 24); AAD Lengths tested: (0, 128, 256, 8, 24); IV Lengths Tested: (8, 1024); 96BitIV_Supported; OtherIVLen_Supported; GMAC_Supported | #2804 |
| Firmware RSA | ALG[RSASSA-PKCS1_V1_5]<br>SIG (gen) (2048 SHA (256))<br>SIG (ver) (2048 SHA (256)) | #1934 |
| Firmware SHA | SHA-1 (BYTE-only)<br>SHA-256 (BYTE-only) | #1225 |
| Firmware SHA | SHA-512 (BYTE-only) | #3129 |
| Firmware 800-90A Hash-DRBG | Hash_Based DRBG: [Prediction Resistance Tested: Not Enabled (SHA-256)] | #62 |
| Firmware HMAC using SHA | HMAC-SHA256 (Key Size Ranges Tested: KS<BS, KS=BS, KS>BS) | #1597 |
| Firmware 800-132 PBKDF | | Vendor Affirmed |
| Firmware AES CMAC | CMAC (Generation/Verification) (KS: 128; Block Size(s): Partial; Msg Len(s) Min: 1 Max: 2^16; Tag Len(s) Min: 16 Max: 16) (KS: 256; Block Size(s): Partial; Msg Len(s) Min: 1 Max: 2^16; Tag Len(s) Min: 16 Max: 16) | #3760 |
| Firmware 800-38F Key Wrap using AES | KW (AE, AD, AES-256, FWD, 128, 256, 192, 320, 4096) | #2947 |
| Firmware FFC Diffie-Hellman Ephemeral Mode | FFC: (Functions included in implementation: KPG)<br>SCHEMES: Ephem: (KARole: Initiator) FB SHS | #707 |
| Firmware 800-135 KDF<br>Note: The TLS protocol have not been reviewed or tested by the CAVP and CMVP. | TLS (TLS1.2 (SHA 256, 384)) | #708 |
| Firmware AES-GCM (large block size) | GCM (KS: AES_128(e/d) Tag Length(s): 128) (KS: AES_256(e/d) Tag Length(s): 128) PT Lengths Tested: (0, 128, 256, 8, 24); AAD Lengths Tested: (0, 128, 256, 8, 24); IV Lengths Tested: (8 ,1024); 96BitIV_Supported; OtherIVLen_Supported; GMAC_Supported | #3759 |

### 2.4.1 Non-approved but Allowed Algorithms

The following algorithms are non-approved but allowed in FIPS module of operation,

- Diffie-Hellman (key agreement; key establishment methodology provides 112 bits of encryption strength);
- NDRNG– Used to provide entropy

## 2.5 Self-Tests

| Function Tested | Self-Test Type | Implementation | Failure Behavior |
|---|---|---|---|
| ASIC AES | Power-On | Encrypt and Decrypt KATs performed | Enters FIPS Self Test Fail State |
| ASIC SHA | Power-On | Digest KAT performed | Drive fails to come ready and remains unresponsive |
| ASIC RSA | Power-On | Verify KAT performed | Enters FIPS Self Test Fail State |
| ASIC HMAC | Power-On | HMAC KAT performed | Enters FIPS Self Test Fail State |
| Firmware AES | Power-On | Encrypt and Decrypt KATs performed | Enters FIPS Self Test Fail State |
| Firmware AES-GCM | Power-On | Encrypt and Decrypt KAT performed | Enters FIPS Self Test Fail State |
| Firmware RSA | Power-On | Verify KAT performed | Drive Hangs |
| Firmware 800-90 DRBG | Power-On | DRBG KAT performed | Enters FIPS Self Test Fail State |
| Firmware HMAC | Power-On | HMAC KAT performed | Enters FIPS Self Test Fail State |
| Firmware 800-132 PBKDF | Power-On | PBKDF KAT performed | Enters FIPS Self Test Fail State |
| Firmware CMAC | Power-On | CMAC KAT performed | Enters FIPS Self Test Fail 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. | Firmware download is aborted |
| Firmware 800-90 DRBG (CRNGT) | Conditional: When a random number is generated | Newly generated random number is compared to the previously generated random number. Test fails if they are equal. | Enters FIPS Self Test Fail State |
| Firmware 800-90 DRBG Entropy (CRNGT) | Conditional: When entropy is retrieved from entropy pool. | Newly retrieved entropy value is compared to previously retrieved entropy value. Test fails if they are equal. | Enters FIPS Self Test Fail State |
| Firmware 800-38F Key Wrap | Power-On | AES Key Wrap and Unwrap KATs performed | Enters FIPS Self Test Fail State |
| Firmware SHA-512 | Power-On | SHA-512 KAT performed | Enters FIPS Self Test Fail State |
| Firmware FFC Diffie-Hellman Ephemeral Mode | Power-On | Diffie-Hellman KAT performed | Enters FIPS Self Test Fail State |
| Firmware 800-135 KDF | Power-On | KFD KAT performed | Enters FIPS Self Test Fail State |
| Firmware AES-GCM (large block size) | Power-On | Encrypt and Decrypt KAT performed | Enters FIPS Self Test Fail State |

## 2.6 FIPS 140 Approved Modes of Operation

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

From this mode, the operator may choose to initialize the CM to operate in either “ATA Enhanced Security Mode” or “TCG Opal Security Mode”. After setting up (configuring) the CM per the Security Rules detailed in Section 7.1, the CM will remain in FIPS Approved mode of operation until either a critical failure has been detected; or any ‘Exit FIPS Mode’ services is invoked; or the “Show Status” service does not return the expected status (refer to Section 4.1).

An operator can switch the CM between these FIPS Approved modes of operation. To do so, he must first, transition to the uninitialized state (via ‘Exit FIPS Mode’ service) which will zeroize the keys and CSPs. He must then reinitialize the CM per the Security Rules detailed in Section 7.1 to return to a FIPS Approved mode of operation. Thus CSPs are not shared between different modes of operation (both approved modes and the non-Approved mode).

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 Approved mode of operation.

### 2.6.1 ATA Enhanced Security Mode

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

ATA Enhanced Security Mode implements the Master and User roles as defined in ATA. The ATA security lock / unlock states correspond to operator authentication for the Read / Write data services (which use an internal AES 256-bit key for encryption and decryption of data written to and read from the drive media respectively). In addition, a “Drive Owner” CO role is provided, which can enable or disable access to the FW download service for FW upgrade. Additionally, a cryptographic erase service is provided to the Master and User roles through the ATA Security Erase Unit commands. The FW download service (ATA Download Microcode command) provides a FIPS Approved FW load test by verifying the code’s embedded 2048-bit RSA signature.

### 2.6.2 TCG Opal Security Mode

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

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

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

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

#### 2.6.2.1 Single User Data Ranges (SUDRs)

While invoking the Activate method to enter TCG Opal Security Mode, the Drive Owner may elect to classify one or more user data ranges as “Single User Data Ranges” (SUDRs). Such SUDRs conform to the

Single User feature set as defined in the Opal SSC feature set (7) and are managed solely by the associated User role. Details of the differences between SUDRs and normal data ranges can be found in Section 4.1, Table 2.1.

Note that once in TCG Opal Security Mode, the only way to change the classification of a user data range without invoking the “Exit FIPS Mode” service is by using the Reactivate method.

## 2.7 User Data Cryptographic Erase Methods

Since all user data is encrypted / decrypted by the CM for storage / retrieval on the drive media, the data can be erased using a cryptographic method. The data is effectively erased by changing the encryption key (MEK). Thus, the FIPS 140 key management capability of “zeroization” of the key erases all the user data. This capability is available through both FIPS modes. Of course the user data can also be erased by overwriting, but this can be a long operation on high capacity drives.

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

## 2.8 Revert and Revert SP Methods

In either ATA Enhanced Security Mode or TCG Opal Security Mode, the TCG Revert and Revert SP methods may be invoked by an appropriately authenticated Role to transition the CM into the uninitialized state (non-Approved) mode. This corresponds to the “Exit FIPS Mode” service and is akin to a “restore to factory defaults” operation. This operation also provides a means to zeroize keys and CSPs. Subsequently, the CM has to be reinitialized before it can return to a FIPS Approved mode of operation (i.e., ATA Enhanced Security Mode or TCG Opal Security Mode). These Revert and Revert SP methods may be invoked by the Drive Owner, Admin SP Admins, Locking SP Admins, or an unauthenticated role using the public PSID value.

# 3 Identification and Authentication (I&A) Policy

## 3.1 Operator Roles

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

### 3.1.1 Crypto Officer Roles

#### 3.1.1.1 Drive Owner

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

#### 3.1.1.2 Admins (1-4) in Locking SP (TCG Opal Security Mode Only)

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

#### 3.1.1.3 Admins (1-4) in AdminSP (TCG Opal Security Mode Only)

This CO role for TCG Opal Security Mode corresponds to the same named Authority on the Admin SP as defined in Opal SSC (4). This role is disabled by default and can be enabled using SID. Once enabled, this role can invoke the "Exit FIPS Mode" service in TCG Opal Security Mode.

### 3.1.2 User Roles

#### 3.1.2.1 User (1) – ATA Enhanced Security Mode, Users (1-16) – TCG Opal Security Mode

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

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

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

This role corresponds to the same named role as defined in ATA (8). 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.

## 3.2 Authentication

### 3.2.1 Authentication Type

Operator authentication is role-based. For example, the Drive Owner role has its own unique ID and PIN.

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

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

### 3.2.2 Authentication in ATA Enhanced Security Mode

In ATA Enhanced Security Mode, Master and User operator authentication is provided through a PIN provided in the ATA Security command (8). 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 Start Session or Authenticate to Admin SP.

### 3.2.3 Authentication in TCG Opal Security Mode

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

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

### 3.2.4 Authentication Mechanism, Data and Strength

Operator authentication with PINs is implemented by hashing the operator input value and comparing it to the stored hash of the assigned PIN. The PINs have a retry attribute ("TryLimit") that controls the number of unsuccessful attempts before the authentication is blocked until a module reset. The PINs have a maximum length of 32 bytes.

Per the policy security rules, the minimum PIN length is 4 bytes (Rule 4 in Section 7.1). This gives a probability of $1/2^{32}$ of guessing the PIN in a single random attempt. This easily meets the FIPS 140 authentication strength requirements of less than 1/1,000,000.

Each authentication attempt takes 15ms on average to complete. This means that approximately {(60*1000)/15} attempts can be made in one minute. Thus the probability of multiple random attempts to succeed in one minute is about $4000/2^{32}$. This is significantly lower than the FIPS requirement of 1/100,000.

### 3.2.5 Personalizing Authentication Data

The initial value for SID is a manufactured value (mSID). This is a device-unique, 32-byte, public value. The Security Rules (Section 7) for the CM requires that the PIN values must be "personalized" to private values using the "Set PIN" service. Note that for 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 FIPS Services

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

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

## Table 1.1 - FIPS 140 Authenticated Services – ATA Enhanced Security Mode

| Service Name | Description | Operator Access Control | Security Function | Command(s)/Event(s) |
|---|---|---|---|---|
| Set PIN | Change operator authentication data.<br>Note: Setting the User PIN also sets the Drive Owner PIN. | Master*, User*,Drive Owner | PBKDF, Symmetric Key | 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 (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.<br>Note: CM will enter uninitialized state. | Master, User | RNG | ATA SECURITY ERASE PREPARE + ATA SECURITY ERASE UNIT |
| Exit FIPS Mode | Exit ATA Enhanced Security Mode.<br>Note: CM will enter uninitialized state. | User*(optional. Master*) | RNG, Hashing, Symmetric Key | ATA SECURITY ERASE PREPARE + SECURITY ERASE UNIT |

## Table 1.2 - 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 CM satisfies Security Rules (Section 7.1) | None | None | TCG Level 0 Discovery:<br>FIPS Operating Mode Indicator (Byte 30, Bit 0) = 1 |
| Reset Module | Runs POSTs and zeroizes key & CSP RAM storage. | None | None | POR |
| Disable Services | Disables ATA Security commands until POR | None* | None | ATA SECURITY FREEZE LOCK |
| Exit FIPS Mode | Exit ATA Enhanced Security Mode.<br>Note: CM will enter uninitialized state. | None (using PSID) | None | TCG AdminSP.RevertSP() |
| FIPS 140 Compliance Descriptor | Reports FIPS 140 Revision, Overall Security Level, Hardware and Firmware versions, and Module name | None | None | ATA TRUSTED RECEIVE Protocol 0 |

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

| Table 2.1 - FIPS 140 Authenticated Services – TCG Opal Security Mode | | | | |
|---|---|---|---|---|
| Service Name | Description | Operator Access Control | Security Function | Command(s)/Event(s) |
| Set PIN | Change operator authentication data.<br>Note: Locking SP Admins can set PINs for any non-SUDR User or Locking SP Admin. | Locking SP Admin1-4, User1-16 (unless previously disabled by "Disable User Set PIN"),<br>Drive Owner | PBKDF, Symmetric Key | TCG Set Method |
| Disable User Set PIN | Disable a non-SUDR User's ability to change its own PIN. | Locking SP Admin1-4 | None | TCG Set Method |
| Enable / Disable Single User Data Range (SUDR) | Enable / Disable Single User Data Range (SUDR) classification for a data range | Locking SP Admin1-4 | None | TCG Reactivate 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 |
| Enable / Disable Admin SP Admin(s) | Enable / Disable an Admin SP Admin. | Drive Owner | None | TCG Set Method |
| Enable / Disable Locking SP Admin(s), non-SUDR User(s) | Enable / Disable a Locking SP Admin or non-SUDR User Authority. | Locking SP Admin1-4 | None | TCG Set Method |
| Set Range Attributes for non-SUDR | Set the location, size, locking and User access rights of the non-SUDR. | Locking SP Admin1-4 | None | TCG Set Method |
| Set Range Geometry for SUDR | Set the location and size of the SUDR. | User1-16 (if User Ownership), Locking SP Admin1-4 (if Admin Ownership), | 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. | User1-16,<br>Locking SP Admin1-4 (for non-SUDRs) | None | TCG Set Method, ATA SECURITY UNLOCK |
| User Data Read / Write | Encryption / decryption of user data to/from a LBA range.<br>Access control to this service is provided through Lock / Unlock User Data Range. | None* | Symmetric Key | ATA Read / Write Commands |
| Cryptographic Erase of non-SUDR | Erase user data in a non-Single User Data Range by cryptographic means: changing the encryption key. | User1-16,<br>Locking SP Admin1-4 | RNG, Symmetric Key | TCG GenKey Method |
| Cryptographic Erase of SUDR | Erase user data in a Single User Data Range by cryptographic means: changing the encryption key. | Locking SP Admin1-4 | RNG, Symmetric Key | TCG Erase Method |
| | | User1-16 | | TCG GenKey Method, TCG Erase Method |
| Set Admin SP PSK1-8 | Set Pre-Shared Key for Secure Messaging on Admin SP | Drive Owner | Symmetric Key | TCG Set Method |
| Set Locking SP PSK1-8 | Set Pre-Shared Key for Secure Messaging on Locking SP | Locking SP Admin1-4 | Symmetric Key | TCG Set Method |

### Table 2.1 - FIPS 140 Authenticated Services – TCG Opal Security Mode

| Service Name | Description | Operator Access Control | Security Function | Command(s)/Event(s) |
|---|---|---|---|---|
| Enable Secure Messaging | Set up secure communication channel with CM. | None | Key Agreement, Hashing, Symmetric Key | TCG StartTLS Method |
| Exit FIPS Mode | Exit TCG Opal Security Mode. Note: CM will enter uninitialized state. | Drive Owner | RNG, Hashing, Symmetric Key | TCG LockingSPObj.Revert(), TCG AdminSPObj.Revert() |
| | | Admin SP Admin1-4 | | TCG AdminSPObj.Revert() |
| | | Locking SP Admin1-4 | | TCG LockingSP.RevertSP() |

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

### Table 2.2 - FIPS 140 Unauthenticated Services – TCG Opal Security Mode

| Service Name | Description | Operator Access Control | Security Function | Command(s)/Event(s) |
|---|---|---|---|---|
| Unblock PIN | Resets password attempt counters. | None | None | POR |
| Show Status | Reports if CM satisfies Security Rules (Section 7.1) | None | None | TCG Level 0 Discovery:<br>FIPS Operating Mode Indicator (Byte 30, Bit 0) = 1 |
| Reset Module | Runs POSTs and zeroizes keys & CSPs in RAM | None | None | POR |
| FIPS 140 Compliance Descriptor | Reports FIPS 140 Revision, Overall Security Level, Hardware and Firmware versions, and Module name | None | None | ATA TRUSTED RECEIVE Protocol 0 |
| DRBG Generate Bytes | Returns a SP800-90 DRBG Random Number of 32 bytes | None | None | TCG Random() |
| Exit FIPS Mode | Exit TCG Opal Security Mode.<br>Note: CM will enter uninitialized state. | None (using PSID) | None | • AdminSP.RevertSP()<br>• AdminSPObj.Revert() |

## 4.2 Non-FIPS Mode Services

In the uninitialized state, the module supports the following services:

1. Services required to transition the CM to FIPS-Approved modes of operation.
2. Services related to firmware update.
3. Services related to unauthenticated encryption/decryption of user data.
4. Services related to cryptographic erase of user data.
5. Module reset.
6. Services related to status reporting.

All cryptographic algorithms used in FIPS-Approved operating modes are also available in this security uninitialized state.

## 4.3 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.
- Non-critical security parameters are not represented in this table.
- Read access of private values is 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 (Security Identifier), 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 | Exit FIPS Mode | X |
| Master, User MEK | ATA | MEK mixed with MEKEK | Private, AES Key, 256 bits | Master, User | Unlock User Data | X |
| Locking SP Admin1-4 Passwords | TCG | Locking SP Admins Auth. Data | Private, PIN, 32 bytes | Locking SP Admins | Set PIN | W |
| | | | | | Unlock User Data | X |
| Admin SP Admin1-4 Passwords | TCG | Admin SP Admins Auth. Data | Private, PIN, 32 bytes | Admin SP Admins | Set PIN | W |
| User1-16 Passwords | TCG | Users Auth. Data | Private, PIN, 32 bytes | Locking SP Admins, Users | Set PIN | W |
| | | | | | Unlock User Data | X |
| LBA Range MEKs | TCG | MEK mixed with MEKEK | Private, AES Key, | Locking SP Admins, Users | Unlock User Data | X |

## 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)** |
|---|---|---|---|---|---|---|
| | | | 512 bits | | | |
| ORG0-0 - ORG0-1 | Both | Firmware Load Test and Firmware Integrity Test Signature Verify Key | Public, RSA Key, 2048 bits | Drive Owner (enable FW download) | FW Download, Reset Module | X |
| MEKEK | Both | Media Encryption Key Encryption Key | Private, AES-256 Key | Locking SP Admins, Users | Unlock User Data | X |
| Admin SP PSK1-8 | TCG | Pre-Shared Keys | Private, 1-64 bytes | Drive Owner | Set Admin SP PSK1-8 | W |
| | | | | None | Enable Secure Messaging | X |
| Locking SP PSK1-8 | TCG | Pre-Shared Keys | Private, 1-64 bytes | Locking SP Admins | Set Locking SP PSK1-8 | W |
| | | | | None | Enable Secure Messaging | X |
| CSPSKs | Both | Critical Security Parameter Sanitization Keys | Private, AES 256 Key | Admin SP Admins, Locking SP Admins, Users, Drive Owner, Master | Unlock User Data, Cryptographic Erase, Set PIN | W, X |
| Entropy Input String | Both | Input to a DRBG mechanism of a string of bits that contains entropy* | Private, 32 bytes | None | Services which use the RNG (e.g., cryptographic erase) | X |
| Seed | Both | String of bits that is used as input to a DRBG mechanism* | Private, Hash seed, 56 bytes | None | Services which use the RNG (e.g., cryptographic erase) | X |
| Internal State | Both | Collection of stored information about DRBG instantiation* | Private, V (56 bytes) and C (55 bytes) | None | Services which uses the RNG (e.g., cryptographic erase) | X |
| PBKDF Master Key | Both | Transient key generated by PBKDF | Private, 32 bytes | None | Set PIN, Unlock User Data | X |
| Secure Messaging Session Key | TCG | Derived session unique key | Private, 16 or 32 bytes | None | Enable Secure Messaging | X |

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

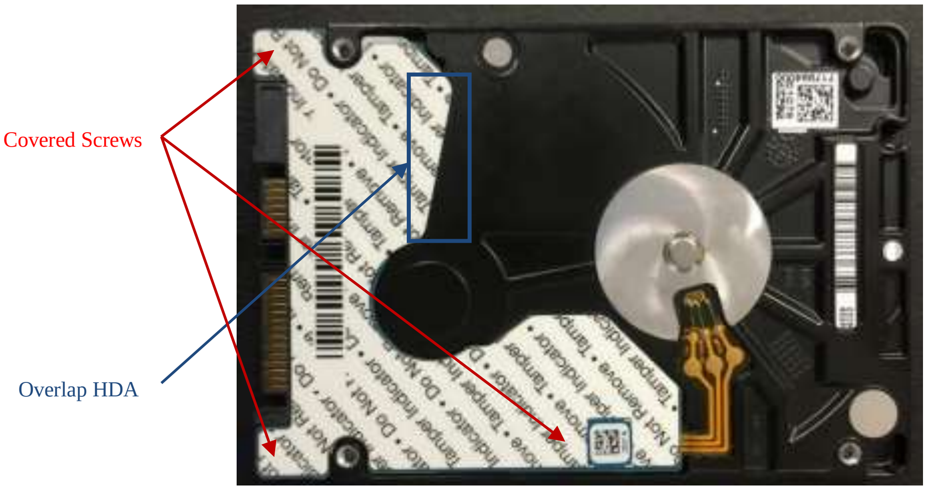
# 5 Physical Security

## 5.1 Mechanisms

The CM has the following physical security:

Production-grade components with standard passivation

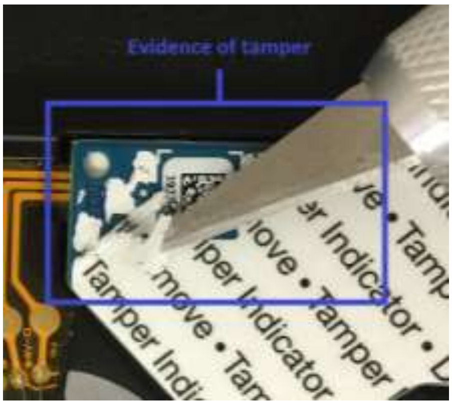
- Opaque, tamper-evident, security label on the exposed (back) side of the PCBA applied by Seagate manufacturing prevents electronic design visibility and protects physical access to the electronics by board removal
- Tamper-evident security labels applied by Seagate manufacturing prevent HDA cover removal 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

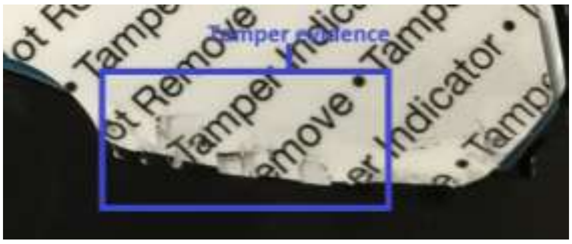


## 5.2 Operator Requirements

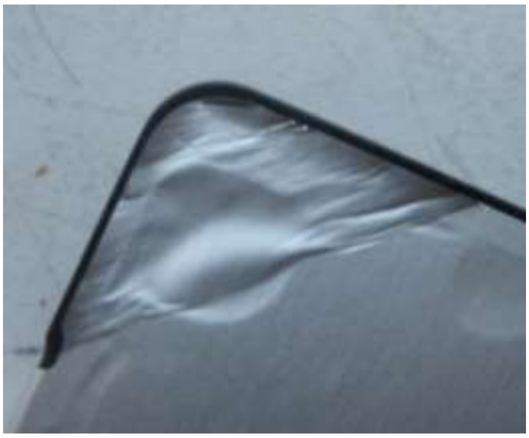
The operator is required to inspect the CM a minimum of once every six months for one or more of the following tamper evidence:

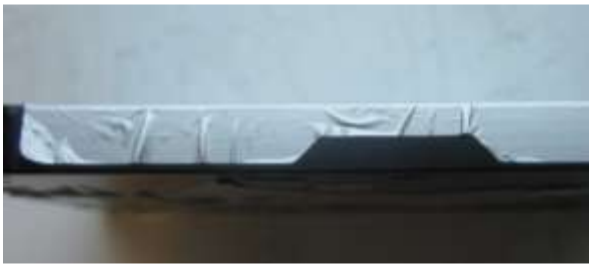
- Checkerboard pattern on security label or substrate
- Security label over screws at indicated locations is missing or penetrated
- Text (including size, font, orientation) on security label does not match original
- Security label cutouts do not match original





- Creasing or crinkling of top cover seal





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 “limited operational environment”. That is, while the module is in operation the operational environment cannot be modified and no code can be added or deleted. FW can be upgraded (replaced) with a signed FW download operation. If the code download is successfully authenticated then the module will begin operating with the new code image.

# 7 Security Rules

## 7.1 Secure Initialization

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

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

1. COs: At receipt of the product examine the shipping packaging and the product packaging to ensure it has not been accessed during shipping by the trusted courier.
2. COs and Users (either mode): At installation and periodically examine the physical security mechanisms for tamper evidence.
3. Transition the CM to one of the Security Modes by doing one of the following:
   - ATA Enhanced Security Mode: User Set PIN.
   - TCG Opal Security Mode: Drive Owner executes Activate method on Locking SP
4. Power-on reset to execute Self-Tests.
5. 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 Opal Security Mode: Drive Owner, Admins and Users
6. COs (Locking SP Admins) for TCG Opal Security Mode: Set ReadLockEnabled and WriteLockEnabled to “True” on at least one data range and it must not be modified.
7. TCG Opal Security Mode: Drive Owner: At installation, disable the “Makers” authority.
8. At installation, the value of LockOnReset for FW Download must be set to “Power Cycle” and it must not be modified.
9. At installation, the value of PortLocked for FW Download must be set to “TRUE”.
10. After secure initialization is complete, do a power-on reset or close all open TCG sessions to clear authentications established during initialization.

    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.

## 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.

# 8 Mitigation of Other Attacks Policy

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