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

Security Level 2

Rev. 0.9 – November 12, 2012

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 Pulsar.2 SSD 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	2
Cryptographic Module Ports and Interfaces	2
Roles, Services and Authentication	2
Finite State Model	2
Physical Security	2
Operational Environment	N/A
Cryptographic Key Management	2
Electromagnetic Interface / Electromagnetic Compatibility (EMI / EMC)	3
Self – tests	2
Design Assurance	2
Mitigation of Other Attacks	N/A

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

1.3 References

1. FIPS PUB 140-2
2. Derived Test Requirements for FIPS PUB 140-2
3. Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program
4. TCG Storage Security Subsystem Class: Enterprise, Specification Version 1.0, Revision 3.00, January 10, 2011
5. TCG Storage Architecture Core Specification, Specification Version 1.0, Revision 0.9, May 24, 2007
6. TCG Storage Interface Interactions Specification, Specification Version 1.0,
7. SCSI Primary Commands-4 Rev 15 (SPC-4)
8. SCSI Block Commands Rev15 (SBC-3)
9. 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
CSPSK	Critical Security Parameter Sanitization Key
DRBG	Deterministic Random Bit Generator
MEK	Media Encryption Key
FIPS 140	FIPS 140-2
HDD	Hard Disk Drive
IV	Initialization Vector for encryption operation
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
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)
SSD	Solid State Drives

2 Cryptographic Module Description

2.1 Overview

The Seagate Secure® TCG Enterprise SSC Self-Encrypting Drive FIPS 140 Module is embodied in Seagate **Pulsar.2 SSD** 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, 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 protocols.

The CM has a multiple-chip embedded physical embodiment. The physical interface to the CM is a SAS connector. The logical interfaces are the industry-standard SCSI (refer to Section1.3, items 7 & 8), TCG SWG (refer to Section1.3, item 5), and Enterprise (refer to Section1.3, item 4) protocols, carried on the SAS (refer to Section1.3, item 9) 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	SAS Connector
Data Output	SAS Connector
Control Input	SAS Connector
Status Output	SAS Connector, LED
Power Input	Power Connector

2.3 Product Versions

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

- Pulsar.2, 2.5-Inch, SAS Interface, 800 GB
  - 800 GB: 1BU282
  - FW Versions: 0003

2.4 FIPS Approved Algorithms

Algorithm	Certificate Number
ASIC AES	#1811
Firmware AES	#1343
RSA	#650
SHA	#1225
800-90 DRBG	#62

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
Firmware AES	Power-On	Encrypt and Decrypt KAT performed	Enters FIPS Self Test Error State
RSA	Power-On	Sign Verify KAT performed.	Enters FIPS Self Test Error State

SHA-1	Power-On	Digest KAT performed	Enters FIPS Self Test Error State
SHA-256	Power-On	Digest KAT performed	Enters FIPS Self Test Error State
800-90 DRBG	Power-On	DRBG KAT performed	Enters FIPS Self Test Error State
Firmware Integrity Check	Power-On	16-bit CRC and ECC	Enters FW Integrity Error State
Firmware Load Check	Conditional: When new firmware is downloaded	RSA PKCS#1 signature verification of new firmware image is done before it can be loaded.	Firmware download is aborted.
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.
Non-Approved NDRNG	Conditional: When a non-Approved 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.

2.6 FIPS 140 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.

There is 1 approved mode of operation, “TCG Security”.

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).

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 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.

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 (0-15) (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 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.

3.1.3 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.

The module has been tested for Security Level 2 compliance in accordance to FIPS 140-2 Standard.

3.2.2 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.

3.2.3 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. The PINs have a maximum length of 32 bytes.

Per the policy security rules, the minimum PIN length is 4 bytes (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 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.

3.2.4 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.

4 Access Control Policy

4.1 Services

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

- Use of the services described below is only compliant if the module is in the noted Approved mode.
- Underlying security functions used by higher level algorithms are not represented (e.g. hashing as part of asymmetric key)
- Operator authentication is not represented in this table.
- Some security functions listed are used solely to protect / encrypt keys and CSPs.
- Service input and output details are defined by the TCG and SCSI 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 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
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
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
Cryptographic Erase	Erase user data in an LBA range by cryptographic means: changing the Media encryption key (MEK). 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.	None	None	TCG Level 0 Discovery
Reset Module	Runs POSTs and zeroizes key & CSP in 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()

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

4.2 Cryptographic Keys and CSPs

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

- The use of PIN CSPs for authentication is implied by the operator access control.
- The Set PIN service is represented in this table even though generally it is only used at module setup.
- All non-volatile storage of keys and CSPs is in the system area of the drive media to which there is no logical or physical access from outside of the module.
- The module uses SP 800-90 DRBG and adopts Hash_DRBG mechanism.
- 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	**Description**	**Type (Pub / Priv, key / CSP (e.g. PIN)), size**	**Operator Role**	**Services Used In**	**Access **(W, X)**	**Zeroization**
SID (Secure ID), aka Drive Owner PIN	Auth. Data	Private, PIN, 32 bytes	Drive Owner	Set PIN	W	Revert SP
EraseMaster	EraseMaster Auth Data	Private, PIN, 32 bytes	EraseMaster	SetPIN	W	Revert SP
BandMaster 0-15 Passwords	Users Auth. Data	Private, PIN, 32 bytes	BandMasters	Set PIN	W	Revert SP
LBA Range MEKs	MEK (per LBA band)	Private, AES Key, 256 bits	Users	Unlock User Data	X	Revert SP, Cryptographic Erase
Entropy Input String	*Input to a DRBG mechanism of a string of bits that contains entropy	Private, 72 bytes	None	Services which use the RNG (e.g; cryptographic erase)	X	Reset
Seed	*String of bits that is used as input to a DRBG mechanism	Private, Hash seed, 96 bytes	None	Services which use the RNG (e.g. cryptographic erase)	X	Reset
Internal State	*Collection of stored information about DRBG instantiation	Private, V and C	None	Services which uses the RNG (e.g. cryptographic erase)	X	Reset
ORG 0-0 - ORG 0-3	Firmware Load Test Signature Verify Key	Public, RSA Key, 2048 bits	Drive Owner (enable FW download)	FW Download	X	None (Public)
CSPSKs	Critical Security Parameter Sanitization Keys	Private, AES Key, 256 bits	None	Set PIN	X	Revert SP, Cryptographic Erase

* 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 Revert 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
- Tamper-evident security labels applied by Seagate manufacturing prevent top and bottom cover removal for access or visibility to the media
- Exterior of the drive is opaque
- The tamper-evident labels cannot be penetrated or removed and reapplied without tamper-evidence
- The tamper-evident labels cannot be easily replicated with a low attack time
  - Security label on sides of drive provide tamper-evidence of top and bottom cover removal

Figure 1: Top view of tamper-evidence label on sides of drive

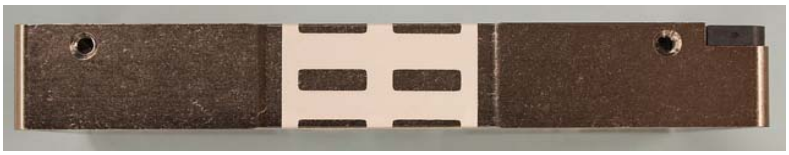


Figure 2: Left-side view of tamper-evidence label on left side of drive

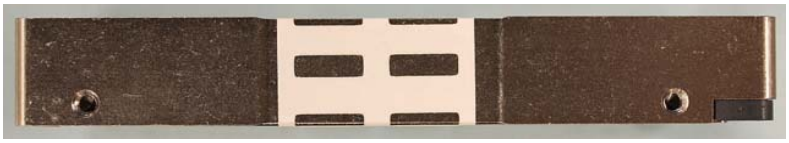


Figure 3: Right-side view of tamper-evidence label on right side of drive

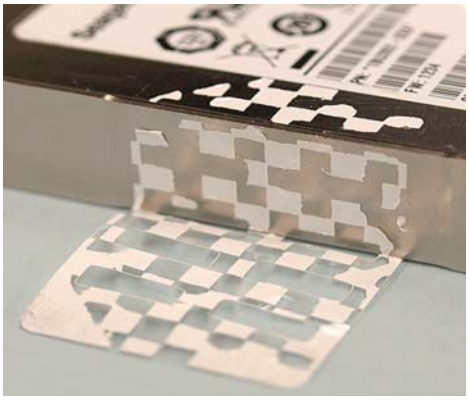
5.2 Operator Requirements

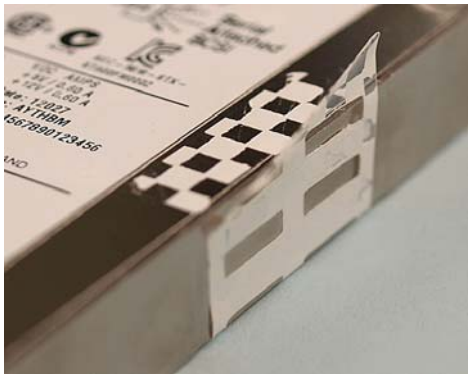
The operator is required to inspect the CM periodically for one or more of the following tamper evidence:

- Checkerboard pattern on security label
- Security label cutouts do not match original

Checkerbox Pattern

Tamper Evidence





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. COs and Users: At installation, set all operator PINs applicable for the FIPS mode to private values of at least 4 bytes length:
   - TCG Security: Drive Owner, EraseMaster and BandMasters
3. Drive Owner: At installation, disable the "Makers" authority (defined in TCG Core Specification [refer to Section1.3, item 5]).
4. At installation, the value of LockOnReset (defined in TCG Core Specification [refer to Section1.3, item 5]) for FW Download must be set to "Power Cycle" and it must not be modified.
5. 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.