Seagate Secure® Cheetah® Self-Encrypting Drive FIPS 140 Module

FIPS 140-2 Security Policy

Rev. 1.9 – Mar. 15, 2010

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® Cheetah® Self-Encrypting Drive (SED).

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.

1.2 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 Workgroup, Security Subsystem Class: Enterprise, Specification Version 1.0, Revision 1.0, January 27, 2009
5. TCG Storage Workgroup Specification Overview and Core Architecture Specification, Specification Version 1.0, Revision 0.9 – draft, May 24, 2007
6. TCG Storage Interface Interactions, Revision 1.0, January 27, 2009
7. [ANSI /INCITS T10/1731-D], Information technology - SCSI Primary Commands – 4 (SPC-4), Revision 15, 20 June 2008

1.3 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
DEK	Data encryption key
FC	Fibre Channel
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
mSID	Manufactured SID, public drive-unique PIN, TCG term
POST	Power on self-test
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)

2 Cryptographic Module Description

2.1 Overview

The Seagate Secure Cheetah Self-Encrypting Drive FIPS 140 Module is embodied in Seagate Cheetah 15K.7 FC SED model disk drives. These products meet the performance requirements of the most demanding mission critical 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 an industry-standard TCG Enterprise SSC interface.

The CM has multiple-chip embedded physical embodiments. The physical interface to the CM is the Fibre Channel connector which the host system uses to power and communicate with the drive as a storage system. The logical interface is the SCSI (7), TCG SWG (5) , and Enterprise SSC (4) protocols. 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, 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 ASIC is an SoC which has the following major logical functions: host interface using an industry standard FC 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-128, is implemented in the data encryption engines.

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: SCSI interface, 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 SCSI write/read commands respectively. Other security operations, including authentication and management of cryptographic secrets, are accessed using SCSI SECURITY PROTOCOL IN / OUT commands. These commands are actually wrappers for another industry standard protocol: TCG Enterprise SSC. The security services provided by the CM through the TCG protocol correspond to the methods of the following SP Templates: Base, Admin, Locking, and Crypto. Some of the TCG-based services are specific to the Seagate implementation and are described in detail in product documentation.

2.2 FIPS 140 Approved Mode of Operation

The CM has one FIPS 140 “Approved mode of operation”. This mode provides both FIPS 140 services and other services which are not security related. The CM does not provide any security services that use non-Approved security functions. After the module is installed and configured per the Security Rules of this policy (see section 7, the drive is always in the Approved mode of operation except when a critical failure has been detected, causing a transition to the “Failed” state.

The operator can determine the operational state by the vendor unique “Device Security Life Cycle State” field of Enterprise SSC “Level 0 Discovery” operation. If the state reported is any value other than 0x80 (“Use”) then the device is not in the Approved mode of operation. Note that if a critical failure has occurred, including a FIPS 140 self-test failure, then the failure condition will persist across power-cycles (resets).

3 Identification and Authentication Policy

3.1 Roles, Authentication Type, and Authentication Data

3.1.1 Authentication in TCG

Operator authentication is provided via the TCG Authenticate method used in a TCG Session to the appropriate TCG Security Provider (SP) as defined by Enterprise SSC [4]. The host application can have only a single session open at a time. During a session the application can invoke services for which the operator has access control. Note that a security rule of the CM is that the host must not authenticate to more than one operator 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.

3.1.2 Authentication Mechanism and Data

Operator authentication with PINs is implemented by hashing the operator-input value and comparing to the stored hash of the assigned PIN. The PINs have retry attributes (which persist across resets, see TCG Core Spec [5]) that control the number of consecutive unsuccessful attempts before the module blocks subsequent authentication is blocked. The PINs can be up to 32 bytes; therefore the probability that a random attempt will succeed is $1/2^{256}$. Per the policy security rules, the minimum PIN length is 4 bytes to meet FIPS 140 authentication strength requirements for a single random attempt; i.e. $1/2^{32}$, which is less than 1/1,000,000. With a 4 byte PIN value and the PIN attribute *TryLimit* set to default of 1024 the probability of multiple random attempts to succeed is $1024 * (1/2^{32})$, which is less than 1/100,000.

3.1.3 Factory-installed PIN values

The initial value for all operator PINs is the same as the value for MSID (manufacturing Secure ID). This is a device-unique, 32-byte, public value. The value is printed on the drive label (identified as SID) and can be read by the host application at any time with a non-security operation. The security rules (7) for the CM require that the PIN values must be "personalized" to private values using the "Set PIN and retry attributes" service.

3.1.4 Crypto Officer Roles

3.1.4.1 Drive Owner

This CO role corresponds to SID (Secure ID) role as defined in Enterprise SSC [4]. This role is used to download a FW image. An operator is authenticated to this role with role-based authentication. Note: only the validated firmware can be loaded to the module. Otherwise, the module is not operating in FIPS mode.

3.1.4.2 EraseMaster

This CO role corresponds to same named role as defined in Enterprise SSC [4]. This role is used to enable/disable BandMasters, set PIN retry attributes, and erase user data region (LBA band). An operator is authenticated to this role with role-based authentication.

3.1.5 User Roles

3.1.5.1 BandMasters

This user role corresponds to the same named role as defined in Enterprise SSC [4]. The 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 1-16 user data bands, which are controlled by their respective BandMasters. By default, the BandMasters for the "Global_Range" (BandMaster0) and "Band 1" are enabled. BandMasters (and thus bands) 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.

4 Access Control Policy

4.1 Services

The following table represents the FIPS 140 services in terms of the Approved Security Functions and operator access control. Note the following:

- 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 SSC 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 - FIPS 140 Services

Service Name	Description	Operator Access Control	Security Function	Command
Set PIN and retry attributes	Operator authentication data changed by the corresponding operator. BandMaster PIN retry attributes can only be changed by EraseMaster	All	Hashing, Symmetric Key	TCG Set Method
Lock / Unlock FW Download Port	Enable / Disable FW Download Service	Drive Owner	None	TCG Set Method
Lock FW Download Port on Reset	State of FW Download Service after reset.	Drive Owner	None	TCG Set Method
Firmware Download	Load complete firmware image. If the self-test of the code load passes then the device is reset and will run with the new code. Access control to this service is provided through Lock / Unlock FW Download Port.	None *	Asymmetric Key	SCSI Write Buffer
Enable / Disable BandMaster	Enable / Disable a BandMaster Authority. Allows a band to be configured (position and size) for use.	EraseMaster	None	TCG Set Method
Set Band position and size	Set the location and size of the LBA band.	BandMasters	None	TCG Set Method

Table 1 - FIPS 140 Services

Service Name	Description	Operator Access Control	Security Function	Command
Lock / Unlock User Data Band	Block or allow read (decrypt) / write (encrypt) of user data in a band. Locking also requires read/write locking to be enabled.	BandMasters	None	TCG Set Method
User Data Read (decrypt) / Write (encrypt)	Encryption / decryption of user data to/from a LBA band. Access control to this service is provided through Lock / unlock User Data Band.	None *	Symmetric Key	SCSI Read, Write, Pre-fetch, Reassign, Verify, Commands
Cryptographic Erase	Erase user data in an LBA band by cryptographic means: changing the encryption key. BandMaster PIN is also reset.	EraseMaster	RNG, Symmetric Key	TCG Erase Method
Show Status	Reports “drive security life cycle state” (corresponds to FIPS 140 mode)	None	None	TCG Level 0 Discovery
Reset (run POSTs)	Runs POSTs and zeroizes keys & CSPs in RAM	None	None	Power on reset

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 generation, input / output, storage and zeroization. Note the following:

- The use of PIN CSPs for authentication is implied by the operator access control
- 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.
- Non-critical security parameters are not represented in this table.
- Read access of private values are internal only to the CM.
- There is no security-relevant audit feature.

Table 2 – “Key Management”

Name	Description	Type (Pub / Priv, Key / CSP)	Operator Role	Services Used In	Access (R,W,Z)	Lifecycle				
						Creation (Generation / Modification)	Storage	Storage Form (Plaintext / Encrypted)	Entry / Output	Zeroization
mSID	Mfg Secure ID	Public, 32 bytes	None	Device Identification (not a security function)	R	Mfg - Drive Unique	Media (System Area)	Plaintext	Output: Host can retrieve	None - Public value

Table 2 – “Key Management”

Name	Description	Type (Pub / Priv, Key / CSP)	Operator Role	Services Used In	Access (R,W,Z)	Lifecycle				
						Creation (Generation / Modification)	Storage	Storage Form (Plaintext / Encrypted)	Entry / Output	Zeroization
SID	Secure ID, Drive Owner auth. data	Private, CSP (PIN), 32 bytes	Drive Owner	Set PIN	W	Mfg - Drive Unique, Operator set by electronic input	Media (System Area)	SHA digest	Entry: Electronic Input from Host Output: none	None – logically protected
BandMaster IDs (N=16)	User auth. data (per LBA Bands)	Private, CSP (PIN), 32 bytes	BandMaster	Set PIN	W	Mfg - Drive Unique, Host changed by electronic input	Media (System Area)	SHA digest	Entry: Electronic Input from Host Output: none	Crypto Erase
			EraseMaster	Crypto Erase	W					

Table 2 – “Key Management”

Name	Description	Type (Pub / Priv, Key / CSP)	Operator Role	Services Used In	Access (R,W,Z)	Lifecycle				
						Creation (Generation / Modification)	Storage	Storage Form (Plaintext / Encrypted)	Entry / Output	Zeroization
EraseMaster ID	EraseMaster auth data	Private, CSP (PIN), 32 bytes	EraseMaster	Set PIN	W	Mfg - Drive Unique, Host changed by electronic input	Media (System Area)	SHA digest	Entry: Electronic Input from Host Output: none	None – logically protected
FDE Keys (N=16)	DEKs (per LBA Band)	Private, AES-128 Keys	EraseMaster	Crypto Erase	Z	Mfg - using CMs RNG, RNG regeneration by zeroization	Media (System Area)	Plaintext	None	Crypto Erase
			None, subject to band lock state	Read / Write User Data between host and media	R					
ORG0-0 - ORG0-3 (N=4)	Public keys for code load self-test	RSA-2048, Public Keys	None, subject to fw download port lock state	FW Download	R	Mfg	Media (System Area)	Plaintext	None	None - Public value

Table 2 – “Key Management”

Name	Description	Type (Pub / Priv, Key / CSP)	Operator Role	Services Used In	Access (R,W,Z)	Lifecycle				
						Creation (Generation / Modification)	Storage	Storage Form (Plaintext / Encrypted)	Entry / Output	Zeroization
Seed Key (XKEY)	seed key for RNG	Private, CSP, 64 bytes	No role	All RNG uses	R, W	Set to RNG state at each RNG usage	RAM	Plaintext	None	Transient - Cleared after used
Seed	seed for RNG	Private, CSP, 520 bytes	No role	1st RNG use after reset	R	Entropy collected at power-up.	RAM	Plaintext	None	Transient - Cleared after used

4.3 Non-Critical Security Parameters

This section lists the security-related information which do not compromise the security of the module.

- AES IV
  The CM HW AES IV (CBC mode) is derived from the LBA of the data on the media.
- PIN Retry Attributes – TryLimit and Persistence
  These parameters affect the handling of failed authentication attempts.

5 Physical Security

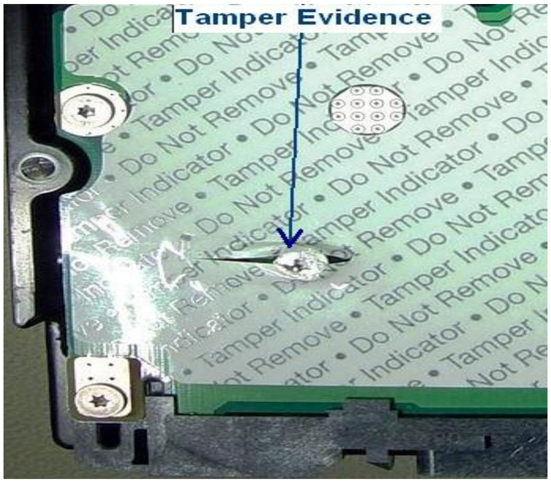
5.1 Mechanisms

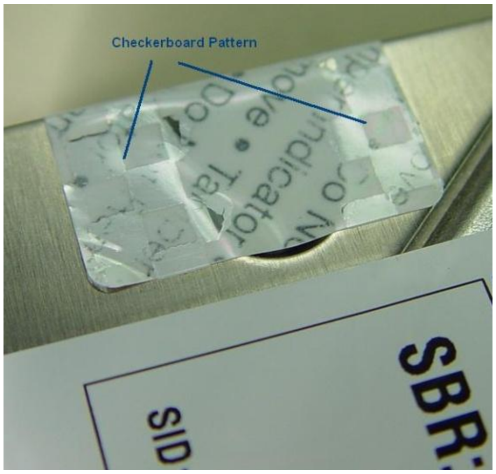
The CM has the following physical security:

- Production-grade components with standard passivation,
- Opaque, tamper-evident, security label on the exposed (back) side of the PCBA which prevents electronic design visibility and protects physical access to the electronics by board removal ,
- Tamper-evident security labels that 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

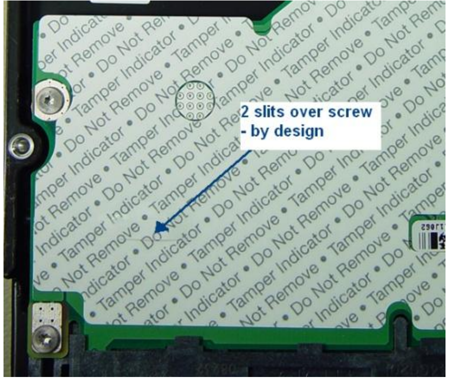
The operator is required to inspect the CM periodically for one or more of the following tamper evidence:





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

- Penetration of the security label, *except where indicated below*



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

6 Operational Environment

The FIPS 140-2 Section 4.6 Operational Environment requirements are not applicable because the CM operates in a "limited operational environment". That is, while the module is in operation the FW cannot be changed and no code can be added or deleted. FW can be upgraded (replaced) with a signed FW download operation, to take effect upon the next power-up.

7 Security Rules

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. Users: At installation and periodically confirm drive is in FIPS approved mode with the Show Status service.
3. COs and Users: At installation, set PINs (i.e., SID, EraseMaster, BandMasters) to private values of at least 4 bytes length.
4. Drive Owner: At installation, disable the "Makers" authority (using SID_Set_Makers ACE to the Admin SP). To query this setting, perform the Get method for the Makers authority on the Admin SP, specifying the "enabled" column.
5. Users: Do not change Band attribute "LockonReset" from the default value of TRUE. To query this attribute, perform the Get method on the Locking SP, for the locking table row representing the band, specifying the "LockOnReset" column. The return value will indicate a set containing the value 0x00 if the LBA range locks when a power cycle occurs
6. COs and Users: A TCG session must only be authenticated to a single operator role.

8 Mitigation of Other Attacks Policy

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