Momentus® FDE

Attached Storage Drives

FIPS 140 Module Security Policy

Rev. 1.7 – June 29, 2011

Seagate Technology, LLC

Table of Contents

1 Introduction

1.1 Scope

This security policy applies to the FIPS 140-2 Cryptographic Module (CM), Seagate® Momentus® FDE Attached Storage drives.

This document meets the requirements of the FIPS 140-2 standard (Appendix C) and Implementation Guidance (section 14.1). For details needed to develop a compliant application see the referenced technical specifications.

1.2 Document 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. ATA-8 ACS
5. Serial ATA Rev 2.6 (SATA)
6. DriveTrust SDK SeaCOS Command Reference Manual
7. DriveTrust Life Cycle Manual
8. EXTERNAL-FDE dCard Life Cycle Manual
9. ISO/IEC 7816-4

1.3 Acronyms

3DES	Triple DES
AES	Advanced Encryption Standard (FIPS 197)
APDU	Application Protocol Data Unit (ISO 7816)
CM	Cryptographic Module
CO	Crypto-officer
CSP	Critical Security Parameter
dCard	disc Card, virtual Smart Card
DEK	Data encryption key
FDE	Full Disk Encryption
HDA	Head and Disk Assembly
HDD	Hard Disk Drive
KAT	Known Answer Test
LBA	Logical Block Address
mSID	Manufactured SID, public drive-unique PIN
PBA	Preboot Application
POR	Power-on reset (ATA defined)
POST	Power on self-test
RNG	Random Number Generator
SeaCOS	Seagate Card Operating System
SID	Security ID, PIN for Drive Owner CO role
SoC	System-on-a-Chip
TE	Trusted Exchange (ATA Trusted Send/Receive sequence)
XF	Extended Filesystem (of dCards)

2 Cryptographic Module Description

2.1 Overview

The Momentus® FDE Attached Storage Drive is a FIPS 140-2 Level 2 module which provides full disk encryption with operator authentication. It is designed to prevent data breaches due to loss or theft on the road, in the office. The cryptographic module provides a wide range of cryptographic services using FIPS approved algorithms in a FIPS-Approved mode. Services include hardware-based data encryption, instantaneous user data disposal with cryptographic erase, device identification, and authenticated FW download. The services are provided through industry-standard ATA / SATA interfaces.

The module is a multiple-chip embedded physical embodiment, and the physical boundary of the CM is the entire HDD. The module can be enclosed in external hard drive products with an external case, USB bridge (connector, board and firmware) and software applications, which are all not included in the CM boundary or the scope of this validation. The physical interfaces to the CM are the SATA connector, power connector and jumper block pins. The logical interface is the industry-standard ATA command set (Doc Ref. 4), with vendor-unique extensions, carried on the SATA transport interface (Doc Ref. 5), through the SATA connector. 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 CM functionality is implemented in the ASIC, Serial Flash, SDRAM and firmware. 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 from outside the CM and not accessible through any CM service.

The ASIC is a SoC which has the following major logical functions: host interface using an industry-standard SATA interface, a RW Channel interface to the HDA, an interface to media motor controller, a data encryption engine, and processing services which execute the firmware. An Approved Security Function, AES-128, is implemented in the data encryption engine. During drive operation, the SDRAM hosts some of the firmware and the encrypted user data being transferred between the media and the ASIC.

Security functions of the firmware can be categorized into the following groups: ATA security commands, ATA read / write commands, misc ATA commands and Seagate proprietary security protocol commands (DriveTrust) sent through the ATA Trusted Exchange interface. The Seagate security protocol is implemented by a subsystem called SeaCOS. This protocol is an implementation of the ISO 7816 standard for Smart Cards. The architecture provides virtual Smart Cards, dCards, with file systems in a reserved area of the disc media. The host application interface with the file systems is through a command-response mechanism referred to as APDUs. The FIPS-approved mode in this certification is supported by 3 Seagate provided dCards: Admin, FDE and User. The User dCard is only used to store password hints and track if the drive has been configured (user password changed from default value); it provides no cryptographic services.

The drive also includes software applications which run on the host computer to provide a user interface to some of the functions. However, these applications are not within the logical boundary of the FIPS module; they do not execute on the processor of the hard drive. They are host applications which are bundled with (written on) the drive; see section 2.5. Other applications could additionally be used to interact with the CM. This security policy describes the FIPS 140 capabilities available to any application.

Any application software included on the disc media (host applications) are considered out of scope and not validated.

2.2 Hardware and Firmware Versions

The Momentus® FDE Attached Storage Drive, FIPS 140 Module is identified as HW version (Model #) ST9500326AS, FW version (config) 566.

2.3 FIPS 140 Approved Mode of Operation

By following the Security Rules (Section 8) in this document, an operator can operate the CM in FIPS 140 compliant manner (an "Approved mode" of operation). The module's FIPS mode of operation is enforced both through configuration and through policy. Violating the policy (detailed in Section 8) is equivalent to operating the product in a non-compliant manner.

If a FIPS self-test fails, either at power on or during operation, then the CM will enter an error state. From this error state, all services except show status are disabled. The host can reset the CM with a power cycle in attempt to clear the error state. If the POSTs succeed, then the CM has recovered from the error. Otherwise, the drive can no longer operate in FIPS mode. Note that these errors are very rare, but if they occur they will likely be accompanied by other failures.

FIPS approved services are provided through industry-standard ATA commands, SeaCOS APDUs addressed to the Admin dCard (resident on the drive), and SeaCOS APDUs addressed to the *FDE dCard* (resident on the drive). Note, some ATA Security commands are disabled in this product and their functionality is provided through the APDUs.

2.4 Services Disabled in Manufacturing

This product shares an architecture with Momentus internal drives which have different use cases. Some of the functionality differences are implemented in firmware while others are provided through different manufacturing processes related to the files on the dCards. Specifically the FDE dCard used for this product is created in the factory and has some differences from an FDE dCard created on internal drives (by applications). These differences are in access control, file activation state, and device file operations. Of particular note is that certain features, while implemented in the firmware, are not accessible because the operator authentication for the FDE dCard Owner role is disabled during manufacturing. Additionally, some files storing key values are deactivated and thus cannot be set to private values or referenced by services. For completeness purposes all functionality possible in the FW is described, independent of the fact that the services are disabled. The following are the services which are *disabled* in this product (also noted in Services and Key Management sections):

- Key Inject
- Secure Messaging
- Set PIN for FDE dCard Owner: EF-CARD-OWNER
- Setting or Referencing private key values used in Key Inject and Secure Messaging: EF-EXCHANGE-KEY, EF-RSA-VERIFY, EF-3DES-DRIVE-TO-HOST, EF-3DES-HOST-TO-DRIVE, and EF-3DES-DL-HASH

2.5 "Preboot" (LBA Remapping Function) for Data Access Control

The CM provides several mechanisms for the Lock/Unlock User Data service. One of the methods is an indirect effect of mapping the storage space available for the host from two different areas of the drive: 1) XF space of the dCard filesystem, 2) the "user data area". The XF that can be addressed is referred to as the "preboot area" because for internal drives an application can be executed under control of a BIOS *before* the operating system is loaded ("booted"). This capability of the drive firmware to address the preboot area instead of the user area with the same LBA addressing is called "LBA remapping".

When the LBA space is mapped to the preboot area the user area is unavailable and vice versa. This then provides a means for access control of reads and writes (always encrypted) of the user data. The LBA mapping is host controlled by a "device file" on the FDE dCard (EF-USER-LOCK or EF-LBA-REMAPPING-BYPASS). The host application controls this setting by writing to the file.

The purpose of this capability is to allow a host to have a read-only application in a secure area of the drive such that a host BIOS or operating system will execute the application automatically upon detection of the connection of the drive. In the case of attached storage drives, the host operating system will often see the drive as a CD and "autorun" the application loaded in the preboot area. The preboot application is typically used to "configure" the security of the drive and unlock the "user area" for access. The "unlock" operation is accomplished by switching the LBA addressing from the preboot area to the user area.

The CM is customized for an attached storage drive product during manufacturing with the placement of a host application in the preboot area and LBA Remapping enabled when the FDE dCard is created. Thus, when the drive is connected to a host, the operating system will automatically execute the preboot application and will not have access to the user data. The first time the drive is connected to the host the application will present a user interface to set the authentication data (drive owner, master and user passwords) for the CM. Subsequently the application will present a user interface to authenticate the user and "bypass" the LBA Remapping setting, thus unlocking the user data. However, as described in the overview section above, the host applications are not part of the CM and thus the operator interface to the drive may vary.

2.6 User Data Cryptographic Erase Methods

All user data is internally encrypted / decrypted by the CM for storage / retrieval on the drive media. As a result, the data can be effectively erased by changing the encryption key, DEK, and discarding the previous value. Thus, the FIPS 140 key management capability "zeroization" of the key erases all the user data. Of course the user data can also be erased by overwriting, but this can be a long operation on high capacity drives.

The Cryptographic Erase feature is available with 2 methods (device files) each with different access controls: one is available to the Master role, the other is for the Secure Erase Master role. The 2nd method can be provided as an unauthenticated service depending on the module setup; i.e. if the default PIN for the role is set to a private value.

3 Identification and Authentication (I&A) Policy

3.1 Operator Roles

Note: The following identifies the CO roles with a *general* description of the purposes. For further details of the Approved Security services performed by each role, as well as security related services which do not require an operator role, see section 4.1

3.1.1 Crypto Officer Roles

3.1.1.1 Drive Owner

This role has the ability to enable or disable the FW download service.

3.1.1.2 FDE dCard Owner

This role is disabled during manufacturing. To authenticate to this role, a random value needs to be supplied. However, this random value is generated and discarded at manufacturing, effectively disabling this role. As such, the end user has no knowledge of this value and cannot authenticate to this role.

This role has the ability to enable or disable the Key Inject Service. This service allows the operator to optionally inject (electronically input) a data encryption key (DEK). As described above, though implemented in the firmware, the CM is manufactured with this role and the services provided to this role disabled. See section 2.4.

3.1.1.3 Masters (4)

This role is used to enable/disable Master, User and Secure Erase Master IDs with the Set PIN service. It is also used to erase data that has been written to the drive by zeroizing the DEK with the Cryptographic Erase service. There are 4 Master IDs.

3.1.2 User Roles

3.1.2.1 Users (4)

This role can unlock (and also lock) the drive so that an operator can read and write data to the drive. There are 4 User IDs.

3.1.2.2 Secure Erase Master

This role can erase data that has been written to the user area of the drive by zeroizing the DEK. Note that if the default authentication data for this role is not changed at Secure Initialization then this role is effectively unauthenticated (by virtue that the default value is printed on the drive label; identified as “SID”).

3.1.3 Unauthenticated Role

This role can perform Show Status services and Device Identification. If this operator has physical access to the drive, this role can also power cycle the drive as well as configure the jumper block to control the interface speed between the host and drive (a non-security relevant service).

3.2 Authentication

3.2.1 Authentication Types

The CM supports role-based and identity-based authentication. The Drive Owner and Secure Erase Master role use role-based authentication as there is only one ID and one PIN. There are 4 Master and User operators. Each of these operators is assigned a unique ID to which a PIN is associated, thus this provides identity-based authentication.

3.2.2 Authentication in ATA Security Commands

Authentication supplied for certain ATA Security commands is provided through a PIN provided in the ATA Security command parameters, as defined in Doc. Ref. 4. In the event of authentication failure, the ATA

command will abort. A password attempt counter is implemented as specified in ATA, which when reached, blocks User service authentication (with command abort), until the module is reset (Unblock PIN service).

3.2.3 Authentication for DriveTrust Commands

Authentication for services provided through DriveTrust commands is provided through a PIN provided in the Verify PIN APDU command, as defined in Doc. Ref.6. In the event of authentication failure, the response message will indicate the failure. If the operator role does not have access to the subsequent service then the command will similarly fail. A password attempt counter is implemented, which when reached, blocks User service authentication (with corresponding response indication), until the module is reset (Unblock PIN service). Depending on a module setting (FDE dCard file EF-ATA-SECURITY-INTERFACE-ACCESS), the ATA Security Unlock command can also be used to authenticate as Master or User for the User Data Read / Write service.

For the DEK Key Input (Inject) service, the Card Owner authentication is provided through a Challenge-Response APDU sequence using an RSA key pair and a CM generated random value. The public key, "RSAVerify" is provided by the host to the CM during module setup. See section 2.4 for limitations.

Per the Security Rules of this Security Policy, to switch operator roles, the host application must clear a previous authentication using the Warm Reset APDU command. This command should be addressed to the applicable dCard. For services with indirect access control (authentication with a separate enable / unlock service) the host may choose to disable/lock services for access control.

3.2.4 Authentication Mechanism, Data and Strength

Operator authentication with PINs is implemented in the CM by hashing the host supplied value and comparing to the stored hash of the assigned PIN. The PINs have a retry attribute that controls the number of unsuccessful attempts before the authentication is blocked. The various PINs have maximum lengths of 16 to 32 bytes. Per the policy security rules, the minimum PIN length is 4 bytes (32 bits) 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. The PIN blocking feature limits the number of random attempts to 5 (it "unblocks" with module reset) and the minimum time for a module reset is 4 seconds (15/min). Thus the probability of multiple random attempts to succeed is $(5*15)/2^{32}$. which is less than the FIPS requirement of 1/100,000.

3.2.5 Personalizing Authentication Data

The initial value for some operator PINs is a manufactured value (mSID). This is a device-unique, 25-byte, public value. The value is printed on the drive label (identified as SID). The security rules (section 7) for the CM require that the PIN values must be "personalized" to private values using the "Set PIN" service. In some cases the factory-installed data is an unknown random value that must be changed with the Set PIN service to enable the operator.

4 Access Control Policy

4.1 Services

The following table represents the FIPS 140-2 services in terms of the Approved Security Functions and operator access control. Note the following:

- Personalization of PINs and keys as required by the Security Rules and described in the I&A Policy section are not described here.
- Underlying security functions used by higher level algorithms are not represented (e.g. hashing as part of asymmetric key)
- See the technical specification references for the command/response input and output details.
- Unauthenticated services (e.g. Show Status, Reset, Device Identification) 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.
- ** Some services are disabled in Manufacturing; see section 2.4 for details.

Table 1 - FIPS 140 Services

Service Name	Description	Operator Access Control	Security Function	Command(s) / dCard dev file
Set PIN	Change operator authentication data.	All Note: Any Master can set the PIN for any Master or User. Secure Erase Master PIN is set with any Master	Hashing, Symmetric Key	Change PIN APDU
Unblock PIN	Reset password attempt counter.	All Note: Any Master can Unblock the PIN for any Master, User or Secure Erase Master. Drive Owner PIN can only be unblocked with POR.	None	POR, Unblock PIN APDU
Enable / Disable FW Download	Enable / Disable FW Download Service	Drive Owner	None	Update Binary Device File APDU on Admin: /dev/EF-DOWNLOAD-MICROCODE bit 0
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.	None (* FW Download enabled)	Asymmetric Key	ATA DOWNLOAD MICROCODE

Table 1 - FIPS 140 Services				
Service Name	Description	Operator Access Control	Security Function	Command(s) / dCard dev file
Lock / Unlock User Data	Enable / Disable User Data Read / Write service. Note: POR or COMRESET (SSP disabled) disables (locks) the User Data service.	Any Master or Any User	Symmetric Key (to unwrap DEK)	ATA SECURITY UNLOCK Update Binary Device File APDU on FDE: /dev/EF-USER-LOCK, (or /dev/EF-LBA-REMAPPING-BYPASS)
User Data Read / Write	Encryption / decryption of user data.	None (* User Data Unlocked)	Symmetric Key	ATA Read / Write Commands
Cryptographic Erase	Erase user data by cryptographic means: changing the encryption key. Note: Some PINs are reset to default values. See Secure Initialization. Note: The use of Secure Erase Master may be an unauthenticated key zeroization operation. See section 2.6.	Any Master, Secure Erase Master	RNG, Symmetric Key	Update Binary Device File APDU on FDE: /dev/EF-SECURE-ERASE, /dev/EF-SECURE-ERASE-WITH-SECURE-ERASE-PIN
Generate Symmetric Key **	Generate, store and return (encrypted) a private key value.	Depends on ACL for specified key	RNG, Symmetric Key	Get Challenge + Generate Symmetric Key APDU
Device Identification **	CM cryptographically identifies to host using encryption of random challenge with specified key.	Depends on ACL for specified key	Symmetric Key, Asymmetric Key	Internal Authenticate APDU
Show Status	Reports if Security System is operational. Operational != 0x0020	None	None	Read Record (6) APDU on Admin dCard file EF-CARD-STATUS (bytes 2-3)
DEK Key Inject **	Key Management: Electronic input of (encrypted) data encryption key to CM. Note: PINs are reset and must be reinitialized.	Master/User or Drive Owner + Card Owner (with RSAVerify credential)	Symmetric Key	Update Binary Device File APDU on FDE: /dev/EF-ENCRYPTION-KEY
Reset Module	Runs POSTs and zeroizes keys & CSPs RAM storage.	None	None	Power cycle (POR)

Table 1 - FIPS 140 Services				
Service Name	Description	Operator Access Control	Security Function	Command(s) / dCard dev file
Disable Services	Disables ATA Security Unlock or DriveTrust APDUs and ATA Security Unlock until Reset	None Master or User	None	ATA SECURITY FREEZE LOCK, Update Binary Device File APDU on FDE: /dev/EF-FREEZE-LOCK
Perform Security Operation	General purpose cryptographic services. Note: Excluded by policy. See Section 7.2. RSA Sig gen is non-compliant.	Varies depending on key references.	Hashing, Symmetric Key, Asymetric Key	Perform Security Operation APDU

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.
- 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.
- Read access of private values are internal only to the CM.
- There is no security-relevant audit feature.
- ** Some Keys and CSPs cannot be used or changed in the field because the authentication data to control them is discarded during manufacturing.
- The Access column indicates R=Read, W=Write, X=Execute, Z=Zeroize.

Table 2 - Key Management

Name	dCard	Description	Type (Pub / Priv, key / CSP (e.g. PIN)), size	Operator Role	Services Used In	Access (R,W,X, Z)	Lifecycle				
							Initial Value or Initialization Method	Storage	Storage Form (Plaintext / Encrypted / Logically Protected)	Entry / Output	Zeroization
mSID (EF-MFG-SID)	Admin	Drive-unique default value for secure initialization	Public, PIN, 25 bytes	Master, Secure Erase Master	Cryptographic Erase	R	Random value created at Mfg	Media (System Area)	Plaintext	Entry: None Output: none	None, Public Value
SID (Secure ID), aka Drive Owner	Admin	Auth. Data	Private, PIN, 25 chars	Drive Owner	Set PIN	W	Electronic Input at Module Setup	Media (System Area)	SHA Digest	Entry: Electronic Input from Host Output: none	Cryptographic Erase
				Master / User	Cryptographic Erase	Z					
				FDE dCard Owner	DEK Key Inject **	Z					

Table 2 - Key Management											
Name	**dCard**	**Description**	**Type (Pub / Priv, key / CSP (e.g. PIN)), size**	**Operator Role**	**Services Used In**	**Access (R,W,X, Z)**	**Lifecycle**				
							Initial Value or Initialization Method	**Storage**	**Storage Form (Plaintext / Encrypted / Logically Protected)**	**Entry / Output**	**Zeroization**
FDE dCard Owner Password	FDE	Auth. Data	Private, PIN, 16 bytes	FDE dCard Owner	Set PIN **	W	Mfg, Random, unknown	Media (System Area)	SHA Digest	Entry: Electronic Input from Host Output: none	Electronic Input from Host
Secure Erase Master PIN	FDE	Auth. Data	Public/Private, PIN, 25 bytes	Master, FDE dCard Owner	Set PIN	W	Mfg, mSID	Media (System Area)	SHA Digest	Entry: Electronic Input from Host Output: none	Cryptographic Erase
Master0-3 Passwords	FDE	Auth. Data	Private, PIN, 32 bytes	Any Master	Set PIN	W	Electronic Input at Module Setup	Media (System Area)	SHA Digest	Entry: Electronic Input from Host Output: none	Cryptographic Erase
				Any Master	Cryptographic Erase	Z					
				FDE dCard Owner	DEK Key Inject **	Z					
User0-3 Passwords	FDE	Auth. Data	Private, PIN, 32 bytes	Any Master, User	Set PIN	W	Electronic Input at Module Setup	Media (System Area)	SHA Digest	Entry: Electronic Input from Host Output: none	Cryptographic Erase
				Any Master	Cryptographic Erase	Z					
				FDE dCard Owner	DEK Key Inject **	Z					

Table 2 - Key Management											
Name	**dCard**	**Description**	**Type (Pub / Priv, key / CSP (e.g. PIN)), size**	**Operator Role**	**Services Used In**	**Access (R,W,X, Z)**	**Lifecycle**				
							Initial Value or Initialization Method	**Storage**	**Storage Form (Plaintext / Encrypted / Logically Protected)**	**Entry / Output**	**Zeroization**
Master0-3, User0-3 DEKs	FDE	DEK mixed with PINs	Private, AES Key, 128 bits	Master/User or Drive Owner + FDE dCard Owner	DEK Key Inject **	W	Mfg, Random, Unknown	Media (System Area)	Plaintext	Electronic Encrypted Key Input through Write Binary of EF-ENCRYPTION-KEY device file	Cryptographic Erase
				Any Master	Cryptographic Erase	Z					
				Any Master or User	Security Unlock	R					
Seed Key (XKEY)	None	RNG Key	Private, Hash Key, 64 bytes	None	Services which use the RNG (e.g. cryptographic erase, operator authentication)	X, W	Mfg	RAM	None	None	Reset

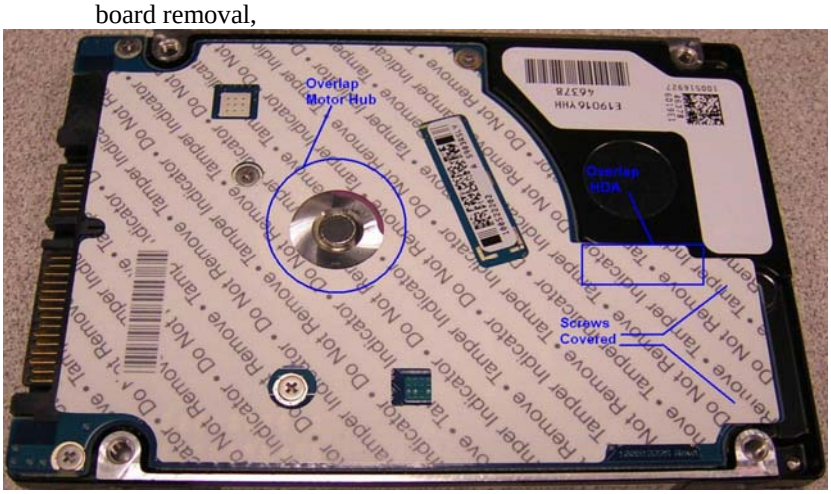
Table 2 - Key Management											
Name	**dCard**	**Description**	**Type (Pub / Priv, key / CSP (e.g. PIN)), size**	**Operator Role**	**Services Used In**	**Access (R,W,X, Z)**	**Lifecycle**				
							Initial Value or Initialization Method	**Storage**	**Storage Form (Plaintext / Encrypted / Logically Protected)**	**Entry / Output**	**Zeroization**
Seed	None	RNG seed (entropy)	Private, Hash seed, 536 bytes	None	1st RNG use after POST	X	Entropy collected at power up	RAM	None	None	Reset
ORG0-0 - ORG0-3	None	Firmware Load Test Signature Verify Key	Public, RSA Key, 1024 bits	None subject to FW download enabled (Drive Owner)	FW Download	X	Mfg	Media (System Area)	Plaintext	None	None (Public)
EF-RSA-VERIFY **	FDE	Auth. Data, Encryption Key	Public, RSA Key, 1024 bits	FDE dCard Owner	DEK Key Inject ** (Card Owner Authentication)	X	Electronic Input at Module Setup	Media (System Area)	Plaintext	Read / Update Binary BER TLV **	None (Public)
EF-3DES-EXCHANGE **	FDE	Key Encryption Key	Private, 3DES Key, 16 bytes	FDE dCard Owner	DEK Key Inject **	X	RNG Generated at Module Setup	Media (System Area)	Plaintext	Read / Update Binary BER TLV **	Update Binary BER TLV **
EF-3DES-DRIVE-TO-HOST, EF-3DES-HOST-TO-DRIVE **	FDE	Encryption Keys for protecting message payloads between host and drive	Private, 3DES Key, 16 bytes	FDE dCard Owner	Secure messaging **	X	RNG Generated at Module Setup	Media (System Area)	Plaintext	Read / Update Binary BER TLV **	Update Binary BER TLV **
EF-3DES-DL-HASH **	FDE	Key for generating HMAC of message payload.	Private, Hash Key, 16 bytes	FDE dCard Owner	Secure messaging **	X	RNG Generated at Module Setup	Media (System Area)	Plaintext	Read / Update Binary BER TLV **	Update Binary BER TLV **

5 Physical Security

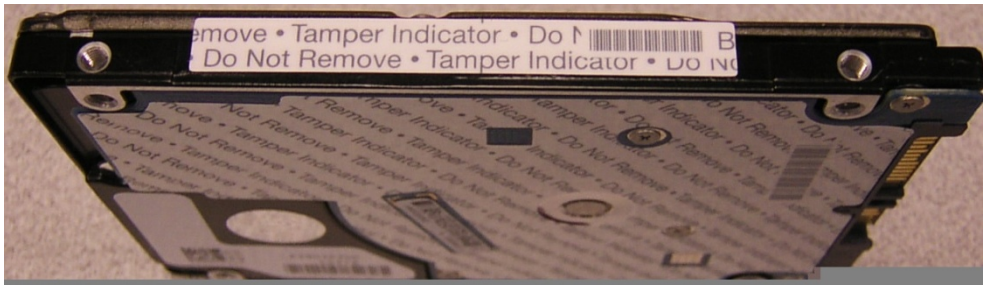
5.1 Mechanisms

The CM has the following physical security:

- Production-grade components with standard passivation,
- Exterior of the drive is opaque,
- Opaque, tamper-evident security labels which cannot be penetrated or removed and reapplied without tamper-evidence.
- Security labels cannot be easily replicated with a low attack time.
- Security label on the exposed (back) side of the PCBA protects physical access to the electronics by board removal,



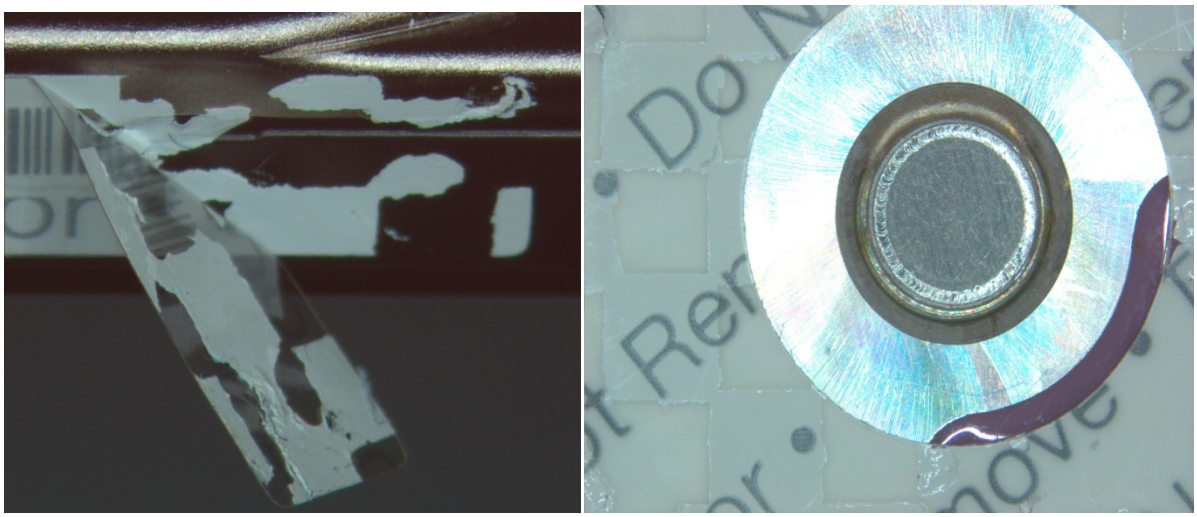
- Security labels on side of drive to provide tamper-evidence of HDA cover removal,



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 reset and operate with the new code image.

7 Security Rules

7.1 Secure Initialization

The CM remains in FIPS mode across module resets and all services. 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. 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. At installation and periodically examine the physical security mechanisms for tamper evidence.
3. At installation, set all operator PINs to private values of at least 4 bytes length (CHANGE PIN APDU)
4. COs: Ensure EF-LBA-REMAPPING is enabled as this will provide access control after a module reset, to the User Data Read / Write service. The access control to this setting is any Master. The command to set this value is the UPDATE BINARY DEVICE FILE APDU applied to the specified device file on the FDE dCARD.
5. COs: Ensure EF-DOWNLOAD-MICROCODE bits 0 and 1 are set to 0 to enable access control for the Download Microcode service. The access control to this setting is Drive Owner. The command to set this value is the UPDATE BINARY DEVICE FILE APDU applied to the Admin dCARD /dev/EF-DOWNLOAD-MICROCODE file.
6. COs: If it is desirable to only provide Cryptographic Erase as an authenticated service then set the Secure Erase Master PIN to a private value(CHANGE PIN APDU). The access control to this setting is any Master.
7. After all the above settings have been made then perform a power-on reset.

7.2 Ongoing Policy Restrictions

1. Operators must clear authentication prior to assuming a new role. This is accomplished via power-on reset or the Warm Reset APDU.
2. COs must not modify EF-LBA-REMAPPING and EF-DOWNLOAD-MICROCODE (bit 1) after the Secure Initialization process.
3. After use of the Cryptographic Erase service all operator PINs must be set to private values as described in Secure Initialization.
4. DES is a non-Approved algorithm and shall not be used for encryption/decryption.
5. Do not use the Perform Security Operation APDU as this is unauthenticated (except through access control to the referenced key).

8 Mitigation of Other Attacks Policy

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