Momentus® FDE Drives

FIPS 140 Module Security Policy

Rev. 2.1 – July 6, 2010

Seagate Technology, LLC

Seagate
Momentus 7200 FDE.2
320 GB
DO NOT COVER BREATHER HOLE
SID: VCMTY 0C7A5 28M61 WAGXY EQXS9
Canada Class B digital apparatus ICES – 003/
Classe B appareil numérique NMB – 003.
Made in CN
DP/N XXXXXX
SATA
Capacity: 320 GB
7200 RPM
Firmware: DED0
CN – XXXXXX – 21232 – 98A – 001Y – X00
WWN: 5000C50018FCA63C
CAUTION: Avoid excessive shock; do not push on top cover or remove any seal or label.
+5V 0.451 A
Date: 10064
Site: WU
E190397
STX – 72004 (B)
N176
SN: 5VH07B0L
ST9320427ASG
PN: 9UVG4E – 030
FW: DED0
中国产品
Product of China

Table of Contents

1 Introduction

1.1 Scope

This security policy applies to the FIPS 140-2 Cryptographic Module (CM), Seagate® Momentus® FDE 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 SeaCOS Commands Reference Manual
7. DriveTrust Technology Life Cycle Manual
8. DriveTrust FDE Card Life Cycle Manual
9. Momentus FDE Product Manual
10. 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
HMAC	Hashed Message Authentication Code
KAT	Known Answer Test
mSID	Manufactured SID, public drive-unique PIN
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)

2 Cryptographic Module Description

2.1 Overview

The Momentus® FDE Drives, FIPS 140 Modules are FIPS 140-2 Level 2 modules which provide full disk encryption with user authentication. These products are 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 two FIPS-Approved modes: ATA Enhanced Security Mode and DriveTrust Security 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 drive is a multiple-chip embedded physical embodiment, and the physical boundary of the CM is the entire drive. The certified drive models are nearly identical, but have some minor security-relevant differences (as described in section 2.2); they primarily differ in terms of storage capacity (#disks). 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). 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. 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 two FIPS modes in this certification are supported by 2 Seagate provided dCards: Admin and FDE. The Admin dCard provides storage for keys, CSPs and non-critical security parameters of the CM and operates ATA Enhanced Security Mode. The FDE dCard, when operationally active, allows the operator to use the CM in DriveTrust Security Mode rather than ATA Enhanced Security Mode. Each of the 2 FIPS-Approved Mode provides unique roles and services, which are covered in Sections 2, 3, and 5 of this document.

2.2 Hardware and Firmware Versions

The Momentus® FDE Drives, FIPS 140 Module is offered in six configurations:

1) HW ver #ST9500422AS, FW ver #500: 500GB capacity, OEM non-customer unique FW.
2) HW ver #ST9250412AS, FW ver #070: 250GB capacity, Customer unique FW 1 This FW does not support FW loading, aka EF-DOWNLOAD-MICROCODE service.
3) HW ver #ST9250412AS, FW ver #500: 250 GB capacity, OEM non-customer unique FW.
4) HW ver #ST9320427ASG, FW ver #030: 320GB capacity, Customer unique FW 2.
5) HW ver #ST9250414ASG, FW ver #030: 250GB capacity, Customer unique FW 2.
6) HW ver #ST9160419ASG, FW ver #030: 160GB capacity, Customer unique FW 2.

All of the configurations are externally identical. The cover of this document shows configuration #4 above.

2.3 FIPS 140 Approved Modes 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). After setting up (configuring) the module per the Security Rules of this policy, an operator can communicate with the drive in either ATA Enhanced Security Mode or DriveTrust Mode.

Both of the module’s FIPS modes of operation are enforced both through configuration and through policy. Violating these ongoing policy restrictions (detailed in Section 8, Ongoing Policy restrictions) would mean that one is no longer using the drive in a FIPS compliant mode of operation.

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.

2.3.1 ATA Enhanced Security Mode

This mode provides services through industry-standard ATA commands, and SeaCOS APDUs addressed to the Admin dCard, resident on the drive. Some of the services are based on the ATA Security Feature set, with vendor-unique extensions (e.g. encryption of user data on media). Other services are based on the Seagate proprietary security commands (SeaCOS).

This 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 128-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 (not available in FW #070). Additionally, a cryptographic erase service is provided to the Master and User roles through the ATA security erase unit commands. When executed, the cryptographic erase service changes the AES-128 bit DEK resulting in incorrect decryption of the original plaintext data). The FW download service (ATA Download Microcode command) provides a FIPS-compliant FW load test by verifying the image’s embedded 1024-bit RSA signature (again, this service is not available in FW #070).

2.3.2 DriveTrust Security Mode

This mode provides services 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). It provides all of the services of the ATA Enhanced Security Mode and additional features through Seagate proprietary security commands (SeaCOS). Some ATA Security commands are disabled in this mode and their functionality is provided through the APDUs.

In addition to the Drive Owner, Master and User roles, this mode implements a CO role to administer the additional features, FDE dCard owner. The additional features of this mode include:

- Master role has the following CO capabilities: administration of User role and authority for Cryptographic Erase
- Four Master and four User IDs
- Perform Security Operation (e.g. encryption, decryption, signature, hashing)
- Device Identification
- Key inject
- Secure messaging with message encryption and authenticity

The Perform Security Operation and Device Identification services produce cryptograms from a random value generated by the CM using the requested algorithm and a shared secret encryption key. The Key Inject service provides key input of the data encryption key. Secure messaging can be applied to all APDUs to provide encrypted and authenticated messages. These features utilize the Generate Symmetric Key service to create the shared secret keys. The CM generates the key and returns it to the host in encrypted form.

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 services performed by each role in each FIPS mode, as well as services which do not require an operator role, see section 5.1

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 (not available in FW #070).

3.1.1.2 FDE dCard Owner

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).

3.1.1.3 Master(s)

This role is used to enable/disable Master and User 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. In DriveTrust Security Mode there are up to 4 Master IDs. Note that in ATA Enhanced Security mode there is a single Master ID and it only provides a backup authentication to the User ID; it does not have access to administration services beyond those of the User role.

3.1.2 User Roles

3.1.2.1 User(s)

This role can unlock (and also lock) the drive so that an operator can read and write data to the drive. When operating in the ATA Enhanced Security mode, this role can also call the Cryptographic Erase service. When operating in DriveTrust Security Mode, one can configure up to four separate users (User IDs).

3.1.3 Unauthenticated Role

This role can perform Show Status services, Perform Security Operation, 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

Some operator roles are role-based and others are identity-based. For example, the Drive Owner role uses role-based authentication as there is only one ID and one PIN. In DriveTrust Security Mode, the CM has up to 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.

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

3.2.2 Authentication in ATA Enhanced Security Mode

In ATA Enhanced Security Mode, Master and User operator authentication is provided through a PIN provided in the ATA Security command, 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).

Depending on a parameter of the Set PIN service for the User password, the Security Unlock service is extended to the Master role. If the Master Password Capability is set to High then either role can access that service, otherwise only the User role has access to those services.

Drive Owner authentication for the Enable/Disable FW Download service, is provided through the SeaCOS Verify PIN APDU.

3.2.3 Authentication in DriveTrust Security Mode

In DriveTrust Security Mode, Drive Owner, FDE dCard Owner, Master, and User operator authentication 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.

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.

3.2.4 Authentication Mechanism, Data and Strength

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 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 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 8) 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.

For DriveTrust Security Mode, if the host intends to use the DEK Key Inject service then the module must also be configured with the public key (RSAVerify) that will be used for FDE dCard Card Owner authentication. The access control for setting this value is the FDE dCard Owner PIN.

3.3 Setup of Keys (DT mode)

For DriveTrust Security Mode, CM setup includes generating encryption keys for various services (DEK Key Inject and Secure Messaging). These keys will be shared secrets between the host and the CM, which are used to encrypt/decrypt data in the message payloads. The Generate Symmetric Key service is used to create the values in the CM. The access control for this service is dependent on the key being generated. They key values are returned to the host in encrypted form, using the previous key value. See Doc. Ref. 6 for details. For Secure Messaging a message authentication code is generated and attached to the messages. This HMAC is generated using a hash key which is similarly generated by the CM, using the Generate Symmetric Key service, at module setup.

3.4 Effects of SATA COMRESET and ATA SSP

In compliance with the SATA standard, the CM supports a communications reset from the host application, COMRESET. This signal over the SATA interface *does not* trigger the Reset Module service or clear a FIPS self-test error state. The drives also support the related ATA Software Settings Preservation (SSP) feature set, though this feature can be disabled by the host application. If SSP is *disabled*, then a COMRESET will clear authentication of the User Data Read / Write service (i.e. the service / data will be locked), and if Services were disabled (Disable Services) then they will be enabled.

4 Secure Messaging

In DriveTrust Security mode, services can be provided with a FIPS-compliant Message Authentication (HMAC) to establish message integrity. In addition to the HMAC in the message, the message payload is encrypted using shared secret keys. The CM implements this feature in adherence to the SmartCard Messaging Protocol described in Doc. Ref. 10. This capability is available for APDUs (not ATA commands). This capability is requested by the host via a field (CLA) in the command APDU header. The hash algorithm type (e.g. HMAC) and reference to the hash key used to generate the MAC are also indicated by fields in the command APDU.

5 Access Control Policy

5.1 Services

The following tables represent the FIPS 140 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. 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)
- See the technical specification references for the low-level 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.
- If the Operator value contains "opt" then the access is dependent on the module setup (see 3.2.2).

Table 1 - FIPS 140 Services – ATA Enhanced Security Mode

Service Name	Description	Operator Access Control	Security Function	ATA Command(s), other events
Set PIN	Change operator authentication data.	All (* Security Unlocked for Master/User)	Hashing, Symmetric Key	SECURITY SET PASSWORD, Change PIN APDU on AdmindCard (for Drive Owner PIN)
Unblock PIN	Reset password attempt counter.	None	None	POR
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. Note: Service not available on some FW versions.	None (* FW Download enabled)	Asymmetric Key	DOWNLOAD MICROCODE
Unlock User Data	Enable User Data Read / Write and Set PIN services. Note: POR or COMRESET (SSP disabled) disables (locks) the User Data service.	User (opt. Master)	Symmetric Key (to unwrap DEK)	SECURITY UNLOCK,

Table 1 - FIPS 140 Services – ATA Enhanced Security Mode

Service Name	Description	Operator Access Control	Security Function	ATA Command(s), other events
User Data Read / Write	Encryption / decryption of user data.	None (* Security Unlocked)	Symmetric Key	ATA Read / Write Commands
Cryptographic Erase	Erase user data through cryptographic means: by zeroizing the encryption key and the User PIN. Note: FIPS mode is exited.	Master, User	RNG	SECURITY ERASE PREPARE + SECURITY ERASE UNIT
Show Status	Reports if ATA Enhanced Security mode is operational. Operational: ID word/bit 85 = 1 and dCard Status = 0x0020.	None	None	IDENTIFY DEVICE word / bits 85/1 + Read Record (6) APDU on Admin dCard file EF-CARD-STATUS bytes 2-3
Reset Module	Runs POSTs and zeroizes key & CSP RAM storage.	None	None	Power cycle
Disable Services	Disables ATA Security commands until Reset	None	None	SECURITY FREEZE LOCK
Exit ATA Enhanced Security Mode	Exit FIPS Mode and zeroize User PIN.	User (opt. Master) (* Security Unlocked)	RNG, Hashing, Symmetric Key	SECURITY DISABLE PASSWORD, SECURITY ERASE PREPARE + SECURITY ERASE UNIT

Table 2 - FIPS 140 Services – DriveTrust Security Mode

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.	Hashing, Symmetric Key	Change PIN APDU to appropriate dCard
Unblock PIN	Reset password attempt counter.	All Note: Any Master can Unblock the PIN for any Master or User.	None	POR, Unblock PIN APDU on associated dCard
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. Note: Service not available on some FW versions.	None (* FW Download enabled)	Asymmetric Key	ATA DOWNLOAD MICROCODE
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
User Data Read / Write	Encryption / decryption of user data.	None (* Security Unlocked)	Symmetric Key	ATA Read / Write Commands
Cryptographic Erase	Erase user data by cryptographic means: changing the encryption key and PINs. Note: FIPS mode is exited.	Master	RNG, Symmetric Key	Update Binary Device File APDU on FDE: /dev/EF-SECURE-ERASE

Table 2 - FIPS 140 Services – DriveTrust Security Mode

Service Name	Description	Operator Access Control	Security Function	Command(s) / dCard dev file
Generate Symmetric Key	Generates, stores and returns a (3DES encrypted) key e.g., to personalize exchange key (3DES-EXCHANGE).	Depends on ACL for specified key	RNG, Symmetric Key	Get Challenge + Generate Symmetric Key APDU
Perform Security Operation	Performs selected cryptographic function (DES, TDES, RSA SHA-1, RSA) on provided data.	Depends on ACL for specified key	Symmetric Key, Asymmetric Key, Hashing,	Perform Security Operation 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 DriveTrust mode is operational (i.e. FDE dCard exists). 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 DriveTrust mode is exited.	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
Disable Services	Disables ATA Security commands and DriveTrust APDUs until Reset	Master or User	None	ATA SECURITY FREEZE LOCK, Update Binary Device File APDU on FDE: /dev/EF-FREEZE-LOCK
Secure Messaging	Message Authentication and Encryption for APDUs	Depends on ACL for specified key.	HMAC, Symmetric Key	Any APDU

5.2 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:

- Lifecycle – Initial Value represents the value after the required Security Rules for module setup have been completed.
- 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.
- 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 3 - Key Management

Name	Mode (ATA / DT / Both)	dCard	Description	Type (Pub / Priv, key / CSP (e.g. PIN)), size	Operator Role	Services Used In	Access (R,W,X, Z)	Lifecycle (starting after Module Setup)				
								Initial Value / Method (after Setup)	Storage	Storage Form (Plaintext / Encrypted / Logically Protected)	Entry / Output	Zeroization
SID (Secure ID), aka Drive Owner	Both	Admin	Auth. data	Private, PIN, 25 chars	Drive Owner	Set PIN	W	Default value / 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 (DT only)	Z					

Table 3 - Key Management

Name	Mode (ATA / DT / Both)	dCard	Description	Type (Pub / Priv, key / CSP (e.g. PIN)), size	Operator Role	Services Used In	Access (R,W,X, Z)	Lifecycle (starting after Module Setup)				
								Initial Value / Method (after Setup)	Storage	Storage Form (Plaintext / Encrypted / Logically Protected)	Entry / Output	Zeroization
Master, User Passwords	ATA	None	Auth. Data	Private, PIN, 32 bytes	None subject to unlocked	Set PIN	W	Default value / Electronic Input at Module Setup	Media (System Area)	SHA Digest	Entry: Electronic Input from Host Output: none	Cryptographic Erase
					Master, User	Cryptographic Erase	Z					
Master, User DEKs	ATA	None	DEK mixed with PINs	Private, AES Key, 128 bits	Master, User	Cryptographic Erase	Z	Set during manufacturing, RNG generated upon Cryptographic Erase	Media (System Area)	Plaintext	None	Cryptographic Erase
					User / Master	Security Unlock	X					
FDE dCard Owner Password	DT	FDE	Auth. Data	Private, PIN, 16 bytes	FDE dCard Owner	Set PIN	W	Electronic Input at Module Setup	Media (System Area)	SHA Digest	Entry: Electronic Input from Host Output: none	Cryptographic Erase

Table 3 - Key Management

Name	Mode (ATA / DT / Both)	dCard	Description	Type (Pub / Priv, key / CSP (e.g. PIN)), size	Operator Role	Services Used In	Access (R,W,X, Z)	Lifecycle (starting after Module Setup)				
								Initial Value / Method (after Setup)	Storage	Storage Form (Plaintext / Encrypted / Logically Protected)	Entry / Output	Zeroization
Master0-3 Passwords	DT	FDE	Auth. Data	Private, PIN, 32 bytes	Master	Set PIN	W	Default value / Electronic Input at Module Setup	Media (System Area)	SHA Digest	Entry: Electronic Input from Host Output: none	Cryptographic Erase
					Master	Cryptographic Erase	Z					
					FDE dCard Owner	DEK Key Inject	Z					
User0-3 Passwords	DT	FDE	Auth. Data	Private, PIN, 32 bytes	Master, User	Set PIN	W	Default value / Electronic Input at Module Setup	Media (System Area)	SHA Digest	Entry: Electronic Input from Host Output: none	Cryptographic Erase
					Master	Cryptographic Erase	Z					
					FDE dCard Owner	DEK Key Inject	Z					
Master0-3, User0-3 DEKs	DT	FDE	DEK mixed with PINs	Private, AES Key, 128 bits	Master/User or Drive Onwer + FDE dCard Owner	DEK Key Inject	W	Set during manufacturing, RNG generated upon Cryptographic Erase	Media (System Area)	Plaintext	Electronic Encrypted Key Input through Write Binary of EF-ENCRYPTION-KEY device file	Cryptographic Erase
					Master	Cryptographic Erase	Z					
					Master, User	Security Unlock	R					

Table 3 - Key Management

Name	Mode (ATA / DT / Both)	dCard	Description	Type (Pub / Priv, key / CSP (e.g. PIN)), size	Operator Role	Services Used In	Access (R,W,X, Z)	Lifecycle (starting after Module Setup)				
								Initial Value / Method (after Setup)	Storage	Storage Form (Plaintext / Encrypted / Logically Protected)	Entry / Output	Zeroization
Seed Key (XKEY)	Both	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
Seed	Both	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	Both	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	DT	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	Yes, Read / Update Binary BER TLV	None (Public)

Table 3 - Key Management

Name	Mode (ATA / DT / Both)	dCard	Description	Type (Pub / Priv, key / CSP (e.g. PIN)), size	Operator Role	Services Used In	Access (R,W,X, Z)	Lifecycle (starting after Module Setup)				
								Initial Value / Method (after Setup)	Storage	Storage Form (Plaintext / Encrypted / Logically Protected)	Entry / Output	Zeroization
EF-3DES-EXCHANGE	DT	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	No (by policy)	Cryptographic Erase
EF-3DES-DRIVE-TO-HOST, EF-3DES-HOST-TO-DRIVE	DT	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	No (by policy)	Cryptographic Erase
EF-3DES-DL-HASH	DT	FDE	Key for generating HMAC of message payload.	Private, Hash Key, 16 bytes	FDE dCard Owner	Secure messaging	X	Electronic Input at Module Setup	Media (System Area)	Plaintext	No (by policy)	Cryptographic Erase

5.3 Non-Critical Security Parameters

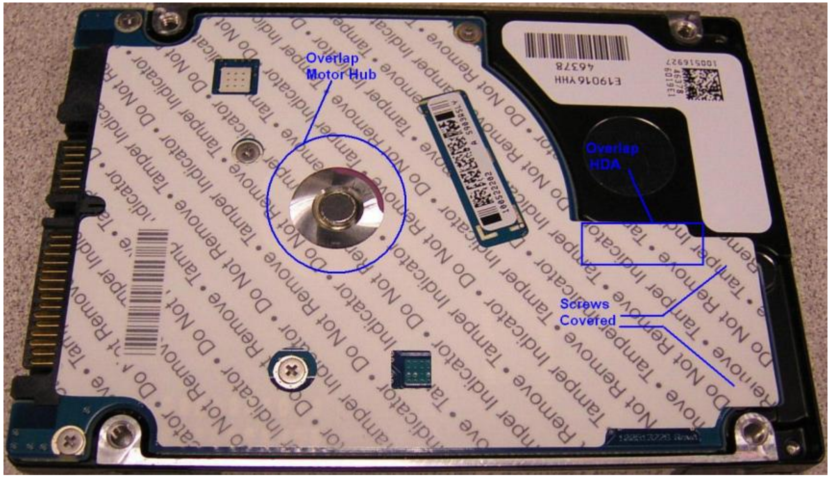
See the appropriate DriveTrust Life Cycle Manual (7, 8) for the complete filesystems of the Admin and FDE dCards.

6 Physical Security

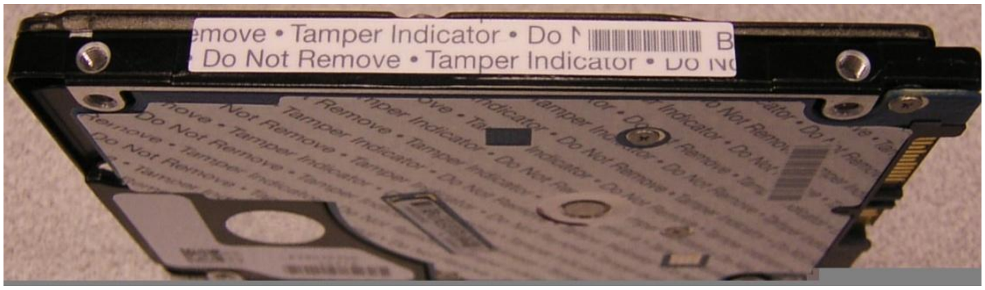
6.1 Mechanisms

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,



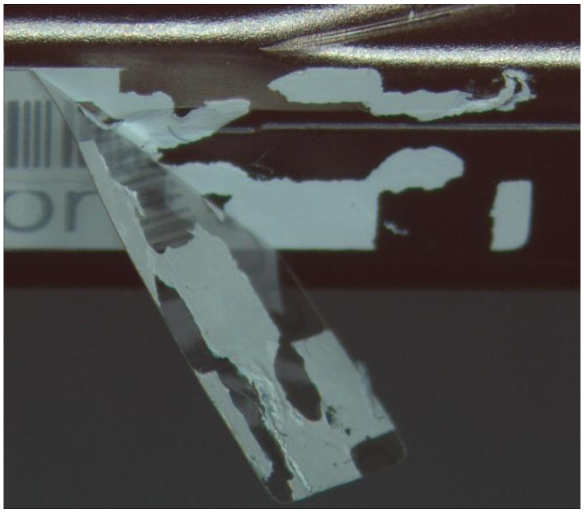
- Security labels on side of drive to provide tamper-evidence of HDA cover removal,

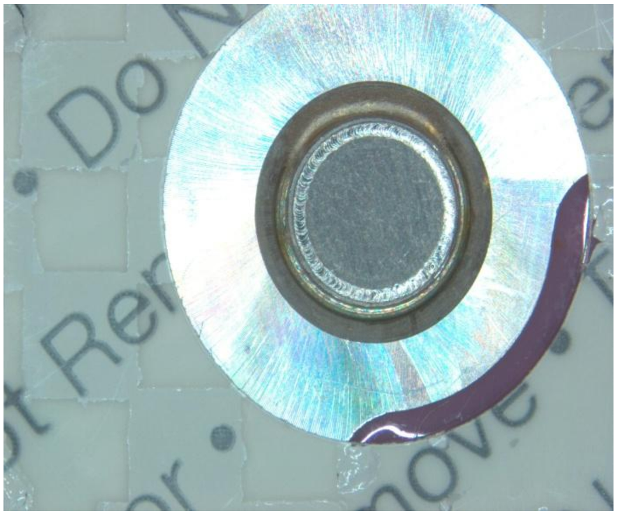


6.2 Operator Requirements

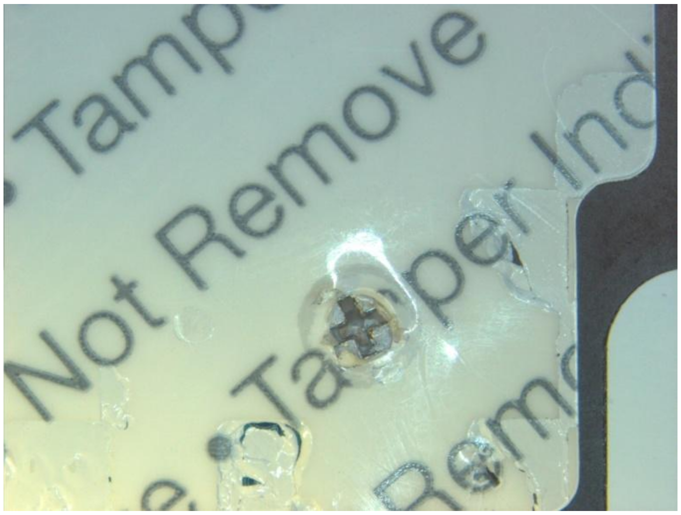
The operator is required to inspect the CM periodically for one or more of the following tamper evidence:

- 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.

7 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.

8 Security Rules

The following are the security rules for initialization and operation of the CM in a FIPS 140 compliant manner. For specific command details see the appropriate technical spec:

- ATA Commands - Doc. Ref.4,
- SeaCOS Commands: Doc. Ref. 6,
- Admin dCard: Doc. Ref. 7, and
- FDE dCard: Doc. Ref. 8.

8.1 Secure Initialization

The CM remains in FIPS mode across module resets. However, certain operations can result in exiting the FIPS Approved mode. In some of the exit scenarios (e.g. returning the drive to the manufacturer for failure analysis), the drive cannot be restored to FIPS mode and does not provide any FIPS services. For example, if the drive is returned to the manufacturer, the remanufacturing process will result in the module exiting the FIPS mode if the drive is to be returned to the customer

If the module does not have an FDE dCard present and the operator wishes to use the CM in DriveTrust Mode, the operator must first configure the drive via a configuration utility.

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. COs and Users: At installation, set all operator PINs applicable for the FIPS mode to private values of at least 4 bytes length:
    - ATA Mode: Drive Owner, Master, and User. For the Master, set the “Master Password Capability” to “High” (CHANGE PIN APDU, ATA SECURITY SET PASSWORD).
    - DriveTrust: Drive Owner, FDE dCard Owner, Masters, Users (CHANGE PIN APDU)
4. COs (DriveTrust): If DEK Key Inject service will be used, then activate and personalize EF-RSA-VERIFY (RSA public key) and EF-3DES-EXCHANGE (3DES key used for encryption of DEK). The GENERATE SYMMETRIC KEY APDU command is used. See sections 3.2.5 and 3.3 for details.
5. COs (DriveTrust): If Secure Messaging will be used, then personalize EF-HOST-TO-DRIVE, EF-DRIVE-TO-HOST, and EF-3DES-DL-HASH keys using the Generate Symmetric Key service (with the same named APDUs addressed to the specified device files on the FDE dCard). The access control for these values is FDE dCard Owner. Note that these values must not be changed via Update APDUs.
6. COs (DriveTrust): Set EF-LOCK-ON-STARTUP to enabled (0x01) to prevent unauthenticated access after a module reset, to the User Data Read / Write service. The access control for this setting is any Master. The command to set this value is the UPDATE BINARY DEVICE FILE APDU applied to the FDE dCARD /dev/EF-LOCK-ONSTARTUP file.
7. COs (either mode): Set EF-DOWNLOAD-MICROCODE bits 0 and 1 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.
8. After all the above settings have been made then perform a power-on reset.

8.2 Ongoing Policy Restrictions

1. Operators must log off prior to assuming a new role via power-on reset or warm reset to clear the previous authentication.

2. The Master must not modify the EF-LOCK-ON-STARTUP setting after it has been enabled (0x01) during the Secure Initialization process.

3. DES is a non-Approved algorithm and shall not be used for encryption/decryption.

9 Mitigation of Other Attacks Policy

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