Seagate Secure™

Self-Encrypting Drive
Non-Proprietary FIPS 140-3 Module Security Policy

Security Level 2
Revision 0.8

Contents

1 Introduction

1.1 Scope

This security policy applies to the FIPS 140-3 Cryptographic Module (CM) embedded in Seagate Secure® Self-Encrypting Drive products.

This document meets the requirements of the FIPS 140-3 standard. 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 Overview

The Seagate Secure® Self-Encrypting Drive FIPS 140-3 Module is embodied in Seagate Exos™ Enterprise SED model devices. These products meet the performance requirements of the most demanding Enterprise applications. The Cryptographic Module (CM) provides a wide range of cryptographic services including:

- Hardware based data encryption (AES-XTS)
- Instantaneous user data disposal with cryptographic erase
- Independently controlled and protected user data LBA bands
- Authenticated FW download.

These services are provided through industry standard TCG Enterprise SSC, SATA, or SCSI protocols.

1.3 General

ISO/IEC 24759:2017 Section 6 [Number Below]	FIPS 140-3 Section Title	Security Level
1	General	2
2	Cryptographic Module Specification	2
3	Cryptographic Module Interfaces	2
4	Roles, Services, and Authentication	2
5	Software / Firmware Security	2
6	Operational Environment	N/A
7	Physical Security	2
8	Non-Invasive Security	N/A
9	Sensitive Security Parameter Management	2
10	Self-Tests	2
11	Life-Cycle Assurance	2
12	Mitigation of Other Attacks	N/A

Table 1-1: Security Levels

The overall security level pursued for the CM (Cryptographic Module) is Security Level 2.

1.4 Terms and Acronyms

Term / Acronym	Definition
AES	Advanced Encryption Standard (FIPS 197)
CBC	Cipher Block Chaining
CKG	Cryptographic Key Generation
CM	Cryptographic Module
CMAC	Cipher-based Message Authentication Code
CO	Crypto-Officer

Term / Acronym	Definition
CSP	Critical Security Parameter
CSPSK	Critical Security Parameter Sanitization Key
DRBG	Deterministic Random Bit Generator
ECB	Electronic Codebook Mode
FW	Firmware
GCM	Galois Counter Mode
HDD	Hard Disk Drive
HMAC	Hash-based Message Authentication Code
IID	Independent and Identically Distributed
IV	Initialization Vector
KAT	Known Answer Test
KAS SSC FFC	Key Agreement Schemes Shared Secret Computation Finite Field Cryptography
KDF	Key Derivation Function
LBA	Logical Block Address
MEK	Media Encryption Key
MEKEK	Media Encryption Key Encryption Key
PCBA	Printed Circuit Board Assembly
PBKDF	Password-Based Key Derivation Function
POR	Power-On Reset
PSP	Public Security Parameter
PSK	Pre-Shared Key (for TLS handshake)
PSID	Physical Security ID
RSA	Rivest-Shamir-Adleman public-key cryptosystem
SAK	Signing Authority Key
SAS	Serial Attached SCSI
SATA	Serial ATA (AT Attachment)
SCSI	Small Computer System Interface
SED	Self-Encrypting Drive
SHA	Secure Hash Algorithm
SSC	Security Subsystem Class
SSP	Sensitive Security Parameter
TCG	Trusted Computing Group
XTS	XEX-based tweaked-codebook mode with ciphertext stealing

Table 1-2: Terms and Acronyms

2 Cryptographic Module Specification

2.1 Cryptographic Module Information

The Cryptographic Module (CM) is defined as a hardware module. It is a multi-chip embedded physical embodiment contained in a full drive enclosure. No part of the enclosure is excluded from the security requirements. A photo of an example module is provided in Figure 1.

The physical interface to the CM is a SATA or SAS connector. The data carried over the SATA and SAS connectors conform to the industry-standard SCSI, SATA, or TCG Enterprise SSC.

The primary function of the module is to provide data encryption access control and cryptographic erase of the data stored on the drive media. The human operator of the drive interfaces with the CM through a “host” application on a host system. There is also an LED status indicator on the CM.

The CM may operate in one of two mutually exclusive security modes:

- TCG Security Mode – In the Security mode, access control for User Data is managed by the Locking SP. In TCG mode the CM can support multiple independent User Data bands/ranges via the TCG Enterprise SSC protocol. To operate the CM in TCG Security Mode, the host must follow the steps described in 11.1.1 and 11.1.2.

- ATA Security Mode – In ATA mode, access control for User Data is managed by the ATA Security State. In ATA mode, the CM only supports a single User Data LBA band/range that includes all LBAs on the CM. To operate the CM in ATA Security Mode, the host must follow the steps described in 11.1.3 and 11.1.4.

  Note: ATA Security mode is only supported on CMs that support the ATA Security feature set.

  When the CM is in the TCG Security Mode or ATA Security Mode, the CM is in a Compliant state if the steps described in 11.1 are followed. If the CM is in a Compliant state, whether or not the CM is in an Approved mode or a Non-Approved mode is dependent on what types of services the host invokes. If the host invokes an Approved service, then the CM is an Approved mode. If the host invokes a Non-Approved service, then the CM is in a Non-Approved mode.

Figure 1: Seagate Self-Encrypting Drive

2.2 Cryptographic Module Tested Configurations

Model	Hardware [Part Number and Version]	Firmware Version	Distinguishing Features
Exos X18 3.5" SAS HDD	ST18000NM007J	EP7U EF07	Self-Encrypting Drive SAS (Enterprise SSC)
	ST16000NM007J	EP7U EF07 P705 PSFG FQD4 HPD5	
	ST14000NM007J	EP7U EF07	
	ST12000NM007J	EP7U EF07 P705 PJ07 FQD4	
	ST10000NM016G	EP7U EF07	
Exos 7E10 3.5" SAS HDD	ST10000NM022B	EF34 EF04	Self-Encrypting Drive SAS (Enterprise SSC)
	ST10000NM011B	EF34 KF04	
	ST8000NM022B	EF34 EF04 GCN6 LT0E FRD6 FCE7 FCL7 3P01 HPD5	
	ST8000NM011B	EF34 KF04 L708	
	ST6000NM024B	EF34 EF04 FCE7 FCL7	
	ST6000NM013B	EF34 KF04	
	ST4000NM013B	EF34	

Model	Hardware [Part Number and Version]	Firmware Version	Distinguishing Features
		NF04 FRB5 FKE8 FKL8 HPD6	
	ST4000NM029B	EF34 EF04 3P01	
	ST4000NM017B	EF34 KF04 L708	
Exos 7E10 3.5" SATA HDD	ST10000NM021B	SZFP SF04	Self-Encrypting Drive SATA (Enterprise SSC)
	ST8000NM021B	SZFP SF04 HPG4	
	ST6000NM023B	SZFP SF04	
	ST4000NM012B	SZFP TF04 HPG4	
	ST4000NM028B	SZFP SF04	

Table 2-1: Cryptographic Module Tested Configurations

Select Hardware and Firmware Version combinations will output a different hardware version identification during the "Compliance Indicator Service" as detailed in the table below. There has been no change to the hardware itself.

Hardware [Part Number and Version]	Firmware Version	Show Version Output
ST8000NM022B	3P01	SCBP8000S5xeF7.2
ST4000NM029B	3P01	SCBP4000S5xeF7.2
ST8000NM022B	HPD5	MB008000MYDUD
ST4000NM013B	HPD6	MB004000MYDUB
ST8000NM021B	HPG4	MB008000SYDUC
ST4000NM012B	HPG4	MB004000SYDUA
ST16000NM007J	HPD5	MB016000MYDKC
ST12000NM007J	PJ07	STEPSKF4CLAR12T0

Table 2-2: Hardware Substitute Configurations

2.3 Algorithms

This section describes the algorithms used by the CM. The Approved algorithms are described in section 2.3.1 and the Non-Approved Not Allowed algorithms are described in section 2.3.2. The CM does not implement any of the following categories of cryptographic algorithms:

- Non-Approved Algorithms Allowed in the Approved Mode of Operation
- Non-Approved Algorithms Allowed in the Approved Mode of Operation with No Security Claimed

Note: Not all algorithms, modes, and key sizes that appear in the module's ACVP certificates are utilized by the module.

2.3.1 Approved Algorithms

The Approved algorithms used by the CM are shown in Table 2-3: Approved Algorithms (HW) and Table 2-4: Approved Algorithms (FW).

CAVP Cert	Algorithm & Standard	Mode / Method	Description / Key Size(s) / Key Strength(s)	Use / Function
#A1082	Counter DRBG [SP 800-90A]	AES-256	Prediction Resistance: Yes Mode: AES-256 Derivation Function Enabled: Yes Additional Input: 0 bits, 256 bits Entropy Input: 256 bits Nonce: 128 bits Personalization String Length: 0 bits, 256 bits Returned Bits: 256 bits	Random-bit generation
#A1090	AES-XTS [SP 800-38E]	XTS	Key Size: 256 bits Key Strength: 256 bits	Encryption / decryption
#A1091	HMAC-SHA2-256 [FIPS 198-1]	SHA2-256	MAC: 256 bits Key Length: 8-512 bits, Increment 8	Pseudo random function for PBKDF
#A1092	SHA2-256 [FIPS 180-4]	SHA2-256	Message Length: 0-65528 bits, Increment 8 bits	Cryptographic hashing
#A1093	RSA SigVer (FIPS186-4) [FIPS 186-4]	PKCS 1.5	Signature Type: PKCS 1.5 Modulo: 2048, 3072 Key Strength: 112-bit, 128-bit Hash Algorithm: SHA2-256 (#A1092) Public Exponent Mode: Random	Signature verification
#A3515	AES-CMAC [SP 800-38B]	CMAC	Direction: Generation Key Length: 256 bits Key Strength: 256 bits MAC Length: 8-128 bits, Increment 8 bits Message Length: 128-512 bits Increment 128 bits	Conditioner for the raw entropy from the Ring Oscillator entropy source
N/A	ENT (P) [SP 800-90B]	Ring Oscillators Entropy Source	N/A	Used as a part of the DRBG
N/A	ENT (P) [SP 800-90B]	PES Entropy Source	N/A	Used as a part of the DRBG

Table 2-3: Approved Algorithms (HW)

CAVP Cert	Algorithm & Standard	Mode / Method	Description / Key Size(s) / Key Strength(s)	Use / Function
#A1080	AES-GCM [SP 800-38D][1]	GCM	Direction: Encrypt, Decrypt IV Generation: Internal IV Generation Mode: 8.2.2 Key Length: 128 bits, 256 bits Tag Length: 128 bits IV Length: 96 bits Payload Length: 128 bits, 256 bits AAD Length: 0 bits, 256 bits	Key wrapping (encryption / decryption)
#A1081	AES-CMAC [SP 800-38B]	CMAC	Direction: Generation, Verification Key Length: 128 bits, 256 bits MAC Length: 128 bits Message Length: 0-65536 bits Increment 8 bits	Conditioner for the raw entropy
#A1083	HMAC-SHA2-256 [FIPS 198-1]	SHA2-256	MAC: 256 bits Key Length: 8-512 bits Increment 8 bits	Key derivation for Secure Messaging
#A1084	KAS-FFC-SSC Sp800-56Ar3 [SP 800-56A rev3]	dhEphem	Domain Parameter Generation Methods: ffdhe2048 Key Strength: 112 bits Scheme: dhEphem: KAS Role: initiator, responder	Key Agreement for Secure Messaging
#A1084 (KAS-FFC-SSC Cert.), #A1089 (KDF TLS Cert)	KAS [SP 800-56A rev3]	SP 800-56A rev3. KAS-FFC per IG D.F Scenario 2 path (2)	Key Size: 2048 bits Key Strength: 112 bits	Key Agreement and Derivation for Secure Messaging
#A1085	PBKDF [SP 800-132 rev1]	Option 2a[2]	Iteration Count: 1-10000000, Increment 1 HMAC Algorithm: HMAC-SHA2-256 (#A1091) Password Length: 8-64 bytes Increment 1 Salt Length: 128-512 bits, Increment 8 bits Key Data Length: 112-4096 bits Increment 8 bits	Key derivation[3]
#A1087	Safe Primes Key Generation [SP 800-56A rev3]	ffdhe2048	Safe Prime Groups: ffdhe2048 Key Strength: 112 bits	Key Generation for dhEphem
#A1088	SHA2-256 [FIPS 180-4]	SHA2-256	Message Length: 0-65528 bits Increment 8 bits	Cryptographic hashing
	SHA2-384 [FIPS 180-4]	SHA2-384	Message Length: 0-65528 bits Increment 8 bits	Cryptographic hashing

[1] The 96-bit IV used for AES GCM is generated by the module randomly by the DRBG.
[2] The value of the Iteration Count used is 1000 which meets the requirements in [SP 800-132 rev1] and customer performance requirements.
[3] All keys derived used PBKDF are only used for storage applications.

#A1089	KDF TLS (CVL) [SP 800-135 rev1]	TLS v1.2	TLS Version: v1.2 Hash Algorithm: SHA2-256 (#A1088), SHA2-384 (#A1088)	Key derivation for Secure Messaging. No parts of the TLS protocol, other than the approved cryptographic algorithms and TLS KDF, have been tested by the CAVP and CMVP.
#A1094	AES-KW [SP 800-38F]	KW	Direction: Decrypt, Encrypt Cipher: Cipher Key Length: 256 bits Key Strength: 256bits Payload Length: 128 bits, 192 bits, 256 bits, 320 bits, 4096 bits	Key wrapping
#A1095	AES-CBC [SP 800-38A]	CBC	Key Length: 128 bits, 256 bits Key Strength: 128bits, 256 bits	Encryption / decryption
Vendor Affirmed	CKG [SP 800-133 rev2]	Sections 4, 5.2 and 6.1	Cryptographic Key Generation; SP 800-133 rev2 and IG D.H	Key Generation Note: Symmetric keys and seeds used for asymmetric key pairs are produced using the unmodified/direct output of the DRBG.

Table 2-4: Approved Algorithms (FW)

2.3.2 Non-Approved, Not Allowed Algorithms

The Non-Approved, Not Allowed algorithms used by the CM are shown in Table 2-5: Non-Approved Algorithms Not Allowed in the Approved Mode of Operation.

Algorithm / Function	Use / Function
AES-CMAC (non-compliant)	Message authentication
AES-GCM (non-compliant)	Key wrapping (encryption / decryption)
AES-KW (non-compliant)	Key wrapping (encryption / decryption)
AES-XTS (non-compliant)	Encryption / decryption
PBKDF (non-compliant)	Password-based key derivation
RSA SigGen (non-compliant)	Signature generation

Table 2-5: Non-Approved Algorithms Not Allowed in the Approved Mode of Operation

2.4 Cryptographic Boundary

The cryptographic boundary is the enclosure of the drive. The only accessible interfaces to the CM are the SAS/SATA interface and the Power connector. A block diagram of the CM is provided in Figure 2.

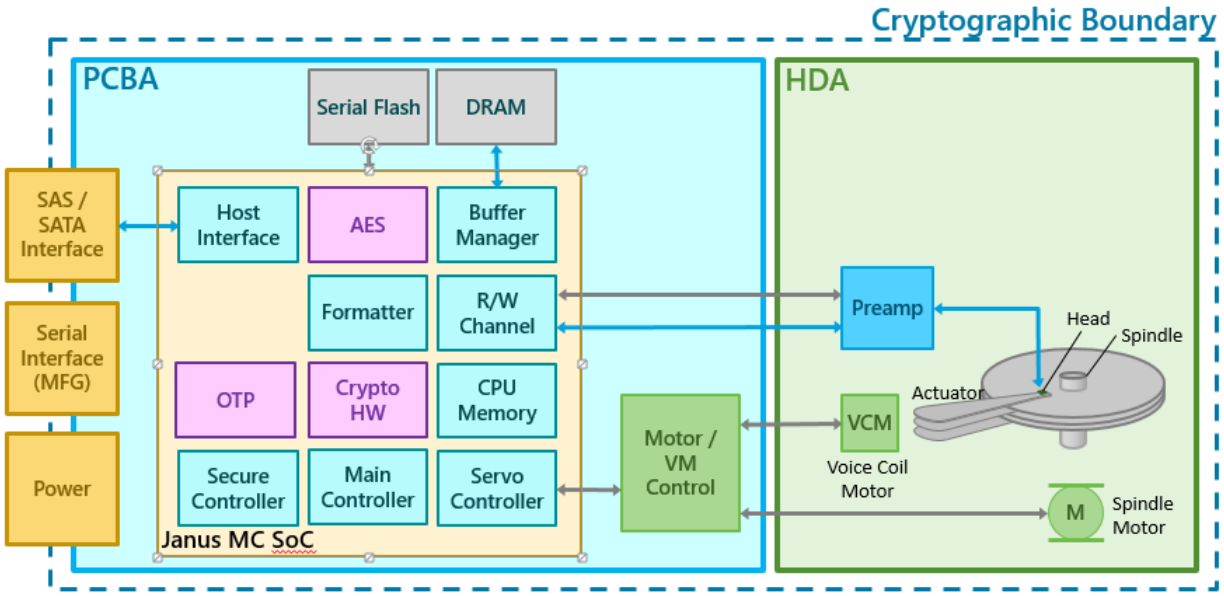

Figure 2: Hardware Block Diagram

2.5 Keys, Authentication, and Other Protected Information

Keys and Protected Information are listed in Section 9 of this document. Authentication is listed in Section 4 of this document.

2.6 Degraded Mode of Operation

The CM does not support a degraded mode of operation.

2.7 Requirements from International Standards

The CM follows many standards including:

- SAS: http://en.wikipedia.org/wiki/Serial_attached_SCSI
- SATA: https://en.wikipedia.org/wiki/Serial_ATA
- TCG Enterprise: https://trustedcomputinggroup.org/work-groups/storage/

3 Cryptographic Module Interfaces

Physical Port	Logical Interface	Data that Passes Over Port / Interface
SAS Connector	• Data input • Data output • Control input • Status output	• TCG Packets • SCSI Packets
SATA Connector	• Data input • Data output • Control input • Status output	• TCG Packets • SATA Packets
LED	Status output	N/A
Power Connector	Power input	N/A
Serial Port	Disabled	N/A

Table 3-1: Ports and Interfaces

The CM does not support a control output interface.

4 Roles, Services, and Authentication

This section describes the roles, services, and authentications supported by the CM.

Some services in this section are identified as aligning with the “lock-based authentication model”. The “lock-based authentication model” is described in IG 4.1.A. The primary purpose of the CM is data-at-rest protection for User Data and the “lock-based authentication model” is sufficient to meet this use case. Assuming the CM has been correctly initialized (see section 11.1), when the CM is powered cycled, the CM will be in a locked state and will require authentication and unlocking prior to the Approved service being available.

4.1 Roles, Service Command, Input and Output – TCG Security Mode

Role	Service	Input	Output
Drive Owner (Crypto Officer)	Set PIN	TCG Set Method	TCG Return Status
	Set FW Ports	TCG Set Method	
	Set TLS PSK	TCG Set Method	
	Create TLS Session	TCG StartTLS Method	
	Send/Receive TLS Message	IF-Send/IF-Receive	Interface Return Status
	FW Download[4]	Interface FW Download Command	
EraseMaster (Crypto Officer)	Set PIN	TCG Set Method	TCG Return Status
	Cryptographic Erase	TCG Erase Method	
	Certified Erase	TCG Erase Method	
	Enable/Disable BandMasters	TCG Set Method	
	Set TLS PSK	TCG Set Method	
	Create TLS Session	TCG StartTLS Method	
	Send/Receive TLS Message	IF-Send/IF-Receive	Interface Return Status
BandMaster (0-31) (Crypto Officer)	Set PIN	TCG Set Method	TCG Return Status
	Set Range Attributes	TCG Set Method	
	Lock / Unlock User Data for Read and/or Write	TCG Set Method	
	Set TLS PSK	TCG Set Method	
	Create TLS Session	TCG StartTLS Method	
	User Data Read / Write (Locking Enabled)[5]	Interface Read / Write Command	Interface Return Status
	Send/Receive TLS Message	IF-Send/IF-Receive	
Unauthenticated	Show Status	TCG Level 0 Discovery, TCG Get Method	

[4] No operator authentication is enforced for the FW Download service that was unlocked by the Set FW Ports service. If the new FW violates device FW rollback policy both the FW Download and Rollback FW Download ports must be unlocked. This service aligns with the “lock-based authentication model” (see section 4).

[5] No operator authentication is enforced for the User Data Read / Write service that was unlocked by the Lock / Unlock User Data for Read and/or Write service. This service aligns with the “lock-based authentication model” (see section 4).

Role	Service	Input	Output
	Reset Module	POR	TCG Return Status
	Unblock PIN	POR	
	DRBG Generate Bytes	TCG Random Method	
	Exit FIPS Mode	TCG RevertSP Method	
	Compliance Indicator	TCG Level 0 Discovery	

Table 4-1: Roles, Service Commands, Input and Output – TCG Security Mode

4.2 Roles, Service Command, Input and Output – ATA Security Mode (if ATA Security supported)

Role	Service	Input	Output
Drive Owner (Crypto Officer)	Set PIN/Password	TCG Set Method	TCG Return Status
	Set FW Ports	TCG Set Method	
	FW Download[6]	Interface FW Download Command	Interface Return Status
Master, User (Crypto Officer)	Set PIN/Password	ATA Security Set Password	Interface Return Status
	Lock / Unlock User Data for Read and/or Write	ATA Authenticate	
	Cryptographic Erase	ATA Erase	
	User Data Read / Write[7]	Interface Read / Write Command	
Unauthenticated	Show Status	TCG Level 0 Discovery	TCG Return Status
	Reset Module	POR	
	Unblock PIN	POR	
	Disable Services	ATA Freeze Lock	
	Exit FIPS Mode	TCG RevertSP Method	
	Compliance Indicator	TCG Level 0 Discovery	

Table 4-2: Roles, Service Commands, Input and Output - ATA Security Mode

4.3 Roles and Authentication – TCG Security Mode

Role	Authentication Method	Authentication Strength
Drive Owner (Crypto Officer)	Role-based authentication. Memorized Secret Authenticator type from SP 800-63B.	Min PIN length is 8 bytes (64 bits) and each failed authentication takes a minimum of 15ms which calculates into a probability to guess the PIN in one minute to $4000/2^{64}$
EraseMaster (TCG Security Mode) (Crypto Officer)	Role-based authentication. Memorized Secret Authenticator type from SP 800-63B.	Min PIN length is 8 bytes (64 bits), and each failed authentication takes a minimum of 15ms which calculates into a probability to guess the PIN in one minute to $4000/2^{64}$

[6] No operator authentication is enforced for the FW Download service that was unlocked by the Set FW Ports service. If the new FW violates device FW rollback policy both the FW Download and Rollback FW Download ports must be unlocked. This service aligns with the “lock-based authentication model” (see section 4).

[7] No operator authentication is enforced for the User Data Read / Write (Locking Enabled) service that was unlocked by the Lock / Unlock User Data for Read and/or Write service. This service aligns with the “lock-based authentication model” (see section 4).

Role	Authentication Method	Authentication Strength
BandMaster (0-31) (TCG Security Mode) (Crypto Officer)	Role-based authentication. Memorized Secret Authenticator type from SP 800-63B.	Min PIN length is 8 bytes (64 bits), and each failed authentication takes a minimum of 15ms which calculates into a probability to guess the PIN in one minute to $4000/2^{64}$

Table 4-3: Roles and Authentication - TCG Security Mode

4.4 Roles and Authentication – ATA Security Mode (if ATA Security supported)

Role	Authentication Method	Authentication Strength
Drive Owner (Crypto Officer)	Role-based authentication. Memorized Secret Authenticator type from SP 800-63B.	Min PIN length is 32 bytes (256 bits), and each failed authentication takes a minimum of 15ms which calculates into a probability to guess the PIN in one minute to $4000/2^{256}$
User (ATA Security Mode) (Crypto Officer)	Role-based authentication. Memorized Secret Authenticator type from SP 800-63B.	Min PIN length is 32 bytes (256 bits), and each failed authentication takes a minimum of 15ms which calculates into a probability to guess the PIN in one minute to $4000/2^{256}$
Master (ATA Security Mode (Crypto Officer)	Role-based authentication. Memorized Secret Authenticator type from SP 800-63B.	Min PIN length is 32 bytes (256 bits), and each failed authentication takes a minimum of 15ms which calculates into a probability to guess the PIN in one minute to $4000/2^{256}$

Table 4-4: Roles and Authentication - ATA Security Mode

4.5 Approved Services, SSPs, Roles, and Access Rights

If the CM is operating in TCG Security Mode, the Approved services provided by the CM are described in section 4.5.1. If the CM is operating in ATA Security Mode, the Approved services provided by the CM are described in 4.5.2.

4.5.1 Approved Services – TCG Security Mode

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys and/or SSPs[8]	Indicator
Set PIN	Change operator authentication data	PBKDF (#A1085), AES-GCM (#A1080), HMAC-SHA2-256 (#A1091), SHA2-256 (#A1092)	EraseMaster Password, BandMaster Password, SID	EraseMaster, BandMaster, Drive Owner	W	TCG Return Status

[8] Definitions for Roles SSP Access column values:

- G = Generate: The module generates or derives the SSP
- R = Read: The SSP is read from the module (e.g., the SSP is an output)
- W = Write: The SSP is updated, imported, or written to the module
- E = Execute: The module uses the SSP in performing a cryptographic operation
- Z = Zeroize: The module zeroizes the SSP

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys and/or SSPs[8]	Indicator
FW Download	Load complete FW image. If code self-test passes with a valid key, device runs new code.	RSA SigVer (#A1093, 3072-bit), SHA2-256 (#A1092)	Firmware Update Key, Platform Key, SAK	Drive Owner[9]	E	ATA/SCSI Status
Enable / Disable BandMasters	Enable / disable a user authority	PBKDF (#A1085), HMAC-SHA2-256 (#A1091), SHA2-256 (#A1092)	BandMaster Password	EraseMaster	E	TCG Return Status
Set FW Ports	Set PortLocked and LockOnReset attributes on the FW Download port or Rollback FW Download port	None	None	Drive Owner	E	TCG Return Status
Set Range Attributes	Set location, size, and locking attributes of an LBA range	None	None	BandMasters	None	TCG Return Status
Lock / Unlock User Data Range for Read and/or Write	Block or allow read (decrypt) or write (encrypt) of user data in a range	AES-KW (#A1094)	MEK, MEKEK, CSPSK	BandMasters	E	TCG Return Status
User Data Read / Write (Locking Enabled)	Encrypt / decrypt user data from an LBA range where Locking is enabled[10]	AES-XTS (#A1090)	MEK	BandMasters[11]	E	ATA/SCSI Status
Cryptographic Erase	Erase user data in LBA range and place the range in the uninitialized state.	None	MEKEK, MEK, Master Key, CSPSK, Bandmaster Password	EraseMaster	Z	TCG Return Status

[9] FW download port must be unlocked.
[10] Locking is enabled for an LBA range if the ReadLockEnabled and WriteLockEnabled values are set to "True" and the LockOnReset value includes "Power Cycle". The current values of these attributes can be determined using the Show Status Approved Service (i.e., the TCG Get Method on the associated LBA range locking object).
[11] User Data range must be unlocked.

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys and/or SSPs[8]	Indicator
FW Rollback	Prevents downgrading FW to a release that violates the device FW rollback policy	None	None	Drive Owner	None	ATA/SCSI Status
Create TLS Session	Support host-initiated TLS Session	Safe Primes Key Generation (# A1087), KAS (#A1084), KDF TLS (#A1089), HMAC-SHA2-256 (#A1083)	Secure Messaging Session Key, Secure Messaging Key Pair, Bandmaster PSKs, EraseMaster PSK, Drive Owner PSK	Drive Owner, EraseMaster, BandMaster	E	TCG Return Status
Set TLS PSK	Set Pre-Shared key used for TLS	None	BandMaster PSKs, EraseMaster PSK, Drive Owner PSK	Drive Owner, EraseMaster, BandMaster	W	TCG Return Status
Send/Receive TLS Message	Send or receive a TLS message	AES-CBC (#A1095), AES-GCM (#A1080), SHA2-256 (#A1088), SHA2-384, (#A1088)	Secure Messaging Session Key, Secure Messaging Key Pair	Drive Owner, EraseMaster, BandMaster	E	ATA/SCSI Status
Certified Erase	Erase user data in LBA range and place the range in the uninitialized state.	None	MEKEK, MEK, Master Key, CSPSK, Bandmaster Password	EraseMaster	Z	TCG Return Status
Show Status	Provides information on the current configuration of the CM and reports whether FIPS service is operational and operating in a Compliant state.	None	None	None	None	TCG Return Status, ATA/SCSI Status

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys and/or SSPs[8]	Indicator
Reset Module	Runs Pre-Operational Self- Tests and zeroizes keys and CSPs in RAM and complete the Secure Boot process by validating the FW on the drive.	RSA SigVer (#A1093, 3072-bit), SHA2-256 (#A1092)	SID, EraseMaster Password, BandMaster Password	None	Z	N/A
Unblock PIN	Resets password attempt counters	None	None	None	None	N/A
DRBG Generate Bytes	Returns SP800-90A rev1 DRBG random number	Counter DRBG (#A1082), AES-CMAC (#A1081) AES-CMAC (#A3515), ENT (P)	None	None	None	TCG Return Status
Exit FIPS Mode	Exit a Compliant state[12]	None	SID Password, EraseMaster Password, BandMaster Password, MEKs, MEKEKs, Master Keys, CSPSKs, EraseMaster PSK, BandMaster PSKs, Drive Owner PSK	None (using PSID)	Z	TCG Return Status
Compliance Indicator	Reports FIPS 140 revision, overall security level, HW and FW revisions, and module name	None	None	None	None	TCG Return Status

[12] CM will enter Uninitialized State.

Table 4-5: Approved Services - TCG Security Mode

4.5.2 Approved Services – ATA Security Mode (if ATA Security supported)

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys and/or SSPs[13]	Indicator
Set PIN/Password	Change operator authentication data. Note: Setting the User PIN may also set the Drive Owner PIN	PBKDF (#A1085), AES-GCM (#A1080), HMAC-SHA2-256 (#A1091), SHA2-256 (#A1092)	Master, User Passwords	Master, User, Drive Owner	W	TCG Return Status, ATA Status
FW Download	Enable / disable FW download port and load complete FW image. If code self-test passes with a valid key, device runs new code	RSA SigVer (#A1093, 3072-bit), SHA2-256 (#A1092)	Firmware Update Key, Platform Key, SAK	Drive Owner[14]	E	TCG Return Status, ATA Status
FW Rollback	Prevents downgrading FW to a release that violates the device FW rollback policy	None	None	Drive Owner	None	ATA Status
Lock / Unlock User Data Range for Read and/or Write	Enable user data read/write and Set PIN services	AES-KW (#A1094)	MEK	User (optional, Master)	E	ATA Status
User Data Read / Write	Encryption / decryption of user data	AES-XTS (#A1090)	MEK	User (optional, Master)[15]	E	ATA Status
Cryptographic Erase	Erase user data on CM and place the CM in the uninitialized state.	None	MEKEK, MEK, Master Keys, CSPSK, User Password	Master, User	Z	ATA Status
Unblock PIN	Reset Master and User password attempt counter	None	None	None	None	N/A
Set FW Ports	Set PortLocked and LockOnReset attributes on the FW Download port or Rollback FW Download port	None	None	Drive Owner	E	TCG Return Status

[13] Definitions for Roles SSP Access column values:
- G = Generate: The module generates or derives the SSP
- R = Read: The SSP is read from the module (e.g., the SSP is an output)
- W = Write: The SSP is updated, imported, or written to the module
- E = Execute: The module uses the SSP in performing a cryptographic operation
- Z = Zeroize: The module zeroizes the SSP

[14] FW download port must be unlocked.

[15] User Data must be unlocked.

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys and/or SSPs[13]	Indicator
Show Status	Provides information on the current configuration of the CM and reports whether FIPS service is operational and operating in a Compliant state.	None	None	None	None	ATA Status / TCG Return Status
Reset Module	Runs Pre-Operational Self-Tests and zeroizes keys and CSPs in RAM and complete the Secure Boot process by validating the FW on the drive.	RSA SigVer (#A1093, 3072-bit), SHA2-256 (#A1092)	Master Password, User Password	None	Z	N/A
Disable Services	Disables ATA Security commands until POR	None	None	None	None	ATA Status
Exit FIPS Mode	Exit a Compliant state[16]	None	Master Password, User Password, MEK, MEKEK, Master Keys, CSPSK	None (using PSID)	Z	TCG Return Status
Compliance Indicator	Reports FIPS 140 revision, overall security level, HW and FW revisions, and module name	None	None	None	None	TCG Return Status

Table 4-6: Approved Services – ATA Security Mode

[16] CM will enter Uninitialized State.

4.6 Non-Approved Services

The Non-Approved services provided by the CM are described in Table 4-7.

Service	Description	Algorithms Accessed	Roles	Indicator
User Data Read / Write (Locking Disabled)	Encrypt / decrypt user data from an LBA range where Locking is disabled[17]	AES-XTS (non-compliant)	None	ATA/SCSI Status
Cryptographic Erase	Generates new range key following sanitization of the electronic media.	Counter DRBG (#A1082)[18], AES-CMAC (non-compliant), AES-KW (non-compliant), AES-GCM (non-compliant), PBKDF (non-compliant)	EraseMaster	ATA/SCSI Status
Certified Erase	Generates new range key and provides certificate of media disposition for each piece of the electronic media following sanitization.	Counter DRBG (#A1082)[18] AES-CMAC (non-compliant), AES-KW (non-compliant), AES-GCM (non-compliant), PBKDF (non-compliant), RSA SigGen (non-compliant)	EraseMaster	ATA/SCSI Status

Table 4-7 Non-Approved Services

[17] Locking is disabled for an LBA range if the ReadLockEnabled or WriteLockEnabled values are set to “False”, or the LockOnReset value does not include “Power Cycle”. The current values of these attributes can be determined using the Show Status Approved Service (i.e., the TCG Get Method on the associated LBA range locking object),

[18] Allowed per FIPS 140-3 IG 4.1.A, Exception b.

5 Software / Firmware Security

During the power-on boot process, the CM will verify the authenticity and integrity of the CM firmware using RSA Signature Verification (certificate #A1093) with the following parameters:

- The key is the Signing Authority Key i.e., SAK (see section 9.2).
- The modulus size is 3072 bits.
- The hash function is SHA2-256 (#A1092).

The operator can invoke the boot firmware integrity test on demand by performing a power-on reset operation on the CM.

6 Operational Environment

The CM operates in a limited operational environment where the CM firmware (FW) may be updated by an external source via the FW download operation. Prior to accepting new FW provided by the FW download operation, the CM will verify the signature of the new FW (see section 10.2).

Note: The ability to download FW to the device is restricted based on the state of the FW Download and Rollback Download logical ports (see section 4.5). All FW downloads require the FW Download port to be unlocked. Rollback FW downloads (i.e., downgrading FW to a release that violates the device FW rollback policy) require both the FW Download and Rollback FW Download ports to be unlocked,

7 Physical Security

The CM is a multi-chip embedded module of product grade components with standard passivation. The CM is surrounded in a metal enclosure that is opaque within the visible spectrum. To meet the level 2 physical security requirements, the CM employs a single factory installed tamper-evident labels to prevent physical tampering. Refer to Table 7-1 for actions required by the operator to ensure that physical security is maintained.

Figure 3: Module 1 Seal Application Locations

Physical Security Mechanism	Recommended Frequency of Inspection / Test	Inspection / Test Guidance Details
Opaque, tamper-evident security label (TEL) on exposed (back) side of PCBA	The frequency of the physical inspection should be determined by the Crypto Officer. It is recommended that the TEL be inspected monthly.	Periodic inspection of TEL to detect evidence of tampering: • Checkerboard pattern on TEL • Security label cutouts do not match original • Security label over PCBA screws not penetrated Upon discovery of tamper evidence, the module should be removed from service. Refer to the End-of-Life section of this document for more information on removing the module from service.

Table 7-1: Physical Security Inspection Guidelines

8 Non-Invasive Security

The CM does not provide mitigation against any non-invasive attacks.

9 Sensitive Security Parameter Management

9.1 SSP Storage Areas

The storage areas on the CM where SSPs may be present are described in Table 9-1.

Table 9-1: SSP Storage Areas

Name	Description	Persistence Type
DRAM	Temporary, volatile memory	Dynamic
HW Registers	Temporary, volatile memory	Dynamic
ROM	Persistent, non-modifiable, non-volatile memory	Static
Media	Persistent, non-volatile memory	Static
Serial Flash	Persistent, non-volatile memory	Static

9.2 SSPs

The SSPs (Sensitive Security Parameters) used by the device are different depending on which security mode the CM is operating. The SSPs used by the CM are described in Table 9-2.

Key / SSP Name / Type	Strength	Security Function & Cert. Number	Generation	Import / Export	Establishment	Storage	Zeroization	Use & Related Keys
SID[19] / CSP	256 bits	PBKDF (#A1085)	N/A	Import: sent from host	N/A	DRAM, plaintext	Reset Module, Set PIN	Set PIN
Master, User Passwords (ATA Security Mode only) / CSP	256 bits	PBKDF (#A1085)	N/A	Import: sent from host	N/A	DRAM, plaintext	Reset Module, Set PIN	Set PIN Unlock user data
Master/User MEK (ATA Security Mode only) / CSP	256 bits	AES-XTS (#A1090), CKG	Internally generated	N/A	N/A	HW Registers, plaintext Media, AES-KW encrypted	Exit FIPS Mode, Cryptographic Erase	Unlock user data Cryptographic erase Encrypted by MEKEKs and CSPSKs
EraseMaster Password (TCG Security Mode) / CSP	64-256 bits	PBKDF (#A1085)	N/A	Import: sent from host	N/A	DRAM, plaintext	Reset Module	Set PIN Cryptographic erase
BandMaster (0-31) Passwords (TCG Security Mode) / CSP	64-256 bits	PBKDF (#A1085)	N/A	Import: sent from host	N/A	DRAM, plaintext	Reset Module, Set PIN, Cryptographic Erase	Set PIN Lock / unlock user data
MEKs / CSP	256 bits	AES-XTS (#A1090), CKG	Internally generated	N/A	N/A	HW Registers, plaintext Media, AES-KW encrypted	Exit FIPS Mode, Cryptographic Erase	Lock / Unlock User Data Range for Read and/or Write Encrypted by MEKEKs and CSPSKs
Entropy Input String / CSP	448 bits	Counter DRBG (#A1082)	Internally generated	N/A	N/A	DRAM, plaintext	N/A	Services using DRBG (cryptographic erase)

[19] Drive Owner PIN

Key / SSP Name / Type	Strength	Security Function & Cert. Number	Generation	Import / Export	Establishment	Storage	Zeroization	Use & Related Keys
DRBG Seed / CSP	384 bits	Counter DRBG (#A1082)	Internally generated	N/A	N/A	HW Registers, plaintext	N/A	Services using DRBG (cryptographic erase, Set PIN)
DRBG Key / CSP	256 bits	Counter DRBG (#A1082)	Internally generated[20]	N/A	N/A	HW Registers, plaintext	N/A	Services using DRBG (cryptographic erase, Set PIN)
DRBG Internal State V / CSP	128 bits	Counter DRBG (#A1082)	Internally generated[20]	N/A	N/A	HW Registers, plaintext	N/A	Services using DRBG (cryptographic erase, Set PIN)
Platform Key[21] / PSP	3072 bits / 128 bits (strength)	RSA SigVer (#A1093)	Pre-loaded at factory	N/A	N/A	ROM, plaintext	N/A	Reset module
Firmware Update Key / PSP	3072 bits / 128 bits (strength)	RSA SigVer (#A1093)	Pre-loaded at factory	N/A	N/A	ROM, plaintext	N/A	FW download
SAK[22] / PSP	3072 bits / 128 bits (strength)	RSA SigVer (#A1093)	Pre-loaded at factory	Import: Embedded in Firmware Download Image	N/Al	Serial Flash, plaintext	N/A	Reset module
MEKEK / CSP	256 bits	AES-KW (#A1094), CKG	Internally generated	N/A	N/A	DRAM, plaintext Media, AES-GCM encrypted	Exit FIPS Mode	Lock / Unlock User Data Range for Read and/or Write Cryptographic erase Set PIN Encrypted by Master Keys
Master Key / CSP	256 bits	AES-GCM (#A1080), PBKDF (#A1085)	Derived	N/A	N/A	DRAM, plaintext	Exit FIPS Mode	Lock / Unlock User Data Range for Read and/or Write Cryptographic erase Set PIN

[20] Source: section 4 Terms and Definitions of NIST Special Publication 800-90A. Values of V and the AES key are the critical values of the internal state on which the security of this DRBG mechanism depends (i.e., V and the AES key are the "secret values" of the internal state).
[21] PK is used for pre-operational FW integrity test and is not an SSP but included in this table for completeness.
[22] SAK is used for pre-operational FW integrity test and are not SSPs but included in this table for completeness.

Key / SSP Name / Type	Strength	Security Function & Cert. Number	Generation	Import / Export	Establishment	Storage	Zeroization	Use & Related Keys
CSPSKs / CSP	256 bits	AES-KW (#A1094), CKG	Internally generated	N/A	N/A	DRAM, plaintext Media, plain text	Exit FIPS Mode	Lock / Unlock User Data Range for Read and/or Write Cryptographic erase Set PIN
Drive Owner PSKs / CSP	32-512 bits	KAS-FFC-SSC Sp800-56Ar3 (#A1084)	N/A	Import: sent from host	N/A	DRAM, plaintext Media, plaintext	Exit FIPS Mode	Set TLS PSK
EraseMaster PSK (TCG Security Mode) / CSP	32-512 bits	KAS-FFC-SSC Sp800-56Ar3 (#A1084)	N/A	Import: sent from host	N/A	DRAM, plaintext Media, plaintext	Exit FIPS Mode	Set TLS PSK
BandMaster PSKs (TCG Security Mode) / CSP	32-512 bits	KAS-FFC-SSC Sp800-56Ar3 (#A1084)	N/A	Import: sent from host	N/A	DRAM, plaintext Media, plaintext	Exit FIPS Mode	Set TLS PSK
Secure Messaging Session Key / CSP	128-256 bits	AES-GCM (#A1080). KDF TLS (#A1089)	Derived	N/A	N/A	DRAM, plaintext	Reset Module	Send/Receive TLS Message
Secure Messaging Key Pair / CSP	2048 bits / 112 bits (strength) & 256 bits	KAS-FFC-SSC Sp800-56Ar3 (#A1084) Safe Primes Key Generation (#A1087) CKG KDF TLS (#A1089)	Internally generated	N/A	N/A	DRAM, plaintext	N/A	Send/Receive TLS Message

Table 9-2: SSPs

9.3 Entropy Sources

The Entropy sub-system uses a Non-Deterministic Random Bit Generator (NRBG) to generate random data. The NRBG is supplied with conditioned entropy via two Entropy sources. Each conditioned output of an entropy source is a 128-bit full entropy output. The NRBG used by the device is the XOR-NRBG construction described in SP 800-90C and the DRBG construction is based on SP 800-90A rev 1.

The DRBG seed used for instantiation is constructed by concatenating the following values:

- Entropy Input (256 bits of conditioned entropy)
- Nonce (128 bits of conditioned entropy)
- Personalization String (64 bits of device unique data such as the device serial number padded to 256 bits)

The concatenated value is passed to the derivation function Block_Ciper_df as described in SP 800-90A rev. 1 which outputs 384 bits of seed material.

The design of the entropy sources is based on the recommendations in SP 800-90B. The entropy sub-system has two independent entropy sources:

- Ring Oscillator entropy source
- PES entropy source

The Entropy sources generate entropy samples when required by the Entropy sub-system. The raw samples from each entropy source are stored in independent entropy pools. The raw entropy samples from each source are concatenated into 128-bit blocks. When there are greater than 256 bits of entropy in an entropy pool , based on the minimum entropy of the sources, the Entropy subsystem concatenates sufficient 128-bit blocks for 256 bits of entropy and passes the concatenation of these blocks to the CMAC conditioner (#A1081 (PES) and #A3515 (Ring Oscillator)).

The entropy sources used by the CM are described in Table 9-3.

Entropy Sources	Minimum Number of Bits of Entropy	Details
Position Error Signal (PES)	3 out of 4-bits	Met IID requirements
Ring Oscillators	6 out of 8-bits	Met IID requirements

Table 9-3: Non-Deterministic Random Number Generation Specification

9.4 Zeroization Methods

The method used by the CM to zeroize SSPs is different depending on where the SSP is stored:

- If a SSP is stored in volatile memory, the CM will zeroize the SSP (when required) by writing the memory where the SSP is stored with a pattern of all bytes set to 0x00.

  Note: When the CM is powered down all SSPs stored in volatile memory are zeroized automatically as the volatile memory can only store data when powered.

- If a SSP is stored unprotected (i.e., plaintext) in non-volatile memory, the CM will zeroize the SSP (when required) by writing the memory where the SSP is stored with a pattern of all bytes set to 0x00 and then writing the new SSP value.

[23] The combined entropy is calculated using Method 2 as described in IG D.O Combining Entropy from Multiple Sources.

- If a SSP is stored protected (i.e., encrypted using another SSP) in non-volatile memory, the CM will zeroize the SSP (when required) by writing the memory where the SSP is stored with a new SSP value.[24]

[24] As indicated in Table 9-2 some keys are stored encrypted on the CM using an approved algorithm. Per IG 9.6.A, they are considered “protected” thus not requiring zeroization when unprotected SSPs are zeroized.

10 Self-Tests

The sections below list all self-tests performed by the module, along with the failure behavior when any of the self-tests fail. While in an error state, the module outputs an error indicator, disables cryptographic operations and the data output interface is inhibited. All pre-operational and conditional self-tests can be executed on-demand by power-cycling the module.

10.1 Pre-Operational Self-Tests

Function Tested	Self-Test Type	Implementation	Failure Behavior
Firmware Integrity	Integrity Test[25]	RSA PKCS#1 3072/SHA-256 signature verification on signed FW stored on the CM (#A1093 and #A1092)[26]. The keys used are the Platform Key and one of the SAKs (see section 9.2).	Enters FW Integrity Error State.

Table 10-1: Pre-Operational Self-Tests

10.2 Conditional Self-Tests

Function Tested	Self-Test Type	Implementation	Failure Behavior
Hardware Self-Tests			
AES-XTS (#A1090)	Cryptographic Algorithm Self-Test	XTS encrypt KAT / 256-bit key	Enters FIPS Self-Test Error State
AES-XTS (#A1090)	Cryptographic Algorithm Self-Test	XTS decrypt KAT / 256-bit key	Enters FIPS Self-Test Error State
AES-XTS (#A1090)	Critical Functions Test: When an AES XTS Key is generated	Generated XTS Key_1 and Key_2 are compared, as per IG C.I, before being used.	Keys are discarded
SHA2-256 (#A1092)	Cryptographic Algorithm Self-Test	Digest KAT	Enters FIPS Self-Test Error State
HMAC-SHA2-256 (#A1091)	Cryptographic Algorithm Self-Test	HMAC SHA-256 KAT / 256-bit key	Enters FIPS Self-Test Error State
RSA SigVer (#A1093)	Cryptographic Algorithm Self-Test	Signature Verification KAT / 3072-bit key	Enters FIPS Self-Test Error State
AES-CMAC (#A3515)	Cryptographic Algorithm Self-Test	CMAC KAT / 256-bit bit key	Enters FIPS Self-Test Error State
Counter DRBG (#A1082)	Cryptographic Algorithm Self-Test	KAT	Enters FIPS Self-Test Error State
Counter DRBG (#A1082)	Critical Functions Test: When a random number is generated	Instantiate, generate, reseed and un-instantiate health tests as per section 11.3 of SP 800-90A	Enters FIPS Self-Test Error State
Firmware Self-Tests			
AES-CBC (#A1095)	Cryptographic Algorithm Self-Test	CBC encrypt KAT / 256 bit key	Enters FIPS Self-Test Error State
AES-CBC (#A1095)	Cryptographic Algorithm Self-Test	CBC decrypt KAT / 256-bit key	Enters FIPS Self-Test Error State
AES-GCM (#A1080)	Cryptographic Algorithm Self-Test	GCM encrypt KAT / 256-bit key	Enters FIPS Self-Test Error State

[25] The algorithm used for the Firmware Integrity Test (RSA) is conditionally tested before it is used in the execution of Firmware Integrity Test.
[26] The SAKs are used as the keys for pre-operational FW integrity test.

Function Tested	Self-Test Type	Implementation	Failure Behavior
AES-GCM (#A1080)	Cryptographic Algorithm Self-Test	GCM decrypt KAT / 256-bit key	Enters FIPS Self-Test Error State
AES-CMAC (#A1081)	Cryptographic Algorithm Self-Test	CMAC KAT / 256-bit key	Enters FIPS Self-Test Error State
SHA2-384 (#A1088)	Cryptographic Algorithm Self-Test	Digest KAT	Enters FIPS Self-Test Error State
HMAC-SHA2-256 (#A1083)	Cryptographic Algorithm Self-Test	HMAC SHA-256 KAT / 256-bit key	Enters FIPS Self-Test Error State
KAS-FFC-SSC Sp800-56Ar3 (#A1084)	Cryptographic Algorithm Self-Test	Diffie-Hellman Primitive Z KAT / 2048-bit key	Enters FIPS Self-Test Error State
AES-KW (#A1094)	Cryptographic Algorithm Self-Test	KW encrypt KAT / 256-bit key	Enters FIPS Self-Test Error State
AES-KW (#A1094)	Cryptographic Algorithm Self-Test	KW decrypt KAT / 256-bit key	Enters FIPS Self-Test Error State
KDF TLS (#A1089)	Cryptographic Algorithm Self-Test	KAT / 384-bit key	Enters FIPS Self-Test Error State
PBKDF (#A1085)	Cryptographic Algorithm Self-Test	KAT / 256-bit key	Enters FIPS Self-Test Error State
Firmware Loading	Firmware Load Test	RSA PKCS#1 3072 / SHA-256 signature verification of new FW image performed before FW can be loaded (#A1093 and #A1092)	Incoming FW package is not loaded and is discarded
ENT	Critical Functions Test: When a seed for DRBG is requested	Repetition Count and Adaptive Proportion tests as per SP 800-90B	Enters FIPS Self-Test Error State
Safe Primes Key Generation (#A1087)	Critical Functions Test: When a key is generated	Assurances as per sections 5.5 and 5.6 of SP 800-56A rev3	Keys are discarded

Table 10-2: Conditional Self-Tests

11 Life-Cycle Assurance

11.1 Delivery and Operation

To initialize the CM into the Compliant state, one of the following procedures must be followed: TCG Enterprise or ATA Security. Upon receiving the CM, the authorized operator must inspect the physical security mechanisms for tamper evidence and verify that the drive boots up in an uninitialized Security Mode.

The “FIPS Operating Mode” Indicator designates whether the drive has been configured to operate in the Compliant state. The “FIPS Operating Mode” Indicator is a bit (byte 30, bit 0) in the Vendor Unique fields in Level 0 Device Discovery. If byte 30, bit 0 of the Vendor Unique fields is set to one (1), then the device is operating in a Compliant state. If the bit is set to zero (0), then the device is operating in a Non-Compliant state and is not considered a FIPS 140 validated CM.

11.1.1 TCG Enterprise Secure Initialization

1. Upon 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 initialization and periodically thereafter, examine the physical security mechanisms for tamper evidence.
3. At initialization, set all enabled operator PINs applicable for the Compliant state to private values of at least 8 bytes (64 bits) in length: Drive Owner, EraseMaster, and BandMasters[27].
4. Set ReadLockEnabled and WriteLockEnabled to “True” and the LockOnReset column to include “Power Cycle”, on at least one (1) User Data range.
5. At initialization, disable the “Makers” authority.
6. At initialization, the value of LockOnReset for FW Download port must be set to include “Power Cycle”.

11.1.2 TCG Enterprise Ongoing Policy Restrictions

1. The ReadLockEnabled and WriteLockEnabled values must be set to “True” and the LockOnReset value must include “Power Cycle”, for at least one (1) User Data range.
2. The “Makers” Authority must be disabled.
3. The LockOnReset value for the FW Download port must include “Power Cycle”.

11.1.3 ATA Security Secure Initialization

1. Upon 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 initialization and periodically thereafter, examine the physical security mechanisms for tamper evidence.
3. Transition the CM to ATA Security Mode by setting the User Password to a private value of 32 bytes (256 bits) in length.
4. At initialization, set the remaining operator Passwords/PINs applicable for the Compliant state to private values of at least 8 bytes (64 bits) in length: Master and Drive Owner (optional).
5. At initialization, the value of LockOnReset for FW Download port must be set to “Power Cycle”.

11.1.4 ATA Security Ongoing policy Restrictions

1. The “Makers” Authority must be disabled.
2. The LockOnReset value for the FW Download port must include “Power Cycle”.

[27] A subset of the operator authority/PINs are enabled by default. If use of any other authority/PINs not enabled by default is required in the Compliant state, the Crypto Officer will need to enable them as part of the initialization steps.

11.2 End of Life

When the CM reaches end-of-life, the Crypto Officer must zeroize all SSPs prior to discarding the CM. The Crypto Officer shall perform the following steps when the CM is at end-of-life:

1. The Crypto Officer shall revert the CM to the factory default state by invoking the Revert or RevertSP methods[28] on the Admin SP.
2. If step 1 fails, all SSPs on the device may not have been sanitized. If this occurs, the Crypto Officer should handle the CM per organizational policies.

[28] The Revert/RevertSP methods will cause the CM to zeroize all the SSPs and exit the Compliant state.

12 Mitigation of Other Attacks

The CM does not make claims to mitigate against other attacks beyond the scope of FIPS 140-3.