Seagate Technology LLC

Seagate SSG3 TCG Enterprise SSC SED FIPS 140 Module

FIPS 140-3 Non-Proprietary Security Policy

Table of Contents

List of Tables

List of Figures

1 General

1.1 Overview

This document is the security policy as defined by [ISO/IEC 19790:2012(E)] Annex B and [SP 800-140B Rev. 1] for the Seagate SSG3 TCG Enterprise SSC SED FIPS 140 Module, hereafter denoted as the "CM".

1.2 Security Levels

The overall FIPS Security Level of the CM is level 2. The Security Levels of the CM for each individual FIPS 140-3 area are described in the following table.

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
	Overall Level	2

Table 1: Security Levels

2 Cryptographic Module Specification

2.1 Description

Purpose and Use: The primary function of the CM is to provide encryption, access control, and cryptographic erase of the User Data stored on the CM. The CM provides a wide range of cryptographic services using approved algorithms. The CM services include:

- Hardware based User Data encryption
- Instantaneous User Data sanitization with cryptographic erase
- Independently controlled and protected User Data band/ranges
- Authenticated FW download
- FW download protection

Module Name: Seagate SSG3 TCG Enterprise SSC SED FIPS 140 Module[1]

Module Type: Hardware

Module Embodiment: Multi-Chip Embedded

Cryptographic Boundary: The cryptographic boundary of the CM is the enclosure that surrounds the CM as described in section 7. A photo of the CM is provided in Figure 1 and a HW block diagram is provided in Figure 2.

Figure 1: CM Photo

[1] This is the value returned in the COMPLIANCE DESCRIPTOR MODULE NAME field of the FIPS 140 compliance descriptor (see [SFSC]).

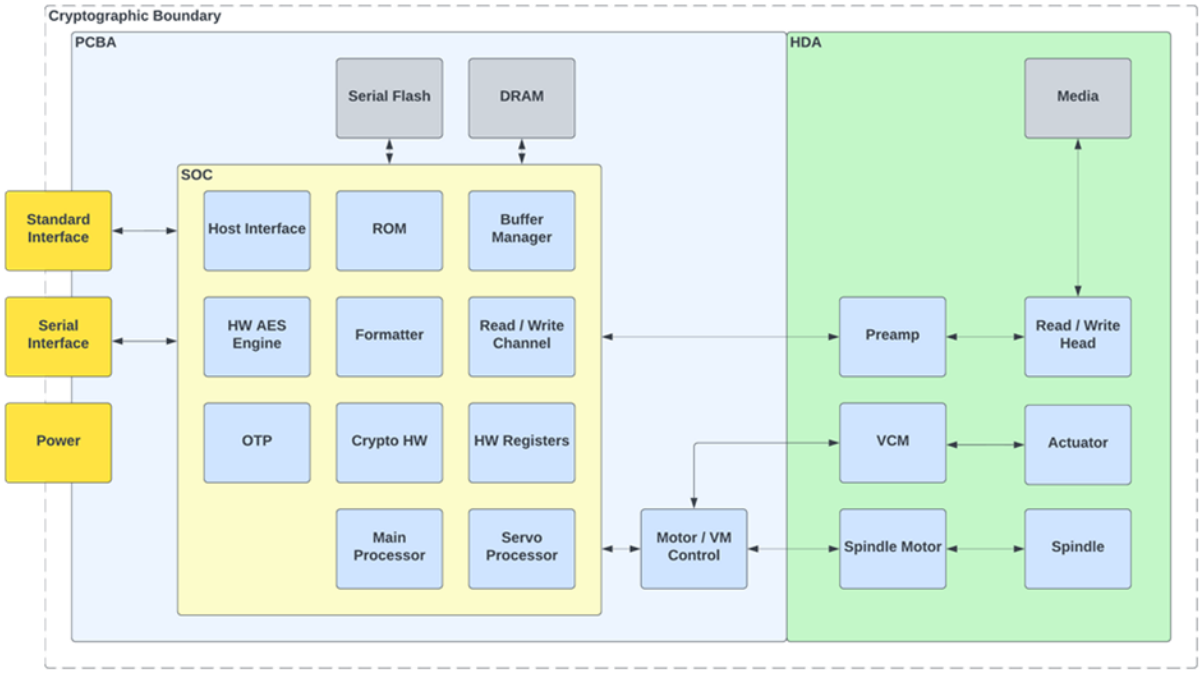

Figure 2: HW Block Diagram

2.2 Tested and Vendor Affirmed Module Version and Identification

2.2.1 Tested Module Identification – Hardware:

This security policy applies to the cryptographic modules (CMs) described in the following tables.

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
ST1200MM0069	Mynaplus ASIC v2.0	NF0A, SSCB, SE0G, HPD0, FLC0, NF3A, CN09	Mynaplus ASIC, ARM Cortex R5 on Mynaplus ASIC	Exos TCG Enterprise SSC SED SAS 10K RPM
ST1200MM0149	Mynaplus ASIC v2.0	CF0A	Mynaplus ASIC, ARM Cortex R5 on Mynaplus ASIC	Exos TCG Enterprise SSC SED SAS 10K RPM
ST1800MM0149	Mynaplus ASIC v2.0	CF0A, NA00, CK09	Mynaplus ASIC, ARM Cortex R5 on Mynaplus ASIC	Exos TCG Enterprise SSC SED SAS 10K RPM
ST2400MM0149	Mynaplus ASIC v2.0	CF0A, SSEK, SBTB, HPD0, CF3A, L2E0, L2F0, CK09	Mynaplus ASIC, ARM Cortex R5 on Mynaplus ASIC	Exos TCG Enterprise SSC SED SAS 10K RPM
ST600MM0239	Mynaplus ASIC v2.0	SE0G	Mynaplus ASIC, ARM Cortex R5 on Mynaplus ASIC	Exos TCG Enterprise SSC SED SAS 10K RPM

Table 2: Tested Module Identification – Hardware

Depending on the firmware version and configuration, the module can output a different show version. The table below shows the possible additional “show version” outputs based on part number and firmware combinations. Combinations not shown below will display the default part number.

Model and/or Part Number	Firmware Version	Show Version Output
ST1800MM0149	NA00	X427_SSKB31T8A10
ST2400MM0149	L2E0,L2F0	ST2400MM0149
ST1200MM0069	SSCB	DL1200MM0069
ST2400MM0149	SSEK	DL2400MM0149
ST2400MM0149	SBTB	DL2400MM0149
ST1200MM0069	SB0G	STSBSN35CLAR1200
ST600MM0239,	SB0G	STSBSN33CLAR600
ST2400MM0149	HPD0	EG002400MZKBD
ST1200MM0069	HPD0	EG001200MZKAU
ST2400MM0149	CF3A	ST2400MM3149
ST1200MM0069	NF3A	ST1200MM3069
ST1800MM0149	FLC0	ST1800MMZ149
ST2400MM0149	CK09	ST2400MMZ149
ST1200MM0069	CN09	ST1200MMZ069

Table 3: HW Substitute Configurations

2.2.2 Tested Module Identification – Software, Firmware, Hybrid (Executable Code Sets):

N/A for this module.

2.2.3 Tested Module Identification – Hybrid Disjoint Hardware:

N/A for this module.

2.2.4 Tested Operational Environments - Software, Firmware, Hybrid:

N/A for this module.

2.2.5 Vendor-Affirmed Operational Environments - Software, Firmware, Hybrid:

N/A for this module.

2.3 Excluded Components

The CM does not have any excluded physical components.

2.4 Modes of Operation

The CM supports both an approved mode of operation (named the TCG Security Mode) and a non-approved mode of operation. Transitioning between the modes occurs based on how the CM is configured. To put the device in the approved mode of operation the user must set ReadLockEnabled and WriteLockEnabled to “True” and the LockOnReset column to include “Power Cycle”, on at least one (1) User Data range. If these configurations are not set to these values then the module is in the Non-Approved mode of operation for a given range.

Modes List and Description:

Mode Name	Description	Type	Status Indicator
TCG Security Mode	The CM is utilizing TCG Security as the method for managing access control and the secure initialization steps have been performed.	Approved	FIPS Operating Mode Indicator has a value of one (1) and the User Data Range columns are configured as follows: ReadLockEnabled is "True", WriteLockEnabled is "True", and LockOnReset contains "Power Cycle"
Non-Approved Mode	The CM/User Data Range is operating in a Non-approved mode	Non-Approved	FIPS Operating Mode Indicator has a value of one (1) and at least one of the User Data Range columns is configured as follows: ReadLockEnabled is "False", WriteLockEnabled is "False", and LockOnReset does not contain "Power Cycle"

Table 4: Modes List and Description

Note: The FIPS Operating Mode Indicator is a bit 0 of byte 20 in the Vendor Unique fields in Level 0 Device Discovery.

2.5 Algorithms

The algorithms used by the CM are described in this section.

2.5.1 Approved Algorithms:

Algorithm	CAVP Cert	Properties	Reference
AES-CBC	A7701	Direction - Decrypt, Encrypt Key Length - 128, 256	SP 800-38A
AES-CBC	A7704	Direction - Decrypt, Encrypt Key Length - 128, 256	SP 800-38A
AES-CMAC	A7701	Direction - Generation Key Length - 128 MAC Length - MAC Length: 8-128 Increment	SP 800-38B

Algorithm	CAVP Cert	Properties	Reference
		8 Message Length - Message Length: 128-768 Increment 128	
AES-GCM	A7701	Direction - Decrypt, Encrypt IV Generation - Internal IV Generation Mode - 8.2.2 Key Length - 128, 256 Tag Length - 128 IV Length - IV Length: 96 Payload Length - Payload Length: 0-2048 Increment 256 AAD Length - AAD Length: 0-256 Increment 8	SP 800-38D
AES-GCM	A7702	Direction - Decrypt, Encrypt IV Generation - Internal IV Generation Mode - 8.2.2 Key Length - 128, 256 Tag Length - 128 IV Length - IV Length: 96 Payload Length - Payload Length: 0-2048 Increment 256 AAD Length - AAD Length: 0-256 Increment 8	SP 800-38D
AES-KW	A7701	Direction - Decrypt, Encrypt Cipher - Cipher Key Length - 256 Payload Length - Payload Length: 128, 192, 256, 320, 4096	SP 800-38F
AES-XTS Testing Revision 2.0	A7704	Direction - Decrypt, Encrypt Key Length - 128, 256 Payload Length - Payload Length: 4096, 4160, 4192, 4224, 33792 Tweak Mode - Number Data Unit Length Matches Payload Length - Yes	SP 800-38E
Hash DRBG	A7701	Prediction Resistance - No, Yes Supports Reseed - Yes Mode - SHA2-256 Entropy Input - Entropy Input: 256 Nonce - Nonce: 128 Personalization String Length - Personalization String Length: 0, 256 Additional Input - Additional Input: 0, 256 Returned Bits - 256	SP 800-90A Rev. 1
HMAC-SHA2-256	A7701	MAC - MAC: 256 Key Length - Key Length: 8-512 Increment 8	FIPS 198-1
HMAC-SHA2-256	A7705	MAC - MAC: 256 Key Length - Key Length: 128, 256, 520	FIPS 198-1
HMAC-SHA2-384	A7701	MAC - MAC: 384 Key Length - Key Length: 8-1024 Increment 8	FIPS 198-1
KAS-FFC-SSC Sp800-56Ar3	A7701	Domain Parameter Generation Methods - ffdhe2048 Hash Function Z - SHA2-512 Scheme -	SP 800-56A Rev. 3

Algorithm	CAVP Cert	Properties	Reference
		dhEphem - KAS Role - responder	
PBKDF	A7701	Iteration Count - Iteration Count: 21000 HMAC Algorithm - SHA2-256 Password Length - Password Length: 16, 32, 65 Salt Length - Salt Length: 128-512 Increment 8 Key Data Length - Key Data Length: 128-256 Increment 8	SP 800-132
RSA SigVer (FIPS186-5)	A7703	Hash Pair - Hash Algorithm - SHA2-256 Salt Length - 0 Modulo - 2048 Signature Type - pkcs1v1.5 Public Exponent Mode - random	FIPS 186-5
RSA SigVer (FIPS186-5)	A7705	Hash Pair - Hash Algorithm - SHA2-256 Modulo - 2048 Signature Type - pkcs1v1.5 Public Exponent Mode - random	FIPS 186-5
Safe Primes Key Generation	A7701	Safe Prime Groups - ffdhe2048	SP 800-56A Rev. 3
SHA2-256	A7701	Message Length - Message Length: 0-65528 Increment 8	FIPS 180-4
SHA2-256	A7703	Message Length - Message Length: 0-65528 Increment 8	FIPS 180-4
SHA2-256	A7705	Message Length - Message Length: 0-65528 Increment 8	FIPS 180-4
SHA2-384	A7701	Message Length - Message Length: 0-65528 Increment 8	FIPS 180-4
TLS v1.2 KDF RFC7627 (CVL)	A7701	Hash Algorithm - SHA2-256, SHA2-384 Key Block Length - Key Block Length: 1024	SP 800-135 Rev. 1

Table 5: Approved Algorithms

Note: Only the algorithms specified in the table above are approved algorithms supported by the module in approved mode of operation.

2.5.2 Vendor-Affirmed Algorithms:

Name	Properties	Implementation	Reference
FW-R5 CKG 1	Key Type:Symmetric and Asymmetric	FW-R5	SP 800-133r2, Section 4, example 1
FW-R5 CKG 2	Key Type:Symmetric	FW-R5	SP 800-133r2, Section 6.3, method 1

Table 6: Vendor-Affirmed Algorithms

2.5.3 Non-Approved, Allowed Algorithms

N/A for this module.

2.5.4 Non-Approved, Allowed Algorithms with No Security Claimed

Name	Caveat	Use and Function
AES-GCM (no security claimed)	IG 2.4.A Scenario 1	Obfuscation
SHA2-512 (no security claimed)	IG 2.4.A Scenario 2	Memory integrity check, no claim of security.

Table 7: Non-Approved, Allowed Algorithms with No Security Claimed

2.5.5 Non-Approved, Not Allowed Algorithms:

Name	Use and Function
FW-R5 AES-GCM (non-compliant)	Key wrapping (encryption / decryption)
FW-R5 PBKDF (non-compliant)	Key Derivation
HW-FDE AES-XTS (non-compliant)	Encryption / decryption
HW-SECA SHA-256 (non-compliant)	Pseudo random function for FW-R5 PBKDF (non-complaint)

Table 8: Non-Approved, Not Allowed Algorithms

2.6 Security Function Implementations

The Security Functions Implementations supported on the CM are described in the following table.

Name	Type	Description	Properties	Algorithms
AES-GCM (No Security Claimed)	BC-Auth	Obfuscates data	Caveat:No Security Claimed	AES-GCM (no security claimed): ()
Encrypt/Decrypt TLS Message	BC-Auth	Send/Receive encrypted TLS message		AES-CBC: (A7701) AES-GCM: (A7701) HMAC-SHA2-256: (A7701) HMAC-SHA2-384: (A7701) SHA2-256: (A7701) SHA2-384: (A7701)
Encrypt/Decrypt User Data	BC-UnAuth	Encrypt or decrypt User data		AES-XTS Testing Revision 2.0: (A7704) AES-CBC: (A7704)
Generate Key	DRBG	Generate key		Hash DRBG: (A7701) AES-CMAC: (A7701) Safe Primes Key Generation: (A7701) FW-R5 CKG 1: () Key Type: Symmetric and

Name	Type	Description	Properties	Algorithms
				Asymmetric FW-R5 CKG 2: () Key Type: Symmetric
Generate Random Number	DRBG	Generate random number		Hash DRBG: (A7701) AES-CMAC: (A7701)
Key Derivation	PBKDF	Key Derivation using host provided PIN/Password		PBKDF: (A7701) HMAC-SHA2-256: (A7705) SHA2-256: (A7705)
Key Wrap 1	BC-Auth	Key wrap using AES-GCM, for storage only		AES-GCM: (A7701)
Key Wrap 2	BC-Auth	Key wrap using AES-KW, for storage only		AES-KW: (A7701)
KTS CBC/HMAC	KTS-Unwrap	Receive encrypted SSP's over TLS using CBC-based ciphers	Caveat:Key establishment methodology provides 128 or 256 bits of security strength Standard:SP 800-38F IG D.G:Approved	AES-CBC: (A7701) HMAC-SHA2-256: (A7701) HMAC-SHA2-384: (A7701) SHA2-256: (A7701) SHA2-384: (A7701)
KTS GCM	KTS-Unwrap	Receive encrypted SSP's over TLS using GCM-based ciphers	Caveat:: Key establishment methodology provides 128 or 256 bits of security strength Standard:SP 800-38F IG D.G:Approved	AES-GCM: (A7702) AES-CBC: (A7701)
SHA2-512 (no security claimed)	SHA	Obfuscates data	Caveat:No security claimed	SHA2-512 (no security claimed): ()
Start TLS Session	KAS-135KDF KAS-SSC KAS-SSC/KDF	Key agreement for TLS session keys	Caveat:Key establishment SSP establishment methodology provides 112 bits of encryption strength IG:IG DF Scenario 2 Path 2 Key Confirmation:No :IG 2.4.B SP 800-	TLS v1.2 KDF RFC7627: (A7701) KAS-FFC-SSC Sp800-56Ar3: (A7701) HMAC-SHA2-256: (A7701) HMAC-SHA2-384: (A7701) SHA2-256: (A7701)

Name	Type	Description	Properties	Algorithms
			135rev1 CVL Key Derivation:SP 800-135rev1 CVL	SHA2-384: (A7701)
Verify FW Digital Signature	DigSig-SigVer	Verifies integrity and authenticity of signed data		RSA SigVer (FIPS186-5): (A7705, A7701, A7703) SHA2-256: (A7705, A7701, A7703)

Table 9: Security Function Implementations

2.7 Algorithm Specific Information

2.7.1 AES-GCM

The method the CM uses to generate IV values for the AES-GCM algorithm is different depending on which Security Function Implementation (see section 2.6) is using the algorithm.

The AES-GCM IV values for the Key Wrap 1 Security Function Implementation are 96 bits in length and are generated internally using the CM RNG (see section 2.8). This complies with scenario 2 in section C.H. of [FIPS 140-3 IG].

The AES-GCM IV values for the Send/Receive TLS Message Security Function Implementation are generated as described in [RFC 5116] and [RFC 5487]. The IV values are 160 bits in length. For each TLS session the first 96 bits are generated internally using the CM RNG (see section 2.8) and the last 64 bits are a counter value that increments with each message. If the counter value exceeds the maximum value of 2^{64}, the CM will return a TLS Alert indicating that the TLS session needs to be renegotiated. This complies with scenario 1 in section C.H. of [FIPS 140-3 IG].

2.7.2 AES-XTS

The CM checks to ensure Key 1 does not equal Key 2 before using the keys in the XTS-AES algorithm. This check occurs within the module boundary.

2.7.3 PBKDF

The CM supports symmetric key derivation from a password by using the PBKDF2 algorithm with option 2a as described in section D.N of [FIPS 140-3 IG] and [SP 800-132] with a 1000 iteration count, a 128-bit Salt, and HMAC-SHA2-256 as the Pseudo Random Function (PRF) while in the approved mode of operation.

The password includes any value from a minimum of 64 bits to a maximum of 256 bits. This leads to the chance of correctly guessing the minimum length PIN being 1 / (2^{64}).

Keys derived from passwords, as shown in SP800-132, may only be used in storage applications.

2.8 RBG and Entropy

The RBG and entropy used by the CM is described in this section. The RBG and entropy used by the CM follows the recommendations as described in [SP 800-90A Rev. 1] and [SP 800-90B].

2.8.1 Entropy Information

An entropy source (see Figure 3) is composed of a few major sections, which map to the conceptual components contained within an [SP 800-90B] entropy source. An entropy source contains the following:

- A noise source
- Health tests
- A conditioning algorithm

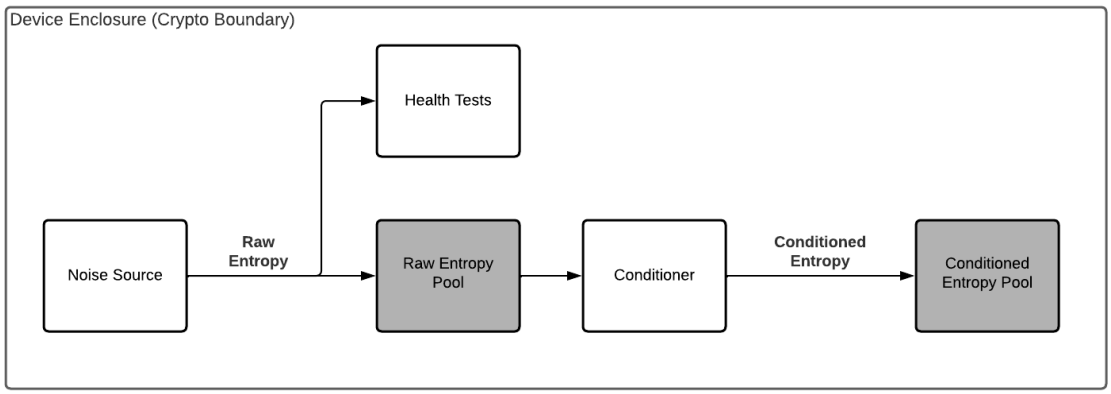

Figure 3: Entropy Source Overview Diagram

A noise source generates samples when required by the CM. The raw samples from the noise source are stored in an entropy pool. When there are enough samples in the pool to meet the desired min-entropy of 256 bits, the entropy in the pool is conditioned. The noise source always generates new samples during each CM reset and the samples are never stored for use after a CM reset. Additionally, each sample from the noise source is subject to health tests as described in section 10. The output of an entropy source is not available until all the health tests have passed.

The noise source used by the CM is the Ring Oscillator noise source, which uses the thermal noise induced jitter of CMOS inverters as the source of randomness. The ESV certificate for the noise source is provided in the following table.

Cert Number	Vendor Name
E319	Seagate Technology

Table 10: Entropy Certificates

The noise source parameters are provided in the following table.

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
Seagate SSG3 SED Entropy Source	Physical	MynaPlus ASIC Rev 2.0	128 bits	128 bits	CMAC-AES-128 (#A7701)

Table 11: Entropy Sources

2.8.2 RNG Information

The DRBG used in the CM is the Hash DRBG (A7701).

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 padded with zeroes to 256 bits)

The output of the RNG is not available until the DRBG has been seeded.

The DRBG is fully seeded to its 256-bit security strength.

2.9 Key Generation

All key generation performed by the CM is in accordance with [SP 800-133 Rev. 2] and uses the CM RNG as described in 2.8 as the source of random bits.

When the CM generates FFC key pairs (i.e., dhEphem), the CM uses the Extra Random Bits method as defined in [SP 800-56A Rev. 3].

When the CM generates the TLS session keys (i.e., the TLS Client Write Encryption Key and the TLS Server Write Encryption Key) for one of the AES-GCM cipher suites, the CM will compare the two keys and if they are equal, the CM will abort the TLS session. This complies with TLS/DTLS 1.2 protocol IV generation in section C.H. of [FIPS 140-3 IG].

2.10 Key Establishment

All key establishment using FFC key pairs (i.e., dhEphem) performed by the CM is in accordance with [SP 800-56A Rev. 3] and utilizes the KAS-FFC-SSC and TLS v1.2 KDF [RFC 7627] approved algorithms. When the CM establishes keys using dhEphem, the CM performs the FFC Full Public-Key Validation Routine as described in [SP 800-56A Rev. 3] on the key received from the host. This complies with scenario 2 path 2 of section D.F. of [FIPS 140-3 IG].

2.11 Industry Protocols

The host communicates with the CM via the following protocols:

- The SAS protocol as described in [SBC] and [SPC]
- The TCG protocol as described in [TCG Core Spec v1], [TCG Ent SSC], and [TCG PSK Ent]

The CM supports TLS v1.2 via TCG commands as described in [TCG PSK Ent].

The following TLS cipher suites are supported:

- 0x00AB TLS_DHE_PSK_WITH_AES_256_GCM_SHA384
- 0x00AA TLS_DHE_PSK_WITH_AES_128_GCM_SHA256
- 0x00B3 TLS_DHE_PSK_WITH_AES_256_CBC_SHA384
- 0x00B2 TLS_DHE_PSK_WITH_AES_128_CBC_SHA256
- 0x00A9 TLS_PSK_WITH_AES_256_GCM_SHA384
- 0x00A8 TLS_PSK_WITH_AES_128_GCM_SHA256
- 0x00AF TLS_PSK_WITH_AES_256_CBC_SHA384
- 0x00AE TLS_PSK_WITH_AES_128_CBC_SHA256

For all random values needed for key establishment, the CM generates those values using the RNG as described in 2.8.

No parts of the TLS protocol, other than the approved cryptographic algorithms and the KDF, have been tested by the CAVP and CMVP.

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

The CM physical port to FIPS 140 logical interface mapping is described in the following table.

Physical Port	Logical Interface(s)	Data That Passes
SAS Connector	Data Input Data Output Control Input Status Output	TCG Packets SCSI Packets
Power Connector	Power	N/A
Serial Interface Connector (Disabled)	None	N/A

Table 12: Ports and Interfaces

4 Roles, Services, and Authentication

4.1 Authentication Methods

The authentication methods used by the CM are described in the following table.

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
TCG PIN Authentication	Authentication for CM roles. Minimum PIN length is 8 bytes (64 bits)	Key Derivation	Strength: 1/(2^64)	800/(2^64)

Table 13: Authentication Methods

4.2 Roles

The following roles/credentials are supported by the CM:

- Drive Owner (FIPS Crypto Officer) – The Drive Owner role (also known as SID) provides access control for the ability to lock/unlock the FW Download port.
- EraseMaster (FIPS Crypto Officer) – The EraseMaster role provides access control for the ability to cryptographically erase LBA bands/ranges and enable/disable BandMasters.
- BandMaster (FIPS Crypto Officer) – The Band Master roles (0 – 31) provide access control for the ability to carry out read and write operations. Each BandMaster can lock/unlock one LBA band/range.

Note: All roles can also establish the TLS PSKs and start TLS sessions.

The mapping of the roles to the FIPS 140-3 operator type and authentication methods is provided in following table.

Name	Type	Operator Type	Authentication Methods
Drive Owner (SID)	Role	Crypto Officer	TCG PIN Authentication
EraseMaster	Role	Crypto Officer	TCG PIN Authentication
BandMasters	Role	Crypto Officer	TCG PIN Authentication

Table 14: Roles

4.3 Approved Services

The Approved services are provided by the CM are described in the following table.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Authenticate	Authenticate the operator	TCG Status	TCG Authenticate Method, TCG Start Session Method	None	Key Derivation Key Wrap 1	BandMasters - BandMaster PINs: W,E - KW AES-GCM IV: E - Master Keys: G,E,Z Drive Owner (SID) - Drive Owner (SID) PIN: W,E - KW AES-GCM IV: E - Master Keys: G,E,Z EraseMaster - EraseMaster PIN: W,E - KW AES-GCM IV: E - Master Keys: G,E,Z
Cryptographic Erase	Erase User Data in LBA range cryptographically by changing the MEK and place the range in the uninitialized state.	TCG Status	TCG Erase Method	None	None	EraseMaster - BandMaster PINs: Z - MEKEKs: Z - MEKs: Z
Exit FIPS Mode / Return to Factory State	Exit the approved mode of operation and return the CM to the factory state	TCG Status	TCG RevertSP Method	None	Generate Random Number Generate Key	Unauthenticated - BandMaster PINs: Z - BandMaster PSKs: Z - DRBG C: G,E,Z - DRBG Entropy

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Input String : G,E,Z - DRBG Seed: G,E,Z - DRBG V: G,E,Z - Drive Owner (SID) PIN: Z - Drive Owner PSK: Z - EraseMaster PIN: Z - EraseMaster PSK: Z - MEKEKs: Z - MEKs: Z
FW Download	New FW is downloaded to device and replaces existing FW	Interface status	Interface FW Download Command	None	Verify FW Digital Signature	Drive Owner (SID) - FW Signing Key: E
Generate Random Bytes	Generate random data for host use	TCG Status	TCG Random Method	Random bytes	Generate Random Number	Unauthenticated - DRBG C: G,E,Z - DRBG Entropy Input String : G,E,Z - DRBG Seed: G,E,Z - DRBG V: G,E,Z
Reset Module	Restart the module. This will run the pre-operational and power-on conditional self-tests.	N/A	Power-on reset	None	Verify FW Digital Signature	Unauthenticated - DRBG C: Z - DRBG Entropy Input String : Z - DRBG Seed: Z - DRBG V: Z - Drive Owner (SID) PIN: Z - Platform Keys: E - Signing Authority Keys: E - TLS Client DHE Public Key: Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- TLS Client Write Encryption Key: Z - TLS Client Write MAC Key: Z - TLS Master Secret: Z - TLS Other Secret: Z - TLS Premaster Secret: Z - TLS Server DHE Private Key: Z - TLS Server DHE Public Key: Z - TLS Server Write Encryption Key: Z - TLS Server Write MAC Key: Z
Set Enable/Disable BandMasters	Enable/disable BandMaster authority	TCG Status	TCG Set Method	None	None	EraseMaster
Set PIN / Password	Change operator authentication data	TCG Status	TCG Set Method	None	Generate Random Number Key Derivation Key Wrap 1	BandMasters - BandMaster PINs: G,W,E,Z - DRBG C: G,E,Z - DRBG Entropy Input String : G,E,Z - DRBG Seed: G,E,Z - DRBG V: G,E,Z - KW AES-GCM IV: G,E Drive Owner (SID) - DRBG C: G,E,Z - DRBG Entropy Input String : G,E,Z - DRBG Seed:

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						G,E,Z - DRBG V: G,E,Z - Drive Owner (SID) PIN: G,W,E,Z - KW AES-GCM IV: G,E EraseMaster - DRBG C: G,E,Z - DRBG Entropy Input String : G,E,Z - DRBG Seed: G,E,Z - DRBG V: G,E,Z - EraseMaster PIN: G,W,E,Z - KW AES-GCM IV: G,E
Set Range Attributes	Set location, size, and locking attributes of an LBA range	TCG Status	TCG Status	None	None	BandMasters
Set TLS PSK	Set pre-shared key used for TLS	TCG Status	TCG Set Method	None	AES-GCM (No Security Claimed) Generate Random Number	BandMasters - BandMaster PSKs: W,Z - DRBG C: G,E,Z - DRBG Entropy Input String : G,E,Z - DRBG Seed: G,E,Z - DRBG V: G,E,Z Drive Owner (SID) - DRBG C: G,E,Z - DRBG Entropy Input String : G,E,Z - DRBG Seed: G,E,Z - DRBG V: G,E,Z - Drive Owner

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						PSK: W,Z EraseMaster - DRBG C: G,E,Z - DRBG Entropy Input String : G,E,Z - DRBG Seed: G,E,Z - DRBG V: G,E,Z - EraseMaster PSK: W,Z
Show Status	Show status of module state, including the value of the FIPS Operating Mode Indicator	TCG Status	TCG Level 0 Discovery, TCG Get Method	Current CM Status Value	None	Unauthenticated
Show Version	Show version of module state	TCG Status	Interface INQUIRY command	Current CM Status Value	None	Unauthenticated
TLS Close Session	Close open TLS session	TCG Status	TCG Close Session	None	None	Unauthenticated - TLS AES-GCM IV: Z - TLS Client DHE Public Key: Z - TLS Client Write Encryption Key: Z - TLS Client Write MAC Key: Z - TLS Master Secret: Z - TLS Other Secret: Z - TLS Premaster Secret: Z - TLS Server DHE Private Key: Z - TLS Server DHE Public Key: Z - TLS Server Write Encryption Key: Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- TLS Server Write MAC Key: Z
TLS Receive Message	CM receives TLS message from host	TCG Status	Interface IF-Send Command	None	Generate Random Number KTS CBC/HMAC KTS GCM Encrypt/Decrypt TLS Message	BandMasters - DRBG C: G,E,Z - DRBG Entropy Input String : G,E,Z - DRBG Seed: G,E,Z - DRBG V: G,E,Z - TLS AES-GCM IV: G,E - TLS Client Write Encryption Key: E - TLS Client Write MAC Key: E Drive Owner (SID) - DRBG C: G,E,Z - DRBG Entropy Input String : G,E,Z - DRBG Seed: G,E,Z - DRBG V: G,E,Z - TLS AES-GCM IV: G,E - TLS Client Write Encryption Key: E - TLS Client Write MAC Key: E EraseMaster - DRBG C: G,E,Z - DRBG Entropy Input String : G,E,Z - DRBG Seed: G,E,Z - DRBG V: G,E,Z - TLS Client Write Encryption Key: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- TLS Client Write MAC Key: E
TLS Send Message	CM sends TLS message to host	TCG Status	Interface IF-Receive Command	Encrypted TLS message	Encrypt/Decrypt TLS Message Generate Random Number	BandMasters - DRBG C: G,E,Z - DRBG Entropy Input String : G,E,Z - DRBG Seed: G,E,Z - DRBG V: G,E,Z - TLS Client Write Encryption Key: E - TLS Client Write MAC Key: E Drive Owner (SID) - DRBG C: G,E,Z - DRBG Entropy Input String : G,E,Z - DRBG Seed: G,E,Z - DRBG V: G,E,Z - TLS Server Write Encryption Key: E - TLS Server Write MAC Key: E EraseMaster - DRBG C: G,E,Z - DRBG Entropy Input String : G,E,Z - DRBG Seed: G,E,Z - DRBG V: G,E,Z - TLS Client Write MAC Key: E - TLS Server Write Encryption Key: E
TLS Start Session	Start host-initiated TLS session	TCG Status	TCG StartTLS Method	None	AES-GCM (No Security Claimed)	BandMasters - BandMaster

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					Generate Key Start TLS Session	PSKs: E - TLS Client DHE Public Key: W,E - TLS Client Write Encryption Key: G - TLS Client Write MAC Key: G - TLS Master Secret: G,E - TLS Other Secret: G,E - TLS Premaster Secret: G,E - TLS Server DHE Private Key: G,E - TLS Server DHE Public Key: G,R - TLS Server Write Encryption Key: G - TLS Server Write MAC Key: G Drive Owner (SID) - BandMaster PSKs: E - TLS Client DHE Public Key: W,E - TLS Client Write Encryption Key: G - TLS Client Write MAC Key: G - TLS Master Secret: G,E - TLS Other Secret: G,E - TLS Premaster Secret: G,E - TLS Server DHE

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Private Key: G,E - TLS Server DHE Public Key: G,R - TLS Server Write Encryption Key: G - TLS Server Write MAC Key: G EraseMaster - BandMaster PSKs: E - TLS Client DHE Public Key: W,E - TLS Client Write Encryption Key: G - TLS Client Write MAC Key: G - TLS Master Secret: G,E - TLS Other Secret: G,E - TLS Premaster Secret: G,E - TLS Server DHE Private Key: G,E - TLS Server DHE Public Key: G,R - TLS Server Write Encryption Key: G - TLS Server Write MAC Key: G
User Data Lock/Unlock Range	Lock/Unlock read/decrypt or write/decrypt of User Data in an LBA range	TCG Status	TCG Set Method	None	Key Wrap 2	BandMasters - MEKEKs: E - MEKs: E
User Data Read / Write	Encrypt/write or decrypt/read User data from an LBA range	Interface Status	Interface Read/Write Command	Plaintext User Data	Encrypt/Decrypt User Data SHA2-512 (no security claimed)	BandMasters - MEKs: E

Table 15: Approved Services

Definitions for Roles SSP Access column values in the table above:

- 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

Note: The following services are identified as aligning with the “lock-based authentication model”:

- User Data Read/Write
- FW Download

The “lock-based authentication model” is described in IG 4.1.A of [FIPS 140-3 IG]. 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), 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.

4.4 Non-Approved Services

The Non-Approved services are provided by the CM are described in the following table. SSPs generated or derived in the approved mode cannot be used in the non-approved mode and vice versa.

Name	Description	Algorithms	Role
Cryptographic Erase	Generates new range key following sanitization of the non-volatile media.	FW-R5 AES-GCM (non-compliant) FW-R5 PBKDF (non-compliant) HW-SECA SHA-256 (non-compliant)	EraseMaster
User Data Read / Write (Locking Disabled)	Encrypt / decrypt user data from an LBA range where Locking is disabled	HW-FDE AES-XTS (non-compliant)	None

Table 16: Non-Approved Services

Note: 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).

4.5 External Software/Firmware Loaded

The CM firmware may be updated by an external source via the FW download operation. Prior to accepting new firmware provided by the FW download operation, the CM will verify the authenticity and integrity of the CM incoming firmware using FW-R5 HW-SECA RSASSA-PKCS1-v1.5 Signature Verification (A7705) with the following parameters:

- The key is the FW Signing Key
- The modulus size is 2048 bits
- The hash function is HW-SECA SHA2-256 (A7705)

Note: The FW Download port needs to be unlocked for the CM to accept new FW. The ports will re-lock on a power-cycle.

5 Software/Firmware Security

5.1 Integrity Techniques

During the power-on boot process or FW download process, the CM will verify the authenticity and integrity of the CM firmware using RSA SigVer (A7703) with the following parameters:

- The key is a Signing Authority Key.[2]
- The modulus size is 2048 bits
- The hash function is SHA2-256 (A7703)

The integrity of the following executable binary files is verified using the above method:

- Boot FW ITCM
- Boot FW IDBA
- Servo FW
- Disc FW

5.2 Initiate on Demand

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

6 Operational Environment

6.1 Operational Environment Type and Requirements

Type of Operational Environment: Limited

How Requirements are Satisfied: The CM operates in a limited operational environment where the CM firmware may be updated by an external source as described in section 5. Only firmware signed by the manufacturer private key will be accepted by the CM.

[2] Per section 7.5 of ISO 19790, the public verification key used for firmware integrity is not considered an SSP.

7 Physical Security

7.1 Mechanisms and Actions Required

The CM is made up of product grade components with standard passivation. The CM is surrounded by a metal enclosure that is opaque within the visible spectrum. To meet the level 2 physical security requirements, the CM employs factory installed tamper-evident labels (TELs) to prevent physical tampering. A photo of each of the TELs is provided in Figures 4-6. The physical inspection guidelines are provided in the following table.

Mechanism	Inspection Frequency	Inspection Guidance
Opaque, TEL on exposed (back) side of the PCBA Opaque, white, TEL on sides of the PCBA	The frequency of the physical inspection should be determined by the Crypto Officer. It is recommended that the TELs be inspected monthly.	Periodic inspection of TELs to detect evidence of tampering: checkerboard pattern on TEL, security label cutouts do not match original, and security label over PCBA screws is not penetrated Upon discovery of tamper evidence, the CM should be handled per organizational policies.

Table 17: Mechanisms and Actions Required

Figure 4: Tamper Evident Label

Figure 5: Tamper Evident Label

Figure 6: Tamper Evident Label

8 Non-Invasive Security

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

9 Sensitive Security Parameters Management

9.1 Storage Areas

The storage areas on the CM where SSPs may be present are described in the following table.

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

Table 18: Storage Areas

9.2 SSP Input-Output Methods

The SSP Input-Output methods supported by the CM are described in the following table.

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
Host Input	Entered	DRAM	Plaintext	Manual	Electronic	
Host Input TLS CBC/HMAC	Entered	DRAM	Encrypted	Manual	Electronic	KTS CBC/HMAC
Host Input TLS GCM	Entered	DRAM	Encrypted	Manual	Electronic	KTS GCM
Host Output	DRAM	Entered	Plaintext	Manual	Electronic	

Table 19: SSP Input-Output Methods

9.3 SSP Zeroization Methods

The methods used by the CM to zeroize SSP are described in the following table.

Zeroization Method	Description	Rationale	Operator Initiation
ZM1	Write volatile memory: Zeroize SSP by writing the memory where the SSP is stored with a pattern of all bytes set to 0x00.	The method ensures that the previous SSP value is entirely overwritten and is no longer stored in volatile memory.	Authenticate, Cryptographic Erase, Exit FIPS Mode / Return to Factory State, Reset Module, Set PIN / Password, Set TLS PSK, TCG Close Session, TLS Close Session, TLS Start Session
ZM2	Write non-volatile memory (unprotected SSPs): Zeroize unprotected (i.e., plaintext or obfuscated) SSPs stored in non-volatile memory by writing the memory where the SSP is stored with a pattern	The method ensures that the previous SSP value is entirely overwritten and is no longer stored in non-volatile memory. Additionally, the two overwrites mitigates the	Exit FIPS Mode / Return to Factory State, Set TLS PSK

Zeroization Method	Description	Rationale	Operator Initiation
	of all bytes set to 0x00 and then writing the new SSP value.	risk of any residual data in the non-volatile memory	
ZM3	Write non-volatile memory (protected SSPs): Zeroize protected (i.e., encrypted using another SSP) SSPs stored in non-volatile memory 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.	The method ensures that the previous SSP value is entirely overwritten and is no longer stored in volatile memory.	Cryptographic Erase, Exit FIPS Mode / Return to Factory State, Set PIN/Password

Table 20: SSP Zeroization Methods

Note: When the CM begins processing a zeroization method, the processing of the method cannot be interrupted. If the CM loses power while processing a zeroization method on non-volatile memory, the CM will resume processing the method when the CM is powered on again

9.4 SSPs

The SSPs supported by the CM are described in the following tables.

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
BandMaster PINs	PINs	64-256 bits - 64-256 bits	Authentication Credential - CSP			Key Derivation
BandMaster PSKs	Pre-Shared Keys	128-512 bits - 128-256 bits	Symmetric - CSP			Start TLS Session
DRBG C	Key for DRBG	256 bits - 440 bits	DRBG Parameter - CSP	Generate Random Number		Generate Random Number Generate Key Start TLS Session
DRBG Entropy Input String	Entropy input for DRBG	384 bits - 384 bits	DRBG Input - CSP	Entropy		Generate Random Number Generate Key Start TLS Session
DRBG Seed	Seed for DRBG	440 bits - 440 bits	DRBG Parameter - CSP	Entropy		Generate Random Number Generate Key Start TLS Session
DRBG V	V value for DRBG	128 bits - 440 bits	DRBG Parameter - CSP	Generate Random Number		Generate Random Number Generate Key Start TLS Session
Drive Owner (SID) PIN	PINs	64-256 bits - 64-256 bits	Authentication Credential - CSP			Key Derivation
Drive Owner PSK	Pre-Shared Keys	128-512 bits - 128-256 bits	Symmetric - CSP			Start TLS Session
EraseMaster PIN	PINs	64-256 bits - 64-256 bits	Authentication Credential - CSP			Key Derivation
EraseMaster PSK	Pre-Shared Keys	128-512 bits - 128-256 bits	Symmetric - CSP			Start TLS Session
FW Signing Key	Signing Key	2048 bits - 112 bits	Public - PSP	Preloaded		Verify FW Digital Signature

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
KW AES-GCM IV	AES-GCM IV used for key wrap	96 bits - 96 bits	Public - PSP	Generate Random Number		Key Wrap 1
Master Keys	Encrypts the MEKEK	256 bits - 256 bits	Symmetric - PSP	Key Derivation		Key Wrap 1
MEKEKs	Encrypts the MEK	256 bits - 256 bits	Symmetric - CSP	Generate Key		Key Wrap 2
MEKs	Media Encryption Key	256 bits - 256 bits	Symmetric - PSP	Generate Key		Encrypt/Decrypt User Data
Platform Keys	Signs the Firmware Integrity Key. Not an SSP.	2048 bits - 112 bits	Public - Neither	Preloaded		Verify FW Digital Signature
Signing Authority Keys	"Firmware Integrity Key. Not an SSP.	2048 bits - 112 bits	Public - Neither	Preloaded		Verify FW Digital Signature
TLS AES-GCM IV	AES-GCM IV used in TLS protocol	160 bits - 96 bits	Public - PSP	Start TLS Session		KTS GCM Encrypt/Decrypt TLS Message
TLS Client DHE Public Key	TLS Handshake Keys	2048 bits - 112 bits	Public - PSP			Start TLS Session
TLS Client Write Encryption Key	TLS Session Keys	128 or 256 bits - 128 or 256 bits	Symmetric - CSP	Start TLS Session		KTS CBC/HMAC KTS GCM Encrypt/Decrypt TLS Message
TLS Client Write MAC Key	TLS Session Keys	256 or 384 bits - 256 bits	Symmetric - CSP	Start TLS Session		KTS GCM Encrypt/Decrypt TLS Message
TLS Master Secret	TLS Session Keys	384 bits - 256 bits	Derivation - CSP	Start TLS Session		Start TLS Session
TLS Other Secret	TLS Other Secret. Used as part of the TLS Premaster Secret when TLS PSK cipher supports KAS FFC	256 bits - 256 bits	Symmetric - CSP		Start TLS Session	Start TLS Session
TLS Premaster Secret	TLS Handshake Keys	128-768 bits - 128-256 bits	Symmetric - CSP	Start TLS Session		Start TLS Session
TLS Server DHE Private Key	TLS Handshake Keys	2048 bits - 112 bits	Private - CSP	Start TLS Session		Start TLS Session
TLS Server DHE Public Key	TLS Handshake Keys	2048 bits - 112 bits	Public - PSP	Start TLS Session		

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
TLS Server Write Encryption Key	TLS Session Keys	128 or 256 bits - 128 or 256 bits	Symmetric - CSP	Start TLS Session		Encrypt/Decrypt TLS Message
TLS Server Write MAC Key	TLS Session Keys	256 or 384 bits - 256 bits	Symmetric - CSP	Start TLS Session		Encrypt/Decrypt TLS Message

Table 21: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
BandMaster PINs	Host Input Host Input TLS CBC/HMAC Host Input TLS GCM	DRAM:Plaintext Media:Obfuscated	Duration of session	ZM1 ZM3	Master Keys:Derives
BandMaster PSKs	Host Input Host Input TLS CBC/HMAC Host Input TLS GCM	DRAM:Plaintext Media:Obfuscated	Duration of session	ZM1 ZM2	TLS Premaster Secret:Derives
DRBG C		HW Registers:Plaintext	Duration of session	ZM1	DRBG Seed:Derived From
DRBG Entropy Input String		DRAM:Plaintext	Duration of session	ZM1	DRBG Seed:Derives
DRBG Seed		DRAM:Plaintext	Duration of session	ZM1	DRBG Entropy Input String :Derived From DRBG C:Derives DRBG V:Derives
DRBG V		HW Registers:Plaintext	Duration of session	ZM1	DRBG Seed:Derived From
Drive Owner (SID) PIN	Host Input Host Input TLS CBC/HMAC Host Input TLS GCM	DRAM:Plaintext Media:Obfuscated	Duration of session	ZM1 ZM2	Master Keys:Derives
Drive Owner PSK	Host Input Host Input TLS CBC/HMAC Host Input TLS GCM	DRAM:Plaintext Media:Obfuscated	Duration of session	ZM1 ZM3	TLS Premaster Secret:Derives

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
EraseMaster PIN	Host Input Host Input TLS CBC/HMAC Host Input TLS GCM	DRAM:Plaintext Media:Obfuscated	Duration of session	ZM1 ZM2	Master Keys:Derives
EraseMaster PSK	Host Input Host Input TLS CBC/HMAC Host Input TLS GCM	DRAM:Plaintext Media:Obfuscated	Duration of session	ZM1 ZM3	TLS Premaster Secret:Derives
FW Signing Key		ROM:Plaintext			
KW AES-GCM IV		DRAM:Plaintext Media:Plaintext	Duration of session		
Master Keys		DRAM:Plaintext	Duration of session	ZM1	Drive Owner (SID) PIN:Derived From BandMaster PINs:Derived From EraseMaster PIN:Derived From MEKEKs:Encrypts
MEKEKs		DRAM:Plaintext Media:Encrypted	Duration of session	ZM1 ZM3	Master Keys:Encrypted by MEKs:Encrypts
MEKs		HW Registers:Plaintext Media:Encrypted	Duration of session	ZM1 ZM3	MEKEKs:Encrypted by
Platform Keys		ROM:Plaintext			
Signing Authority Keys		DRAM:Plaintext Serial Flash:Plaintext	Duration of session		
TLS AES-GCM IV		DRAM:Plaintext	Duration of session		
TLS Client DHE Public Key	Host Input	DRAM:Plaintext	Duration of session	ZM1	TLS Other Secret:Derives
TLS Client Write Encryption Key		DRAM:Plaintext	Duration of session	ZM1	TLS Master Secret:Derived From
TLS Client Write MAC Key		DRAM:Plaintext	Duration of session	ZM1	TLS Master Secret:Derived From
TLS Master Secret		DRAM:Plaintext	Duration of session	ZM1	TLS Premaster Secret:Derived From TLS Client Write Encryption Key:Derives TLS Server Write Encryption

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
					Key:Derives TLS Client Write MAC Key:Derives TLS Server Write MAC Key:Derives
TLS Other Secret		DRAM:Plaintext	Duration of session	ZM1	TLS Client DHE Public Key:Derived From TLS Server DHE Private Key:Derived From TLS Premaster Secret:Derives
TLS Premaster Secret		DRAM:Plaintext	Duration of session	ZM1	BandMaster PSKs:Derived From Drive Owner PSK:Derived From EraseMaster PSK:Derived From TLS Other Secret:Derived From TLS Master Secret:Derives
TLS Server DHE Private Key		DRAM:Plaintext	Duration of session	ZM1	TLS Server DHE Public Key:Paired With TLS Other Secret:Derives
TLS Server DHE Public Key	Host Output	DRAM:Plaintext	Duration of session	ZM1	TLS Server DHE Private Key:Paired With
TLS Server Write Encryption Key		DRAM:Plaintext	Duration of session	ZM1	TLS Master Secret:Derived From
TLS Server Write MAC Key		DRAM:Plaintext	Duration of session	ZM1	TLS Master Secret:Derived From

Table 22: SSP Table 2

Note: The Storage Duration column in the above table is with respect to the volatile version of the SSP (i.e., DRAM or HW Registers). Additionally, the column value Duration of Session can refer to either a TCG/TLS session or a power-on session.

9.5 Transitions

In 2030, the minimum key strength will transition from 112 bits to 128 bits.

10 Self-Tests

10.1 Pre-Operational Self-Tests

The pre-operation self-tests performed by the CM are described in the following table. Algorithms utilized in the Pre-operational firmware integrity tests must pass their own CASTs prior to the integrity tests.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
Disc FW Integrity Test	Modulus: RSA-2048, Hash: SHA-256	KAT	SW/FW Integrity	If test fails, the CM enters FW Integrity Error State	Verify signature on stored DiscFW
Boot FW IDBA Integrity Test	Modulus: RSA-2048, Hash: SHA-256	KAT	SW/FW Integrity	If test fails, the CM enters FW Integrity Error State	Verify signature on stored IDBA FW
Boot FW ITCM Integrity Test	Modulus: RSA-2048, Hash: SHA-256	KAT	SW/FW Integrity	If test fails, the CM enters FW Integrity Error State	Verify signature on stored ITCM FW
Servo Integrity Test	Modulus: RSA-2048, Hash: SHA-256	KAT	SW/FW Integrity	If test fails, the CM enters FW Integrity Error State	Verify signature on stored Controller/Servo FW

Table 23: Pre-Operational Self-Tests

10.2 Conditional Self-Tests

The conditional self-tests performed by the CM are described in the following table.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
Hash DRBG Generate (A7701)	SHA2-256	KAT	CAST	If test fails, CM enters Self-Test Error State	Generate Health Test (see [SP 800-90A Rev. 1])	Bootup
Hash DRBG Instantiate (A7701)	SHA2-256	KAT	CAST	If test fails, CM enters Self-Test Error State	Instantiate Health Test (see [SP 800-90A Rev. 1])	Bootup
Hash DRBG Reseed (A7701)	SHA2-256	KAT	CAST	If test fails, CM enters Self-Test Error State	Reseed Health Test (see [SP 800-90A Rev. 1])	Bootup
90B Continuous Adaptive Proportion Test (APT)	Adaptive Proportion Test	Fault-Detection	CAST	If test fails, CM enters Self-Test Error State	APT	Continuous as entropy is generated from the entropy source.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
90B Continuous Repetition Count Test (RCT)	Repetition Count Test	Fault-Detection	CAST	If test fails, CM enters Self-Test Error State	RCT	Continuous as entropy is generated from the entropy source
90B Start-up Adaptive Proportion Test (APT)	Adaptive Proportion Test	Fault-Detection	CAST	If test fails, CM enters Self-Test Error State	APT	Bootup
90B Start-up Repetition Count Test (RCT)	Repetition Count Test	Fault-Detection	CAST	If test fails, CM enters Self-Test Error State	RCT	Bootup
AES-XTS Comparison Test (A7704)	256-bit key	Comparison Test	Critical Function	If test fails, CM enters Self-Test Error State	Generated XTS keys are compared to ensure Key_1 and Key_2 are not equal	Every time XTS keys are generated
AES-XTS Testing Revision 2.0 Decrypt (A7704)	256-bit key	KAT	CAST	If test fails, CM enters Self-Test Error State	Decrypt	Bootup
AES-XTS Testing Revision 2.0 Encrypt (A7704)	256-bit key	KAT	CAST	If test fails, CM enters Self-Test Error State	Encrypt	Bootup
FW-R5 AES-CBC Decrypt (A7701)	256-bit key	KAT	CAST	If test fails, CM enters Self-Test Error State	Decrypt	Bootup
FW-R5 AES-CBC Encrypt (A7701)	256-bit key	KAT	CAST	If test fails, CM enters Self-Test Error State	Encrypt	Bootup
FW-R5 AES-CMAC (A7701)	AES-256	KAT	CAST	If test fails, CM enters Self-Test Error State	Generate MAC	Bootup
FW-R5 AES-GCM Decrypt (A7701)	256-bit key	KAT	CAST	If test fails, CM enters Self-Test Error State	Authenticated Decrypt	Bootup
FW-R5 AES-GCM Encrypt (A7701)	256-bit key	KAT	CAST	If test fails, CM enters Self-Test Error State	Authenticated Encrypt	Bootup
FW-R5 AES-GCM-SSL	256-bit key	KAT	CAST	If test fails, CM enters	Authenticated Decrypt	Bootup

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
Decrypt (A7702)				Self-Test Error State		
FW-R5 AES-GCM-SSL Encrypt (A7702)	256-bit key	KAT	CAST	If test fails, CM enters Self-Test Error State	Authenticated Encrypt	Bootup
FW-R5 AES-KW Decrypt (A7701)	256-bit key	KAT	CAST	If test fails, CM enters Self-Test Error State	Authenticated Decrypt	Bootup
FW-R5 AES-KW Encrypt (A7701)	256-bit key	KAT	CAST	If test fails, CM enters Self-Test Error State	Authenticated Encrypt	Bootup
FW-R5 HMAC-SHA2-256 (A7701)	256-bit key	KAT	CAST	If test fails, CM enters Self-Test Error State	Generate MAC	Bootup
FW-R5 HMAC-SHA2-384 (A7701)	256-bit key	KAT	CAST	If test fails, CM enters Self-Test Error State	Generate MAC	Bootup
FW-R5 KAS-FFC-SSC (A7701)	2048-bit key	KAT	CAST	If test fails, CM enters Self-Test Error State	Generate Primitive Z	Bootup
FW-R5 PBKDF (A7701)	256-bit key	KAT	CAST	If test fails, CM enters Self-Test Error State	Key Derivation	Bootup
FW-R5 ROM RSA Signature (A7703) Verification	Modulus - 2048-bit Hash: SHA2-256	KAT	CAST	If test fails, CM enters Self-Test Error State.	Verify Signature	Bootup
FW-R5 Safe Primes Key Generation (A7701)	Domain Parameters: ffdhe2048	PCT	PCT	If test fails, CM enters Self-Test Error State	Generate Key Pair	Every time KAS-FFC keys are generated
FW-R5 TLS-KDF (A7701)	Hash Algorithm: SHA2-256, SHA2-384	KAT	CAST	If test fails, CM enters Self-Test Error State	Key Derivation	Bootup
HW-FDE AES-CBC Decrypt (A7704)	256-bit key	KAT	CAST	If test fails, CM enters Self-Test Error State	Decrypt	Bootup
HW-FDE AES-CBC Encrypt (A7704)	256-bit key	KAT	CAST	If test fails, CM enters Self-Test Error State	Encrypt	Bootup

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
HW-FDE AES-XTS Testing Revision 2.0 Decrypt (A7704)	256-bit key	KAT	CAST	If test fails, CM enters Self-Test Error State	Decrypt	Bootup
HW-FDE AES-XTS Testing Revision 2.0 Encrypt (A7704)	256-bit key	KAT	CAST	If test fails, CM enters Self-Test Error State	Encrypt	Bootup
HW-SECA HMAC-SHA2-256(A7705)	256-bit key	KAT	CAST	If test fails, CM enters Self-Test Error State	Generate MAC	Bootup
HW-SECA RSA Signature Verification (A7705)	Modulus - 2048-bit Hash: SHA2-256	KAT	CAST	If test fails, CM enters Self-Test Error State.	Verify Signature	Bootup
HW-SECA RSA Signature Verification FW Load Test (A7705)	Modulus - 2048-bit Hash: SHA2-256	FW Load Test	SW/FW Load	If the test fails, the CM discards incoming FW image, returns failure status, and continues normal operation.	Verify Signature	Test runs every time new FW is loaded to the device

Table 24: Conditional Self-Tests

10.3 Periodic Self-Test Information

The periodic self-tests information is provided in the following tables.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
Disc FW Integrity Test	KAT	SW/FW Integrity	Manual	Reboot
Boot FW IDBA Integrity Test	KAT	SW/FW Integrity	Manual	Reboot
Boot FW ITCM Integrity Test	KAT	SW/FW Integrity	Manual	Reboot
Servo Integrity Test	KAT	SW/FW Integrity	Manual	Reboot

Table 25: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
Hash DRBG Generate (A7701)	KAT	CAST	Manual	Bootup
Hash DRBG Instantiate (A7701)	KAT	CAST	Manual	Bootup
Hash DRBG Reseed (A7701)	KAT	CAST	Manual	Bootup
90B Continuous Adaptive Proportion Test (APT)	Fault-Detection	CAST	Manual	Bootup
90B Continuous Repetition Count Test (RCT)	Fault-Detection	CAST	Manual	Bootup
90B Start-up Adaptive Proportion Test (APT)	Fault-Detection	CAST	Manual	Bootup
90B Start-up Repetition Count Test (RCT)	Fault-Detection	CAST	Manual	Bootup
AES-XTS Comparison Test (A7704)	Comparison Test	Critical Function	Manual	Bootup
AES-XTS Testing Revision 2.0 Decrypt (A7704)	KAT	CAST	Manual	Bootup
AES-XTS Testing Revision 2.0 Encrypt (A7704)	KAT	CAST	Manual	Bootup
FW-R5 AES-CBC Decrypt (A7701)	KAT	CAST	Manual	Bootup
FW-R5 AES-CBC Encrypt (A7701)	KAT	CAST	Manual	Bootup
FW-R5 AES-CMAC (A7701)	KAT	CAST	Manual	Bootup
FW-R5 AES-GCM Decrypt (A7701)	KAT	CAST	Manual	Bootup
FW-R5 AES-GCM Encrypt (A7701)	KAT	CAST	Manual	Bootup
FW-R5 AES-GCM-SSL Decrypt (A7702)	KAT	CAST	Manual	Bootup
FW-R5 AES-GCM-SSL Encrypt (A7702)	KAT	CAST	Manual	Bootup
FW-R5 AES-KW Decrypt (A7701)	KAT	CAST	Manual	Bootup
FW-R5 AES-KW Encrypt (A7701)	KAT	CAST	Manual	Bootup

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
FW-R5 HMAC-SHA2-256 (A7701)	KAT	CAST	Manual	Bootup
FW-R5 HMAC-SHA2-384 (A7701)	KAT	CAST	Manual	Bootup
FW-R5 KAS-FFC-SSC (A7701)	KAT	CAST	Manual	Bootup
FW-R5 PBKDF (A7701)	KAT	CAST	Manual	Bootup
FW-R5 ROM RSA Signature (A7703) Verification	KAT	CAST	Manual	Bootup
FW-R5 Safe Primes Key Generation (A7701)	PCT	PCT	Manual	Bootup
FW-R5 TLS-KDF (A7701)	KAT	CAST	Manual	Bootup
HW-FDE AES-CBC Decrypt (A7704)	KAT	CAST	Manual	Bootup
HW-FDE AES-CBC Encrypt (A7704)	KAT	CAST	Manual	Bootup
HW-FDE AES-XTS Testing Revision 2.0 Decrypt (A7704)	KAT	CAST	Manual	Bootup
HW-FDE AES-XTS Testing Revision 2.0 Encrypt (A7704)	KAT	CAST	Manual	Bootup
HW-SECA HMAC-SHA2-256(A7705)	KAT	CAST	Manual	Bootup
HW-SECA RSA Signature Verification (A7705)	KAT	CAST	Manual	Bootup
HW-SECA RSA Signature Verification FW Load Test (A7705)	FW Load Test	SW/FW Load	Manual	Bootup

Table 26: Conditional Periodic Information

10.4 Error States

The Error State supported by the CM are described in the following table.

Name	Description	Conditions	Recovery Method	Indicator
FW Integrity Error State	FW Integrity Test has failed	Failure of FW Integrity Test during CM power-on sequence	None	Interface error returned on first non-inquiry/identify command
Self-Test Error State (Permanent)	Self-Test has failed	Failure of CAST after reboot from a transient failure	None	Byte 17 of Level 0 Discovery is 0xFF
Self-Test Error State (Transient)	Self-Test has failed	Failure of CAST or Entropy CFT test	Reset Module	Byte 17 of Level 0 Discovery is 0xFF

Table 27: Error States

Note: If the CM enters an error state, the CM returns a failure status, disables all cryptographic operations, and restricts the data output interface. If the error is non-recoverable, there may be SSPs on the CM that have not been sanitized. If this occurs, the Crypto Officer should handle the CM per organizational policies.

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

When the CM is shipped from the factory, it is not in the compliant state. The FIPS Crypto Officer must perform the Secure Initialization steps (see section 11.2.1) for the CM to transition to the compliant state. Additionally, for the CM to remain in the compliant state, there are some Security Policy Restrictions (see section 11.2.2) that need to be maintained.

11.2 Administrator Guidance

The Secure Initialization steps are described in section 11.2.1 and the ongoing policy restrictions are described in section 11.2.2.

The Product Manual is available at the following link:

https://www.seagate.com/content/dam/seagate/assets/support/internal-hard-drive/enterprise-hard-drives/exos-x24/_shared/files/Seagate_Exos_24_SAS_ISE-SED-FIPs(12-16-20-24TB)_Rev-A.pdf

11.2.1 Secure Initialization

The Crypto Officer shall perform the following Secure Initialization steps when the CM is installed to transition the CM into the compliant state:

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 installation and periodically thereafter, examine the physical security mechanisms for tamper evidence.
3. At initialization, set all enabled operator PINs applicable for the approved mode to private values of at least 8 bytes (64 bits) in length: Drive Owner, EraseMaster, and BandMasters[3].
4. At initialization, 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, set the value of LockOnReset for FW Download port to include “Power Cycle”.

11.2.2 Policy Restrictions

For the CM to remain in the compliant state, the Crypto Officer shall ensure the following Security Policy Restrictions are maintained:

- 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
- The “Makers” authority must be disabled.
- The value of LockOnReset for FW Download port must include “Power Cycle”.

[3] 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 FIPS Operating mode, the Crypto Officer will need to enable them as part of the initialization steps.

11.3 Non-Administrator Guidance

There is no non-administrator guidance for the CM.

11.4 Maintenance Requirements

The CM has no maintenance requirements.

11.5 End of Life

When the CM reaches end-of-life, the Crypto Officer must zeroize all SSPs prior to retiring 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 RevertSP method[4] on the Admin SP.
2. If step 1 fails, all SSPs on the CM may not have been sanitized. If this occurs, the Crypto Officer should handle the CM per organizational policies.

[4] The RevertSP method will cause the CM to zeroize all the SSPs and exit the Approved Mode.

12 Mitigation of Other Attacks

The CM does not provide mitigation against any other attacks.

Appendix A. References

[FIPS 140-3] National Institute of Standards and Technology, Federal Information Processing Standards Publication Security Requirements for Cryptographic Modules, FIPS 140-3, March 2019. https://doi.org/10.6028/NIST.FIPS.140-3

[FIPS 140-3 IG] National Institute of Standards and Technology, Implementation Guidance for FIPS 140-3 and the Cryptographic Module Validation Program, 20 December 2024. https://csrc.nist.gov/Projects/cryptographic-module-validation-program/fips-140-3-ig-announcements

[FIPS 180-4] National Institute of Standards and Technology, Federal Information Processing Standards Publication Secure Hash Standard (SHS), FIPS 180-4, August 2015. https://doi.org/10.6028/NIST.FIPS.180-4

[FIPS 186-5] National Institute of Standards and Technology, Federal Information Processing Standards Publication Digital Signature Standard (DSS), FIPS 186-5, February 2023. https://doi.org/10.6028/NIST.FIPS.186-5

[FIPS 197] National Institute of Standards and Technology, Federal Information Processing Standards Publication Advanced Encryption Standard (AES), FIPS 197, November 2001. https://doi.org/10.6028/NIST.FIPS.197

[FIPS 198-1] National Institute of Standards and Technology, Federal Information Processing Standards Publication The Keyed-Hash Message Authentication Code (HMAC), FIPS 198-1, July 2008. https://doi.org/10.6028/NIST.FIPS.198-1

[ISO/IEC 19790:2012(E)] International Standards Organization / International Electrotechnical Commission, Information technology — Security techniques — Security requirements for cryptographic modules, ISO/IEC 19790:2012(E), December 2015. https://www.iso.org/standard/52906.html

[SBC] International Committee for Information Technology Standards (INCITS), Information technology - SCSI Block Commands – X (SBC-X).[5]

[SP 800-38A] National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation Methods and Techniques, NIST Special Publication 800-38A, December 2001. https://doi.org/10.6028/NIST.SP.800-38A

[SP 800-38B] National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, NIST Special Publication 800-38B, May 2005. https://doi.org/10.6028/NIST.SP.800-38B

[SP 800-38D] National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, NIST Special Publication 800-38D, November 2007. https://doi.org/10.6028/NIST.SP.800-38D

[SP 800-38E] National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices, NIST Special Publication 800-38E, January 2010. https://doi.org/10.6028/NIST.SP.800-38E

[SP 800-38F] National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping, NIST Special Publication 800-38F, December 2012. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-38F.pdf

[5] Refer to product manual for exact version of SBC.

[SP 800-56A Rev. 3] National Institute of Standards and Technology, Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography, NIST Special Publication 800-56A Rev. 3, April 2018. https://doi.org/10.6028/NIST.SP.800-56Ar3

[SP 800-90A Rev. 1] National Institute of Standards and Technology, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, NIST Special Publication 800-90A Rev. 1, June 2015. https://doi.org/10.6028/NIST.SP.800-90Ar1

[SP 800-90B] National Institute of Standards and Technology, Recommendation for the Entropy Sources Used for Random Bit Generation, NIST Special Publication 800-90B, January 2018. https://doi.org/10.6028/NIST.SP.800-90B

[SP 800-132] National Institute of Standards and Technology, Recommendation for Password-Based Key Derivation: Part 1: Storage Applications, NIST Special Publication 800-132, December 2010. https://doi.org/10.6028/NIST.SP.800-132

[SP 800-133 Rev. 2] National Institute of Standards and Technology, Recommendation for Cryptographic Key Generation, NIST Special Publication 800-133 Rev. 2, June 2020. https://doi.org/10.6028/NIST.SP.800-133r2

[SP 800-135 Rev. 1] National Institute of Standards and Technology, Recommendation for Existing Application-Specific Key Derivation Functions, NIST Special Publication 800-135 Rev. 1, December 2011. https://doi.org/10.6028/NIST.SP.800-135r1

[SP 800-140B Rev. 1] National Institute of Standards and Technology, CMVP Security Policy Requirements CMVP Validation Authority Updates to ISO/IEC 24759 and ISO/IEC 19790 Annex B Second Public Draft, NIST Special Publication 800-140B, October 2022.

[SPC] International Committee for Information Technology Standards (INCITS), Information technology - SCSI Block Commands – X (SPC-X).[6]

[SFSC] International Committee for Information Technology Standards (INCITS), Information technology – Security Features for SCSI Commands (SFSC) Revision 02, September 2015.

[RFC 5116] Internet Engineering Task Force, An Interface and Algorithms for Authenticated Encryption, RFC 5116, March 2009. https://www.rfc-editor.org/rfc/rfc5116

[RFC 5487] Internet Engineering Task Force, Pre-Shared Key Cipher Suites for TLS with SHA-256/384 and AES Galois Counter Mode, RFC 5487, March 2009. https://www.rfc-editor.org/rfc/rfc5487.html

[RFC 7627] Internet Engineering Task Force, Transport Layer Security (TLS) Session Hash and Extended Master Secret Extension, RFC 7627, September 2015. https://www.rfc-editor.org/rfc/rfc7627.html

[TCG Core Spec v1] Trusted Computing Group, TCG Storage Architecture Core Specification, Specification Version 1.00 Revision 0.9 – draft, May 2007.

[TCG Ent SSC] Trusted Computing Group, TCG Storage Security Subsystem Class: Enterprise, Specification Version 1.01 Revision 1.00, June 2015. https://trustedcomputinggroup.org/wp-content/uploads/TCG_Storage-SSC_Enterprise-v1.01_r1.00.pdf

[TCG PSK Ent] Trusted Computing Group, TCG Storage Enterprise SSC Feature Set: PSK Secure Messaging, Specification Version 1.00 Revision 1.00, August 2015.

[6] Refer to product manual for exact version of SPC.

https://trustedcomputinggroup.org/wp-content/uploads/TCG_Storage-Enterprise_Feature_Set_PSK_Secure_Messaging_v1.00_r1.00.pdf

Appendix B. Terms and Acronyms

Term / Acronym	Definition
AES	Advanced Encryption Standard (see [FIPS 197])
CAST	Cryptographic Algorithm Self-Test
CBC	Cipher Block Chaining Mode (see [SP 800-38A])
CFT	Critical Functions Test
CM	Cryptographic Module
DRBG	Deterministic Random Bit Generator (see [SP 800-90A Rev. 1])
FW	Firmware
ESV	Entropy Source Validation
GCM	Galois Counter Mode (see [SP 800-38D])
HDD	Hard Disk Drive
HMAC	Hash-based Message Authentication Code (see [FIPS 198-1])
HW	Hardware
KAT	Known Answer Test
KAS FFC SSC	Key Agreement Schemes Finite Field Cryptography (see [SP 800-56A Rev. 3])
KDF	Key Derivation Function
KW	Key Wrap (see [SP 800-38F])
LBA	Logical Block Address is the method which is used by the CM when addressing User Data.
MEK	Media Encryption Key
MEKEK	Media Encryption Key Encryption Key
OE	Operating Environment
PBKDF	Password-Based Key Derivation Function (see [SP 800-132])
PCBA	Printed Circuit Board Assembly
PCT	Pair-wise Consistency Test
PSK	Pre-Shared Key (for TLS handshake)
PSID	Physical Security ID
PSP	Public Security Parameter
RSA	Rivest-Shamir-Adleman public-key cryptosystem (see [FIPS 186-5])
SAS	Serial Attached SCSI

Term / Acronym	Definition
SCSI	Small Computer System Interface
SED	Self-Encrypting Drive
SHA	Secure Hash Algorithm (see [FIPS 180-4])
SID	Security ID (i.e., Drive Owner)
SSC	Security Subsystem Class
SSP	Sensitive Security Parameter
TEL	Tamper Evident Label
TCG	Trusted Computing Group
XTS	XEX-based tweaked-codebook mode with ciphertext stealing (see [SP 800-38E])