FIPS 140 - 3 Non-Proprietary Security Policy for:

Toshiba Secure TCG Opal SSC Self-Encrypting Drive Series

MG09SCP18TA and MG09SCP16TA

Prepared by:

TOSHIBA ELECTRONIC DEVICES & STORAGE CORPORATION

Rev 2.4.0

1. General

The Toshiba Secure TCG Opal SSC Self-Encrypting Drive Series (MG09SCP18TA and MG09SCP16TA) is used for hard disk drive data security. The security levels for this Cryptographic Module (CM) are as follows:

ISO/IEC 24759 Section 6. [Number Below]	FIPS 140-3 Section Title	Security Level
1	General	1
2	Cryptographic module specification	1
3	Cryptographic module interfaces	1
4	Roles, services, and authentication	1
5	Software/Firmware security	2
6	Operational environment	1
7	Physical security	1
8	Non-invasive security	N/A
9	Sensitive security parameter management	1
10	Self–tests	1
11	Life-cycle assurance	1
12	Mitigation of other attacks	N/A
	Overall Level	1

Table 1: Security Levels

1.1 Acronyms

AES	Advanced Encryption Standard
CM	Cryptographic Module
CSP	Critical Security Parameter
DRBG	Deterministic Random Bit Generator
EBG	Entropy Bit Generator
FW	Firmware
HMAC	Keyed-Hashing for Message Authentication code
KAT	Known Answer Test
LBA	Logical Block Address
PCA	Printed Circuit Assembly
POST	Power on Self-Test (pre-operational self-tests and conditional algorithm self-tests)
SoC	System on Chip
SSC	Security Subsystem Class
SED	Self-Encrypting Drive
SHA	Secure Hash Algorithm
SID	Security ID
TCG SWG	Trusted Computing Group Storage Work Group
TOEPP	Tested Operational Environment's Physical Perimeter

2. Cryptographic Module Specification

This CM provides various cryptographic services using approved algorithms. Services include hardware-based data encryption, cryptographic erase, independently protected user data LBA ranges, and FW Download. The CM always encrypts the user data, protects CSPs from unauthorized access, and provides secure sanitization methods by supporting TCG Opal SSC features. The operational rules described in this document adheres to TCG Opal.

This CM is a multiple-chip-embedded hardware cryptographic module. The cryptographic boundary of the CM is the entire HDD. The physical interface for power-supply and for communication is one SAS connector. The CM is connected with host system by this SAS connector. The logical interface is the SAS, TCG SWG and Opal SSC.

The CM has the non-volatile storage area for not only user data but also the keys, CSPs, and FW. The latter storage area is called the “system area”, which is not logically accessible / addressable by the host application.

The CM has one approved mode of operation and CM is always in approved mode of operation. The CM provides only approved services defined in 4.2. Non-approved security functions are not implemented.

2.1 Product Version

The Toshiba Secure TCG Opal SSC SED has been validated in the following versions:

Model	Hardware [Part Number and Version]	Firmware Version	Distinguishing Features
MG09SCP18TA	A0	PC82	SAS interface, 18TB
MG09SCP16TA	A0	PC82	SAS interface, 16TB

The tested platform is Toshiba Cryptographic Hardware 88i1215-B1. The CM does not employ any operating system.

Table 2: Cryptographic Module Tested Configuration

2.2 All Security Functions

The CM does not implement any non-approved algorithms allowed in the approved mode of operation. It does not implement any non-approved algorithms allowed in the approved mode of operation with no security claimed. It does not implement any non-approved algorithms not allowed in the approved mode of operation.

CAVP Certs	Algorithm and Standard	Mode/Method	Description / Key Size(s) / Key Strength	Use/Function
A1637	RSA, FIPS PUB 186-4	RSASSA-PKCS#1-v1_5	Modulus: 3072bits, Key Strength: 128bits	Digital signature verification
A1637	SHS, FIPS PUB 180-4	SHA2-256 (BYTE-only)	-	Message digest for RSA
A1638	AES, FIPS PUB 197-	CBC	Key Size: 256bits, Key Strength: 256bits	Data encryption / decryption

CAVP Certs	Algorithm and Standard	Mode/Method	Description / Key Size(s) / Key Strength	Use/Function
	upd1, SP800-38A			
A1638	AES, FIPS PUB 197-upd1, SP800-38E	XTS	Key Size (Key_1): 256bits, Key Size (Key_2): 256bits, Key Strength: 256bits	Data encryption / decryption
A1638	HMAC, FIPS PUB 198-1	SHA2-256	Key Size: 256bits, Key Strength: 256bits, KS < BS	Message authentication for data integrity verification of system area
A1638	SHS, FIPS PUB 180-4	SHA2-256 (BYTE-only)	-	Message digest for HMAC
A1645	Hash-DRBG, SP800-90A rev1	SHA2-256	Prediction Resistance : False	Deterministic random bit generation
A1645	SHS, FIPS PUB 180-4	SHA2-256 (BYTE-only)	-	Message digest for DRBG
ENT (P)	SP800-90B	-	-	Seed generation for Hash-DRBG
Vendor Affirmed	CKG, SP800-133rev2	-	An output of the hash-DRBG is directly used. (Section 4 of SP800-133rev2)	Key generation

There are algorithms, modes, and keys that have been CAVP tested but not used by the module. Only the algorithms, modes/methods, and key lengths/curves/moduli shown in this table are used by the module.

Table 3: Approved Algorithms

Figure 1: MG09SCP16TA

Figure 2: MG09SCP18TA

Figure 3: PCA side

Figure 4: Side of the device

Figure 5: SAS port

Figure 6: Side of the device

Figure 7 shows the CM's block diagram. In this diagram, the cryptographic boundary of the CM, defined by the enclosure of the MG09SCP18TA and the MG09SCP16TA, is indicated by a dashed line. It includes the SAS connector, the SoC, the buffer DRAM, the flash ROM and the magnetic storage medium.

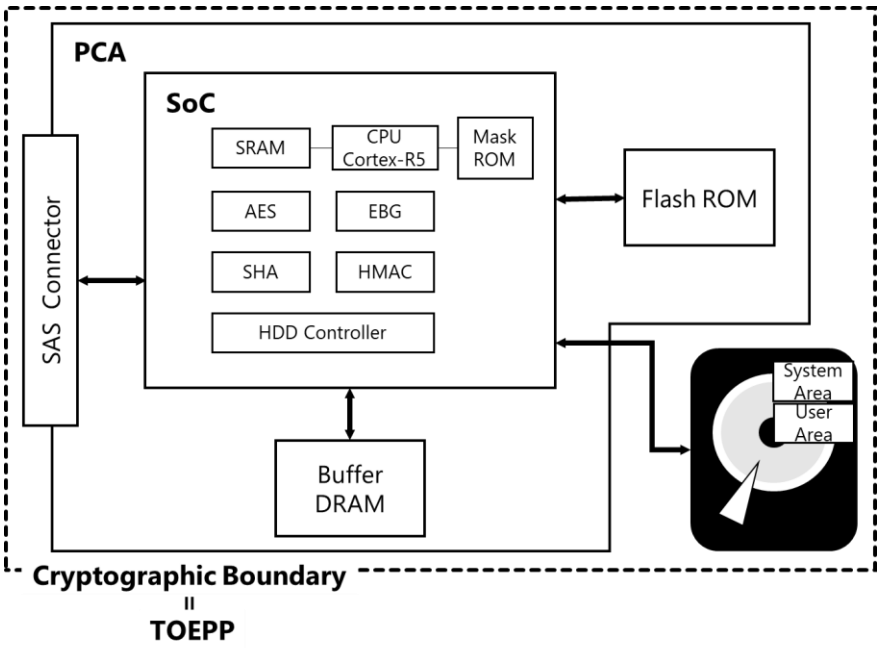

Figure 7: Block Diagram

3. Cryptographic Module Interfaces

The CM does not implement any control output interface.

Physical port	Logical interface	Data that passes over port / interface
SAS connector	Data input interface	User data, FW data
SAS connector	Data output interface	User data
SAS connector	Control input interface	SAS control input data (ex. command frame, data frame)
N/A	Control output interface	N/A
SAS connector	Status output interface	SAS status output data (ex. response frame, data frame)
SAS connector	Power interface	N/A

All data, status, control, and power interfaces above use a single SAS connector that contains multiple pins for power supply, data transmission, and signal exchange.

Table 4: Ports and Interfaces

4. Roles, Services, and Authentication

This section describes roles and services the CM supports. The CM supports 14 Crypto Officer roles listed in Table 5. The roles listed in Table 5 are all Crypto Officer roles.
The CM does not implement any Non-Approved Services.

4.1 Roles

Role[1]	Service	Input	Output
LockingSP.Admin1 … LockingSP.Admin4	Enable / Disable LockingSP Admin/User	Security Protocol Out command	Command response
	Range Lock/Unlock		
	Set range position and size		
	TCG Reactivate		
	TCG Cryptographic Erase (Erase)		
	TCG Cryptographic Erase (GenKey)		
	Zeroization (without RKey)		
LockingSP.User1 … LockingSP.User9	Range Lock/Unlock	Security Protocol Out command	Command response
	Set range position and size		
	TCG Cryptographic Erase (Erase)		
	TCG Cryptographic Erase (GenKey)[2]		
AdminSP.SID	TCG activate	Security Protocol Out command	Command response
	Firmware Download	Security Protocol Out command and Write Buffer command with FW	
None	Reset (run POSTs)	Power on reset command	Command response
	Data read / write	Read/Write commands with User data	Command response, User data
	Random number generation	Security Protocol Out command	Command response, Random number
	Show status	Request Sense command	Command response, Status
	Zeroization (with RKey) (using PSID)	Security Protocol Out command	Command response
	Cryptographic Sanitization	Sanitize command	
	Show versioning information	Inquiry command	Command response, Versioning

[1] TCG Authority (LockingSP.Admin1-4, AdminSP.Admin1, LockingSP.User1-9 or AdminSP.SID) can be assumed by using TCG Start Session method.
[2] Available only when the CM uses TCG Single User Mode functionality.
The CM is always in 140-3 approved mode of operation regardless of this functionality.

Role[1]	Service	Input	Output
			information
	Non-security relevant HDD service	SCSI command	Command response

Table 5: Roles, Service Commands, Input and Output

4.2 Services

The CM supports the TCG Single User Mode functionality defined in the Single User Mode feature set of TCG Opal. A single role (LockingSP.Userx) is assigned to manage the associated range (range X) during the TCG single user mode. The LockingSP.Reactivate or LockingSP.Activate method enables this mode. Authorized roles of some services differ when the CM is in single user mode. About such services, the Role(s) column in Table 6 is divided into two rows. The upper row shows authorized roles in non-single user mode (normal mode), while the lower row shows authorized roles against range X in single user mode.

The CM provides the following services to operators per Section 7.4.3.1 of ISO/IEC 19790_2012_2015:

- Show module's versioning information: Show versioning information service
- Show status: Show Status service
- Perform self-test: Reset (run POSTs) service
- Perform zeroization: Zeroization (with RKey) service, Zeroization (without RKey) services
- Perform approved security functions: Services indicated with Approved Security Functions in Table 6

The modes of access to SSPs shown in Table 6 are defined as:

G = Generate: The module generates or derives the SSP.

R = Read: The SSP is read from the module (e.g. the SSP is 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 = Zeroise: The module zeroises the SSP.

Service	Description	Approved Security Functions	Keys and/or SSPs	Role(s)	Access rights to Keys and/or SSPs	Indicator
Data read/write (decrypt/encrypt)	Encryption / decryption of unlocked user data to/from range Method: SCSI READ, WRITE commands	AES256-XTS	MEK(s)	None	E	Command response

Service	Description	Approved Security Functions	Keys and/or SSPs	Role(s)	Access rights to Keys and/or SSPs	Indicator
Enable /Disable LockingSP Admin/User	Enable/Disable LockingSP Admin/User (except for-Single-User-Data-Range User) Authority Method: SECURITY PROTOCOL OUT command (TCG Set Method)	HMAC SHA2-256(A1638)	N/A	LockingSP.Adminx	N/A	Command response
Random Number generation	Provide a random number generated by the CM Method: SECURITY PROTOCOL OUT command (TCG Random)	Hash_DRBG SHA2-256(A1645)	DRBG C Vector DRBG V Vector	None	E E	Command response
Range Lock/Unlock	Block or allow read (decrypt) / write (encrypt) of user data in a range. Locking also requires read/write locking to be enabled Method: -SECURITY PROTOCOL OUT command (TCG Set Method)	HMAC SHA2-256(A1638)	RKey MEK(s)	LockingSP.Adminx/LockingSP.Userx (LockingSP is active) LocknigSP.Userx	E E	Command response
Set range position and size	Set the location and size of the LBA range Method: SECURITY PROTOCOL OUT command (TCG Set Method)	Hash_DRBG SHA2-256(A1645) AES256-CBC HMAC SHA2-256(A1638) ENT (P) CKG	MEK(s) RKey	LockingSP.Adminx LockingSP.Adminx or LockingSP.Userx	G E	Command response
Reset (run POSTs)	Perform self-tests and delete CSPs in SRAM Method: Power on reset command	RSASSA-PKCS#1-v1_5 SHA2-256(A1637)	DRBG C Vector DRBG V Vector Seed RKey	None	G, Z G, Z G, E, Z E	Command response
TCG reactivate	Switch from/to TCG Opal single user mode Method: SECURITY PROTOCOL OUT command (TCG Reactivate)	HMAC SHA2-256(A1638)	N/A	LockingSP.Adminx	N/A	Command response
Show Status	Report status of the CM Method: REQUEST SENSE command	N/A	N/A	None	N/A	Command response

Service	Description	Approved Security Functions	Keys and/or SSPs	Role(s)	Access rights to Keys and/or SSPs	Indicator
TCG Activate	Activate LockingSP Method: SECURITY PROTOCOL OUT command (AdminSP.activate)	Hash_DRBG SHA2-256(A1645) AES256-CBC HMAC SHA2-256(A1638)	MEK(s) (except for Global Range) RKey	AdminSP.SID	G E	Command response
TCG Cryptographic Erase (Erase)	Erase user data (in cryptographic means) in an LBA range by changing the data encryption key. This method is available only in single user mode. Method: SECURITY PROTOCOL OUT command (TCG Erase)	Hash_DRBG SHA2-256(A1645) AES256-CBC HMAC SHA2-256(A1638) ENT (P) CKG	MEK(s) RKey	N/A LocknigSP.Userx LockingSP.Adminx	G, Z E	Command response
TCG Cryptographic Erase (GenKey)	Erase user data (in cryptographic means) in an LBA range by changing the data encryption key. Method: SECURITY PROTOCOL OUT command (TCG GenKey)	Hash_DRBG SHA2-256(A1645) AES256-CBC HMAC SHA2-256(A1638) ENT (P) CKG	MEK(s) RKey	LockingSP.Adminx LockingSP.Userx	G, Z E	Command response
Zeroization (with RKey)	Initialize the CM by zeroizing RKey, MEKs, and range configuration. Method: SECURITY PROTOCOL OUT command (- AdminSPObj.Revert[3])	Hash_DRBG SHA2-256(A1645) AES256-CBC HMAC SHA2-256(A1638) ENT (P) CKG	MEK(s) RKey	None (using PSID[4])	G, Z G, E, Z	Command response
Zeroization (without RKey)	Initialize the CM by zeroizing MEKs, and range configuration. Method: SECURITY PROTOCOL OUT command (- LockingSP.RevertSP[3] - LockingSPObj.Revert[3])	Hash_DRBG SHA2-256(A1645) AES256-CBC HMAC SHA2-256(A1638) ENT (P) CKG	MEK(s) RKey	LockingSP.Adminx	G, Z E	Command response

[3] AdminSPObj.Revert, LockingSP.RevertSP, LockingSPObj.Revert are methods of TCG Opal SSC.
[4] PSID (Printed SID) is public drive-unique value which is used for the TCG Revert AdminSP method. PSID is printed on the HDD's product label.

Service	Description	Approved Security Functions	Keys and/or SSPs	Role(s)	Access rights to Keys and/or SSPs	Indicator
Firmware Download	Enable / Disable firmware download and load a part of a firmware image. If the firmware load test passes, the CM will run with the new code. Method: SECURITY PROTOCOL OUT command (TCG Set Method), WRITE BUFFER command	RSASSA-PKCS#1-v1_5 SHA2-256(A1637) HMAC SHA2-256(A1638)	PubKey	AdminSP.SID	E	Command response
Cryptographic Sanitization	Erase user data by changing the data encryption key. This service is available only when all ranges are unlocked. Method: SANITIZE CRYPTOGRAPHIC ERASE command	Hash_DRBG SHA2-256(A1645) AES256-CBC HMAC SHA2-256(A1638) ENT (P) CKG	MEK(s) RKey	None	G, Z E	Command response
Show versioning information	Output the model name, HW version and FW version of the CM. Method: INQUIRY Standard Inquiry data command with Byte 32-35 (FW version), VPD Page C2, Byte 4-5 (HW version)	N/A	N/A	None	N/A	Command response
Non-security relevant HDD service	Provide a HDD general service Method: SCSI commands	N/A	N/A	None	N/A	Command response

Table 6: Approved Services

5. Software/Firmware Security

FW integrity check is performed at power on. Signature verification using RSASSA-PKCS#1-v1_5 of the FW codes (in the flash ROM and in the disk media) and EDC verification of the FW code in the Mask ROM are done. The operator can initiate the on-demand FW integrity check by power cycling. All firmware components are in executable form, which cannot be dynamically modified.

6. Operational Environment

The CM is a hardware module and operates in a non-modifiable operational environment, that is its firmware cannot be modified and no code can be added or deleted. SSPs are controlled by the CM itself, and uncontrolled access to CSPs and uncontrolled modifications of SSPs are prevented.
Although firmware can be updated by “Firmware Download” service, whole FW codes (in the flash ROM and in the disk media) are replaced by this service, and the module becomes another module

which requires new 140-3 certification.

7. Physical Security

The CM has the following physical security:

- Production-grade components with standard passivation
- Exterior of the drive is opaque

The operator is required to periodically inspect the enclosure condition of the CM.

8. Non-Invasive Security

The CM does not employ non-invasive mitigation techniques referenced in NIST SP800-140F.

9. Sensitive Security Parameters Management

The CM uses SSPs in the following tables:

Key/SSP/Name/ Type	Strength	Security function and cert. number	Generation	Import/ export	Establishment	Storage	Zeroization	Use & related keys
MEKs/ CSP/ Symmetric	256	AES-XTS(A1638)	By Hash-DRBG (A1645) CKG, SP800-133rev2 Compliant with IG C.I (Key_1 ≠ Key_2)	No	After "Zeroization (with RKey /without RKey)", "TCG Cryptographic Erase (Erase/ GenKey)", "Cryptographic Sanitization", "TCG Activate", and "Set range position and size" services. In the factory	Encrypted by RKey / in System area /Static	By "Zeroization (with RKey /without RKey)", "TCG Cryptographic Erase (Erase / GenKey)", and "Cryptographic Sanitization" services (explicitly)	User data encryption and decryption (only for storage purpose) Encrypted and decrypted by RKey
					By "Range Lock/Unlock" service. By "Reset" service (when the associated range is unlocked)	Plain/ in SRAM (SoC register) /Dynamic	By power-off (implicitly)	
RKey/ CSP/ Symmetric	256	AES-CBC(A1638)	By Hash-DRBG (A1645) CKG, SP800-133rev2	No	After "Zeroization (with RKey)" service. In the factory	Obfuscated (plain in 140-3 means) / in System area /Static	By "Zeroization (with RKey)" service (explicitly)	Encryption and decryption of MEKs

Key/SSP/Name/ Type	Strength	Security function and cert. number	Generation	Import/ export	Establishment	Storage	Zeroization	Use & related keys
					By “Zeroization (with RKey /without RKey)”, “TCG Cryptographic Erase (Erase/ GenKey)”, “Cryptographic Sanitization”, “TCG Activate”, “Set range position and size”, and “Range Lock/Unlock” services. By “Reset” service (when the range is unlocked)	Plain/ in SRAM /Dynamic	After use (implicitly)	
Seed/ CSP/ DRBG seed[5]	N/A[6]	Hash-DRBG(A1645), Entropy source	By Entropy source	No	At instantiation (SP800-90Arev1)	Plain/ in SRAM /Dynamic	By power-off (implicitly)	Instantiation of Hash_DRBG
DRBG C Vector /CSP /internal state	N/A[6]	Hash-DRBG(A1645)	By DRBG	No	At instantiation (SP800-90Arev1)	Plain/ in SRAM /Dynamic	By power-off (implicitly)	Random number generation
DRBG V Vector / CSP/ internal state	N/A[6]	Hash-DRBG(A1645)	By DRBG	No	At instantiation (SP800-90Arev1)	Plain/ in SRAM /Dynamic	By power-off (implicitly)	Random number generation
PubKey/ PSP/ Public	Modulus: 3072 Key Strength :128	RSASSA-PKCS#1-v1_5(A1637)	Manufacturing	No	In the factory	Plain / Embedded in FW in system area /Static	By "Firmware Download” service (explicitly)	Signature verification
					By “Firmware Download” service	Plain/ in SRAM /Dynamic	By power-off (implicitly)	

Table 8: SSPs

Note that there is no security-relevant audit feature and audit data.

[5] Entropy input string and nonce.
[6] The security strength of Hash_DRBG is 256 bits.

Entropy sources	Minimum number of bits of entropy	Details
Entropy source	0.6 / 1	Physical noise source used to seed the approved Hash-DRBG. The overall amount of generated entropy is 48 bytes. This entropy source meets NIST SP800-90B requirements.

Table 9: Non-Deterministic Random Number Generation Specification

If the source may deteriorate to the point when the generation of the sufficient amount of entropy can no longer be guaranteed, health test detects the source deterioration, enter an error state, and halts the CM. When the CM continuously enters in error state in spite of several trials of reboot, the CM shall be sent back to factory to recover from error state.

10. Self-Tests

The CM runs self-tests in the following table.

Function	Self-test type	Description	Operator initiation	Failure behavior
Firmware integrity check	Pre-operational software/firmware integrity test	EDC (32bits) verification of the firmware in the Mask ROM	Power-cycle	Boot error state The CM is not accessible via SAS interface
		Signature verification of the firmware in the flash ROM by RSASSA-PKCS#1-v1_5 with a 3072-bit Modulus using "PubKey2"		Boot error state The CM is not accessible via SAS interface
		Signature verification of the firmware in the disk media by RSASSA-PKCS#1-v1_5 with a 3072-bit Modulus using "PubKey2"		Boot error state Status: CHECK CONDITION(02h), Sense Data: 04 4C 9F
AES CBC	Conditional cryptographic algorithm test	Encrypt KAT with a 256-bit key	Power-cycle	Boot error state Status: CHECK CONDITION(02h), Sense Data: 04 44 92
		Decrypt KAT with a 256-bit key		
AES XTS	Conditional cryptographic algorithm test	Encrypt KAT with a 256-bit key	Power-cycle	
		Decrypt KAT with a 256-bit key		
SHA2-256(A1637)	Conditional cryptographic algorithm test	Digest KAT	Power-cycle	
SHA2-256(A1638)	Conditional cryptographic algorithm test	Digest KAT	Power-cycle	
SHA2-256(A1645)	Conditional cryptographic	Digest KAT	Power-cycle	

	algorithm test			
Hash DRBG	Conditional cryptographic algorithm test	DRBG KAT for instantiate and generate functions	Power-cycle	
HMAC	Conditional cryptographic algorithm test	Digest KAT	Power-cycle	
RSASSA-PKCS#1-v1_5	Conditional cryptographic algorithm test	Signature verification KAT with a 3072-bit Modulus	Power-cycle	
Entropy source	Conditional cryptographic algorithm test	SP800-90B Start-up health test (repetition count test, adaptive proportion test)	Power-cycle	Boot error state Status: CHECK CONDITION(02h), Sense Data: 04 40 91
		SP800-90B Continuous health test (repetition count test, adaptive proportion test)	Power-cycle	Error state (conditional test) Status: CHECK CONDITION(02h), Sense Data: 04 44 92
Firmware load test	Conditional software/firmware load test	Signature verification of firmware image by RSASSA-PKCS#1-v1_5 with a 3072-bit Modulus	N/A	Error state (FW Load Test) Status: CHECK CONDITION(02h), Sense Data: 0B 74 08 The CM discards the new firmware image, then enters the Idle state

The public verification key "PubKey2" used in firmware integrity check resides within the MaskROM code and is not a SSP.

SHA2-256(A1637) is embedded in RSASSA-PKCS#1-v1_5, while SHA2-256(A1638) is used in HMAC, and SHA2-256(A1645) is employed in Hash DRBG.

The CM does not implement reseed function of Hash DRBG.

Table 10: Self-Tests

If the CM fails the self-test, it enters one of three error states: Error State (Conditional Test), Error State (FW Load Test), or Boot Error State. If the SP800-90B continuous health test fails, it enters Error State (Conditional Test); if the firmware load test fails, it goes to Error State (FW Load Test); and for other self-tests, it transitions to Boot Error State. Status indicator for each error state is specified in Table 10 (e.g. "Status: CHECK CONDITION(02h), Sense Data: 04 40 91" indicates the CM is currently in Boot Error State).

When in the error state, the CM does not perform any cryptographic operations or output data. A power cycle is required to clear the error state. When the CM continuously enters the error state despite several reboot attempts, the CM should be returned to the factory for recovery from the error state.

The CM does not support any degraded operation.

11. Life-Cycle Assurance

The following are the secure initialization procedure for the CM.
The CM is always in approved mode of operation in a deployed environment. In addition to this, the following procedure of initial settings will allow further secure operation during power cycling. Please refer to TCG Opal specification (TCG Storage Security Subsystem Class: Opal Version 2.01 Revision 1.00) for the details.

(1) Activate LockingSP by "TCG Activate" service.
(2) Set LockOnReset in Download port to "Power Cycle".
(3) Set ReadLockEnabled and WriteLockEnabled to 1(true) and LockOnReset to "Power Cycle".
(4) Do a power-on-reset.

The longest service life of the CM under suitable conditions and treatment is 5 years. By the end of this period the operator is required to follow the CM's end of life procedures below.

(1) Initialize internal sensitive data in the host system.
(2) Initialize parameters and user information in the CM by "Zeroization (with RKey)" service.

For additional details, refer to the guidance documents provided with the CM:

- 3.5 type SAS Hard Disk Drives Product Specification
- 3.5 type SAS Hard Disk Drives Interface Specification
- 3.5 type Hard Disk Drives SED Specification
- Toshiba SED HDD FIPS140-2/3 Use case Rev.6.0

12. Mitigation of Other Attacks

The CM does not mitigate other attacks beyond the scope of 140-3 requirements.