FIPS 140 - 2 Security Policy for:

Toshiba TCG Enterprise SSC Self-Encrypting Hard Disk Drive

(AL14SEQ model)

TOSHIBA CORPORATION

Rev 1.0.0

Overview

The Toshiba TCG Enterprise SSC Self-Encrypting Hard Disk Drive (AL14SEQ18/12/09EQB, AL14SEQ18/12/09EPB) is used for hard disk drive data security. This Cryptographic Module (CM) provides various cryptographic services using FIPS approved algorithms. Services include hardware-based data encryption, cryptographic erase, and FW download.

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

Section	*Level*
1. Cryptographic Module Specification	*2*
2. Cryptographic Module Ports and Interfaces	*2*
3. Roles, Services, and Authentication	*2*
4. Finite State Model	*2*
5. Physical Security	*2*
6. Operational Environment	*N/A*
7. Cryptographic Key Management	*2*
8. EMI/EMC	*2*
9. Self - Tests	*2*
10. Design Assurance	*2*
11. Mitigation of Other Attacks	*N/A*
Overall Level	*2*

Table 1 - Security Level Detail

Interface	Ports
Data Input	SAS connector
Control Input	SAS connector
Data Output	SAS connector
Status Output	SAS connector
Power Input	SAS connector

Table 1-1 - Physical/Logical Port Mapping

Acronyms

AES	Advanced Encryption Standard
CM	Cryptographic Module
CSP	Critical Security Parameter
DRBG	Deterministic Random Bit Generator
EDC	Error Detection Code
FW	Firmware

HMAC	Keyed-Hashing for Message Authentication code
KAT	Known Answer Test
LBA	Logical Block Address
MSID	Manufactured SID
NDRNG	Non-Deterministic Random Number Generator
PCB	Printed Circuit Board
POST	Power on Self-Test
PSID	Printed SID
SED	Self-Encrypting Drive
SHA	Secure Hash Algorithm
SID	Security ID

Section 1 – Module Specification

The CM has one FIPS 140 approved mode of operation and CM is always in approved mode of operation. The CM provides services defined in Section 2.1 and other non-security related services.

Section 1.1 – Product Version

The Toshiba Enterprise SSC Self-Encrypting Hard Disk Drive has been validated:

HW version: A0 with
AL14SEQ18EQB, AL14SEQ12EQB, AL14SEQ09EQB,
AL14SEQ18EPB, AL14SEQ12EPB, AL14SEQ09EPB

FW version: 0101

AL14SEQxxEQB is 512 byte emulation sector drive. AL14SEQxxEPB is 4K sector drive.

Section 2 – Roles Services and Authentication

This section describes roles, authentication method, and strength of authentication.

Role Name	Role Type	Type of Authentication	Authentication	Authentication Strength	Multi Attempt strength
EraseMaster	Crypto Officer	Role	PIN	$1/2^{48} < 1/1{,}000{,}000$	$15{,}000 / 2^{48} < 1 / 100{,}000$
SID	Crypto Officer	Role	PIN	$1/2^{48} < 1/1{,}000{,}000$	$15{,}000 / 2^{48} < 1 / 100{,}000$
BandMaster0	User	Role	PIN	$1/2^{48} < 1/1{,}000{,}000$	$15{,}000 / 2^{48} < 1 / 100{,}000$
BandMaster1	User	Role	PIN	$1/2^{48} < 1/1{,}000{,}000$	$15{,}000 / 2^{48} < 1 / 100{,}000$
…	…	…	…	…	…
BandMaster8	User	Role	PIN	$1/2^{48} < 1/1{,}000{,}000$	$15{,}000 / 2^{48} < 1 / 100{,}000$

Table 2 Identification and Authentication Policy

Per the security policy rules, the minimum PIN length is 6 bytes. Therefore the probability that a random attempt will succeed is $1/2^{48} < 1{,}000{,}000$ (the CM accepts any value (0x00-0xFF) as each byte of PIN). The CM waits 5msec when authentication attempt fails, so the maximum number of authentication attempts is 12,000 times in 1 min. Therefore the probability that random attempts in 1min will succeed is $12{,}000 / 2^{48} < 1 / 100{,}000$.

Section 2.1 – Services

This section describes services which the CM provides.

Service	Description	Role(s)	Keys & CSPs	RWX(Read, Write,eXecute)	Algorithm(CAVP Certification Number)	Method
Band Lock/Unlock	Block or allow read (decrypt) / write (encrypt) of user data in a band. Locking also requires read/write locking to be enabled	BandMaster0 … BandMaster8	N/A	N/A	N/A	SECURITY PROTOCOL IN(TCG Set Method Result)
Cryptographic Erase	Erase user data (in cryptographic means) by changing the data encryption key	EraseMaster	MEK(s) RKey	W X	Hash_DRBG(#895) AES256-CBC(#3537)	SECURITY PROTOCOL IN(TCG Erase Method Result)
Data read/write(decrypt/encrypt)	Encryption / decryption of unlocked user data to/from band	None	MEKs	X	AES256-XTS(#3538)	SCSI READ/WRITE Commands
Firmware Download	Enable / Disable firmware download and load a complete firmware image, and save it. If the code passes "Firmware load test", the device is reset and will run with the new code.	SID	PubKey	X	RSASSA-PKCS#-v1_5(#1818)	SECURITY PROTOCOL IN(TCG Set Method Result), SCSI WRITE BUFFER
RandomNumber generation	Provide a random number generated by the CM	None	Seed	R	Hash_DRBG(#895)	SECURITY PROTOCOL IN(TCG Random Method Result)
Reset(run POSTs)	Runs POSTs and delete CSPs in RAM	None	N/A	N/A	N/A	Power on reset
Set band position and size	Set the location and size of the LBA range	BandMaster0 … BandMaster8	N/A	N/A	N/A	SECURITY PROTOCOL IN(TCG Set Method Result)
Set PIN	Setting PIN (authentication data)	All for their PIN	RKey	X	AES256-CBC(#3537) SHA256(#2916)	SECURITY PROTOCOL IN(TCG Set Method Result)
Show Status	Report status of the CM	None	N/A	N/A	N/A	SCSI REQUEST SENSE
Zeroization	Erase user data in all bands by changing the data encryption key, initialize range settings, and reset PINs for TCG	None[1]	RKey MEKs PIN	X,W W W	AES256-CBC(#3537) Hash_DRBG(#895)	SECURITY PROTOCOL IN(TCG RevertSP Method Result)

Table 3 – FIPS Approved services

Algorithm	CAVP Certification Number
AES256-CBC	#3537
AES256-XTS	#3538
SHA256	#2916
RSASSA-PKCS#1-v1_5	#1818
Hash_DRBG	#895

Table 4 - FIPS Approved Algorithms

Algorithm	Description
NDRNG	Software RNG used to seed the approved Hash_DRBG. Minimum entropy of 8 bits is 7.28.

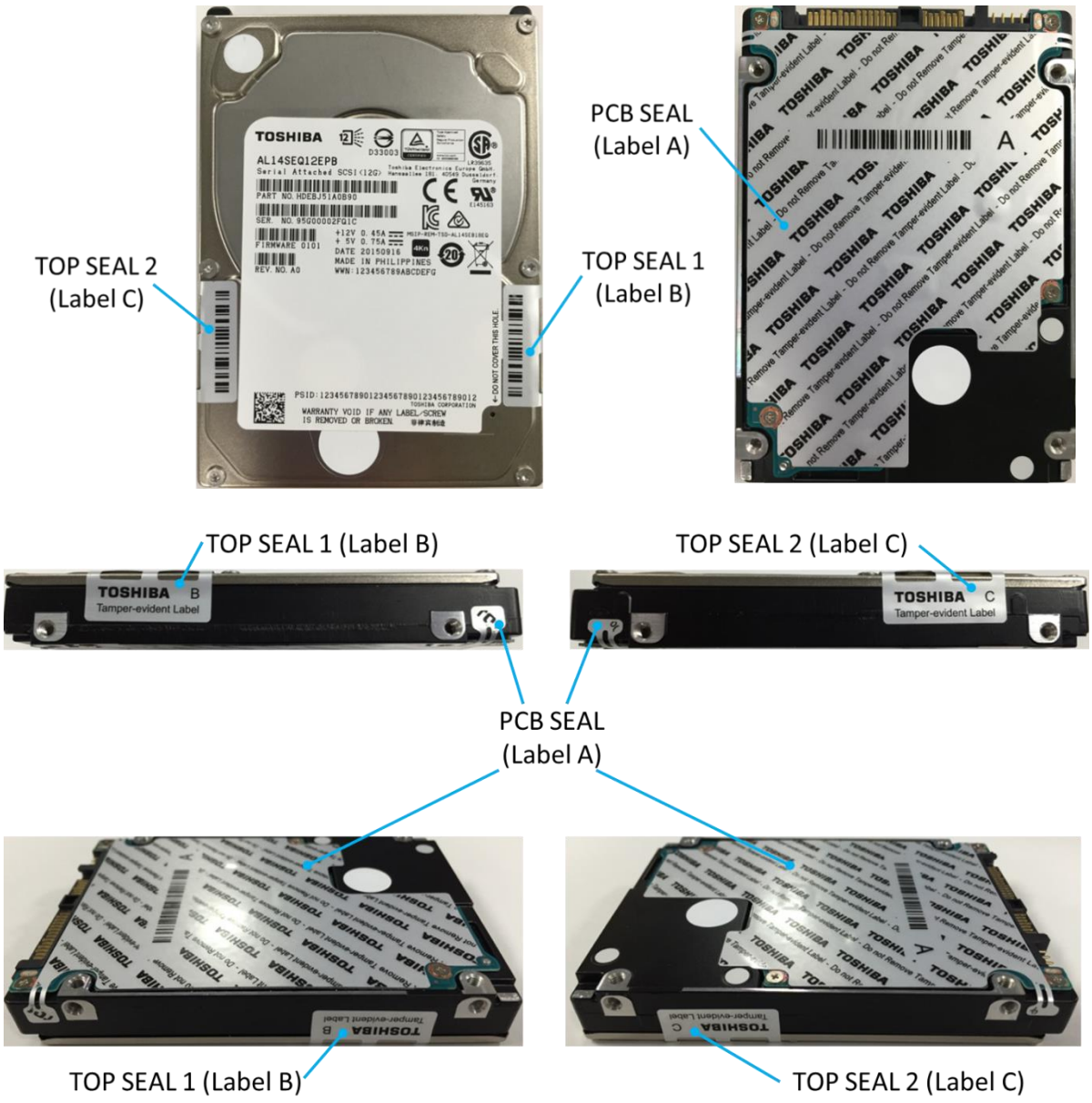
Table 4-1 - Non-FIPS Approved Algorithms

[1] Need to input PSID, which is public drive-unique value used for the TCG RevertSP method.

Section 3 – Physical Security

The CM has the following physical security:

- Production-grade components with standard passivation
- Three tamper-evident security seals are applied to the CM in factory
  - One opaque and tamper-evident security seal (PCB SEAL) is applied to PCB of the CM. This seal prevents an attacker to remove the PCB and survey electronic design
  - Two tamper-evident security seals (TOP SEAL 1 and TOP SEAL 2) are applied to top cover of the CM. These seals prevent top cover removal
- Exterior of the drive is opaque
- The tamper-evident security seals cannot be penetrated or removed and reapplied without tamper-evidence

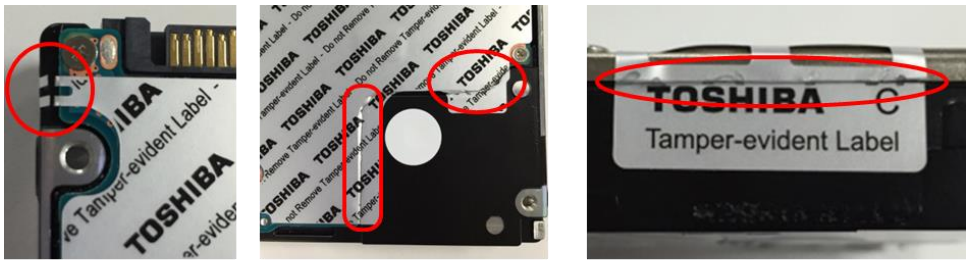


The operator is required to inspect the CM periodically for one or more of the following tamper evidence. If the operator discovers tamper evidence, the CM should be removed.

- Message “VOID” on security seal or top plate
- Text on security seals does not match original
- Cutting line on security seal
- Security seal cutouts do not match original

Mark of alphabetic character(s) which constitute a word "VOID"
(Tamper Evidences of removal)

Mark of alphabetic character(s) which constitute a word "VOID"
(Tamper Evidences of reapplied)



Cutting line (Tamper Evidences of cutting)

Section 4 – Operational Environment

Operational Environment requirements are not applicable because the CM operates in a “non-modifiable”, that is the CM cannot be modified and no code can be added or deleted.

Section 5 – Key Management

The CM uses keys and CSPs in the following table.

Key/CSP	Length	Type	Zeroize Method	Establishment	Output	Persistence/Storage
BandMaster/Erase Master/SID PINs	256	PIN	Zeroization service	Electronic input	No	SHA digest/System Area
MEKs	512	Symmetric	Zeroization service	DRBG	No	Encrypted by RKey / System Area
MSID	256	Public	N/A(Public)	Manufacturing	Output: Host can retrieve	Plain / System Area
PubKey	2048	Public	N/A(Public)	Manufacturing	No	Plain / System Area
RKey	256	Symmetric	Zeroization service	DRBG	No	Obfuscated(Plain in FIPS means) / System Area
Seed	440	DRBG seed	Power-Off	Entropy collected from NDRNG at Power-On	No	Plain/RAM

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

Section 6 – Self Tests

The CM runs self-tests in the following table.

Function	Self-Test Type	Abstract
Firmware Integrity Check	Power-On	EDC 32-bit
FW SHA256	Power-On	Digest KAT
AES(AES CBC)	Power-On	Encrypt and Decrypt KAT
AES(AES XTS)	Power-On	Encrypt and Decrypt KAT
FW Hash_DRBG	Power-On	DRBG KAT
FW RSASSA-PKCS#-v1_5	Power-On	Signature verification KAT
FW Hash_DRBG	Conditional	Verify newly generated random number not equal to previous one
NDRNG	Conditional	Verify newly generated random number not equal to previous one
Firmware load test	Conditional	Verify signature of downloaded firmware image by RSASSA-PKCS#-v1_5

When the CM continuously enters in error state in spite of several trials of reboot, the CM may be sent back to factory to recover from error state.

Section 7 – Design Assurance

Refer to the guidance document provided with the CM.

Section 8 – Mitigation of Other Attacks

The CM does not mitigate other attacks beyond the scope of FIPS 140-2 requirements.