FIPS 140 - 2 Security Policy for:

Toshiba Secure TCG Opal SSC and Wipe technology

Self-Encrypting Drive Series

MQ01ABU050BW, MQ01ABU032BW, and MQ01ABU025BW

TOSHIBA ELECTRONIC DEVICES & STORAGE CORPORATION

Rev 3.1

Overview

The Toshiba Secure TCG Opal SSC and Wipe Technology Self-Encrypting Drive Series (MQ01ABU050BW, MQ01ABU032BW, and MQ01ABU025BW) 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, independently protected user data LBA ranges, host device authentication and secure automatic data invalidation. The last two services are provided by the Toshiba Wipe Technology.

This CM is multiple-chip embedded, and the physical boundary of the CM is the entire HDD. The physical interface for power-supply and for communication is one SATA connector. The CM is connected with host system by this SATA connector. The logical interface is the SATA, TCG SWG, Opal SSC, IEEE1667 (Probe Silo and TCG Storage Silo), and Toshiba Wipe Technology protocol.

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

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. The CM provides services defined in Section 2.1 and other non-security related services. After initial setup steps, this CM is always in approved mode of operation.

Section 1.1 – Product Version

The Toshiba Secure TCG Opal SSC and Wipe technology SED has been validated:

1. MQ01ABU050BW(2.5-inch, SATA Interface, 500GB), HW version: AA, FW version: FN001S, FN002S
2. MQ01ABU032BW(2.5-inch, SATA Interface, 320GB), HW version: AA, FW version: FN001S, FN002S
3. MQ01ABU025BW(2.5-inch, SATA Interface, 250GB), HW version: AA, FW version: FN001S, FN002S

Section 1.2 – Logical to Physical Port Mapping

FIPS140-2 Interface	Module Ports
Data Input	SATA Connector
Data Output	SATA Connector
Control Input	SATA Connector
Status Output	SATA Connector
Power Input	SATA Connector

Section 2 – Roles Services and Authentication

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

Role		Type of Authentication	Authentication	Authentication Strength	Multi Attempt strength
Crypto Officer A (CoLAx)	LockingSP.Admin1	Role	PIN	$1/2^{48} < 1/1{,}000{,}000$	$60{,}000 / 2^{48} < 1 / 100{,}000$
	LockingSP.Admin2	Role	PIN	$1/2^{48} < 1/1{,}000{,}000$	$60{,}000 / 2^{48} < 1 / 100{,}000$
	LockingSP.Admin3	Role	PIN	$1/2^{48} < 1/1{,}000{,}000$	$60{,}000 / 2^{48} < 1 / 100{,}000$
	LockingSP.Admin4	Role	PIN	$1/2^{48} < 1/1{,}000{,}000$	$60{,}000 / 2^{48} < 1 / 100{,}000$
Crypto Officer B(CoAA)	AdminSP.Admin1	Role	PIN	$1/2^{48} < 1/1{,}000{,}000$	$60{,}000 / 2^{48} < 1 / 100{,}000$
Crypto Officer C(CoWA)	Wipe Admin	Role	PIN	$1/2^{48} < 1/1{,}000{,}000$	$60{,}000 / 2^{48} < 1 / 100{,}000$
Crypto Officer D(CoWM)	Wipe Maker	Role	PIN	$1/2^{48} < 1/1{,}000{,}000$	$60{,}000 / 2^{48} < 1 / 100{,}000$
Crypto Officer E(CoLSUx) (*)	LockingSP.User1	Role	PIN	$1/2^{48} < 1/1{,}000{,}000$	$60{,}000 / 2^{48} < 1 / 100{,}000$
	…	…	…	…	…
	LockingSP.User9	Role	PIN	$1/2^{48} < 1/1{,}000{,}000$	$60{,}000 / 2^{48} < 1 / 100{,}000$

User A (ULUx)	LockingSP.User1	Role	PIN	$1/2^{48}$ < 1/1,000,000	60,000 / 2^{48} < 1 / 100,000
	LockingSP.User2	Role	PIN	$1/2^{48}$ < 1/1,000,000	60,000 / 2^{48} < 1 / 100,000
	…	…	…	…	…
	LockingSP.User9	Role	PIN	$1/2^{48}$ < 1/1,000,000	60,000 / 2^{48} < 1 / 100,000
User B(UM)	Master	Role	PIN	$1/2^{48}$ < 1/1,000,000	60,000 / 2^{48} < 1 / 100,000
User C(UU)	User	Role	PIN	$1/2^{48}$ < 1/1,000,000	60,000 / 2^{48} < 1 / 100,000

Table 2 Identification and Authentication Policy

(*)Available only when the CM uses TCG Single User Mode functionality.

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 waits 1msec when authentication attempt fails, so the maximum number of authentication attempts is 60,000 in 1 min. Therefore the probability that random attempts in 1min will succeed is 60,000 / 2^{48} < 1 / 100,000.

Section 2.1 – Services

This section describes services which the CM provides.

The CM supports the Single User Mode functionality defined in the Single User Mode feature set of TCG Opal. The LockingSP.Reactivate or LockingSP.Activate method could enable a single user mode. Authorized roles of some services differ when the CM is in single user mode. About such services, the Role(s) column in table3 is divided into two rows. The upper row shows authorized roles in non-single user mode (normal mode), and the lower row shows authorized roles against range X in single user mode.

Service	Description	Role(s)	Keys & CSPs	RWX(Read/Write/eXecute)	Algorithm (CAVP Certification Number) [JCMVP Algorithm Certification Number]	Method
Cryptographic Erase	Erase user data (in cryptographic means) by changing the data encryption key	UM UU	MEK(s) RKey PIN	W X W	Hash_DRBG (#334)[#5] SHA256 (#2081)[#26] AES256CTR (#2447)[#37]	ATA SECURITY ERASE PREPARE + ATA SECURITY ERASE UNIT
Data read/write (decrypt/encrypt)	Encryption / decryption of unlocked user data to/from range	None	MEK(s)	X	AES256CBC (#2448)[36]	ATA READ,WRITE Commands
Enable/Disable LockingSP Admin/User	Enable/Disable LockingSP Admin/User Authority	CoLAx CoLAx for only Admins (To set for User is impossible)	N/A	N/A	N/A	TRUSTED SEND (TCG Set Method)

Service	Description	Role(s)	Keys & CSPs	RWX(Read/Write/eXecute)	Algorithm (CAVP Certification Number) [JCMVP Algorithm Certification Number]	Method
Host Authentication (Send CHALLENGE)	Send challenge data (optionally encrypted) of wipe challenge and response authentication to a host device	None	Challenge (opt)COKEY RKey	W X X	Hash_DRBG (#334)[#5] AES256CBC (#2447)[#37]	TRUSTED RECEIVE (ADI GetRandomData)
Host Authentication (Verify RESPONSE)	Verify response data of wipe challenge and response authentication to authenticate a host device	None	COKEY Challenge	X/(opt)R R/(opt)X	AES256CBC (#2447)[#37] (opt)HMAC-SHA256 (#1511)[#17]	TRUSTED RECEIVE (ADI SendAuthenticationData)
Random Number generation	Provide a random number generated by the CM	None	seed	X	Hash_DRBG (#334)[#5] SHA256 (#2081)[#26]	TRUSTED RECEIVE (ADI GetRandom) TRUSTED SEND (TCG Random)
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	CoLAx/ULUx (LockingSP is Active) or UU/UM (ATA Security is enable) CoLSUx	N/A	N/A	N/A	-TRUSTED SEND (TCG Set Method) -ATA SECURITY UNLOCK
Reset (run POSTs)	Runs POSTs and delete CSPs in RAM	None	N/A	N/A	N/A	Power on reset
Set range position and size	Set the location and size of the LBA range	CoLAx CoLAx or CoLSUx	N/A	N/A	N/A	TRUSTED SEND (TCG Set Method)
Set PIN	Setting PIN (authentication data)	All role for their PIN CoLAx for CoLSUx's pin (reset) UM for UU's pin (reset)	PIN	W	SHA256 (#2081)[#26] Hash_DRBG (#334)[#5]	・TRUSTED SEND -TCG Set -TCG Reactivate - ADISetPin ・ SECURITY SET PASSWORD ・ SECURITY DISABLE PASSWORD
Set WIPE Mode	Enable/Disable Wipe related services	CoWA	N/A	N/A	N/A	TRUSTED RECEIVE (ADI Set Mode)

Service	Description	Role(s)	Keys & CSPs	RWX(Read/Write/eXecute)	Algorithm (CAVP Certification Number) [JCMVP Algorithm Certification Number]	Method
Show Status	Report status of the CM	None	N/A	N/A	N/A	Read STATUS REGISTER (50/51h)
TCG Activate	Activate LockingSP	AdminSP.SID	MEK(s)(except Global Range) RKey PIN	W X W	Hash_DRBG (#334)[#5] SHA256 (#2081)[#26] AES256CTR (#2447)[#37]	TRUSTED SEND (AdminSP.activate)
TCG Cryptographic Erase (Erase)	Erase user data (in cryptographic means) in an LBA range by changing the data encryption key. User PIN is also reset. This method is available only in single user mode	N/A CoLSUx CoLAx	MEK(s) RKey PIN	W X W	Hash_DRBG (#334)[#5] SHA256 (#2081)[#26] AES256CTR (#2447)[#37]	TRUSTED SEND (TCG Erase)
TCG Cryptographic Erase (GenKey)	Erase user data (in cryptographic means) in an LBA range by changing the data encryption key	CoLAx CoLSUx	MEK(s) RKey	W X	Hash_DRBG (#334)[#5] AES256CTR (#2447)[#37]	TRUSTED SEND (TCG GenKey)
TCG zeroization	Erase user data in all ranges by changing the data encryption key, initialize range settings, and reset PINs for TCG authorities.	CoAA CoLAx AdminSP.PSID (using PSID[1]) AdminSP.SID (using SID)	MEK(s) RKey PIN	W X W	Hash_DRBG (#334)[#5] SHA256 (#2081)[#26] AES256CTR (#2447)[#37]	TRUSTED SEND (- LockingSP.RevertSP - LockingSPObj.Revert - AdminSPObj.Revert)
Wipe Cryptographic Erase	Erase user data in all ranges by changing the data encryption key. Keep range information (PIN and range configuration)	CoWM	RKey MEK(s)	X W	AES256CTR (#2447)[#37] Hash_DRBG (#334)[#5] SHA256 (#2081)[#26]	TRUSTED SEND (ADI Invalidate)
Zeroization	Initialize the CM by zeroize a root key (RKey), all PINs, data encryption keys, and range configuration	CoWM CoWA	RKey MEK(s) COKEY PIN	X,W W W W	AES256CTR (#2447)[#37] SHA256 (#2081)[#26] Hash_DRBG (#334)[#5]	TRUSTED SEND (ADI Exit)

Table 3 – FIPS Approved services

[1] PSID (Printed SID) is public drive-unique value which is used for the TCG Revert AdminSP method.

Algorithm	Certification Number	
	CAVP	JCMVP Algorithm
AES256CBC (HW)	#2448	#36
AES256CBC (FW)	#2447	#37
AES256CTR (FW)	#2447	#37
SHA256 (FW)	#2081	#26
HMAC (FW)	#1511	#17
Hash_DRBG (FW)	#334	#5

Table 4 - FIPS Approved Algorithms

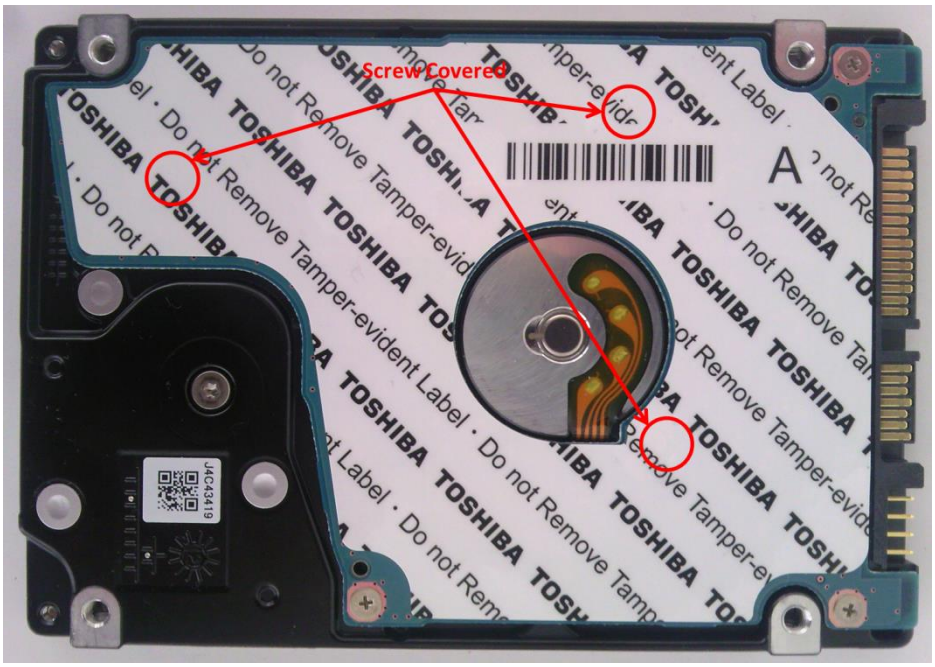
Algorithm	Description
NDRNG	Software RNG used to seed the approved Hash_DRBG. Minimum entropy of 8 bits is 6.70.

Table 4-1 - Non-FIPS Approved Algorithms

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 B and TOP SEAL C) 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



PCB SEAL

TOP SEAL B TOP SEAL C

OVERVIEW OF TOP COVER

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.

- Checkerboard pattern on security seal or top plate
- Text on security seals does not match original
- A scratch on security seals covered screws
- Security seal cutouts do not match original

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(bit)	Type	Zeroize Method	Establishment	Output	Persistence/Storage
Authority PINs(*)	256	PIN	N/A(Hashed)	Electronic input	No	SHA digest/System Area
COKEY	256*2	Symmetric	N/A(Encrypted)	Electronic input	No	Encrypted by RKey / System Area
Challenge	256	Challenge for authentication	Power-Off	RNG	Yes	Encrypted by COKEY / RAM
MEKs	256	Symmetric	N/A(Encrypted)	RNG	No	Encrypted by RKey / System Area
MSID	256	Public value	N/A(Public)	Manufacturing	Yes: Host can retrieve	Plain / System Area
RKey	256	Symmetric	Zeroization service	RNG	No	Plain / System Area
Seed	440	RNG seed	Every time after used	Collected at every random number generation	No	Plain/RAM

(*)PINs for User / Master / AdminSP.Admin1 / LockingSP.Admin1 - 4 / LockingSP.User1-User9 / WIPE Maker / WIPE Admin

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
FW HMAC SHA256	Power-On	Digest KAT
AES(AES CBC)	Power-On	Encrypt and Decrypt KAT
FW AES(AES CBC)	Power-On	Encrypt and Decrypt KAT

FW AES(AES CTR)	Power-On	Encrypt and Decrypt KAT
FW Hash_DRBG	Power-On	DRBG 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

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.