

FIPS 140 - 2 Non-Proprietary Security Policy for:

Toshiba TCG Enterprise SSC Self-Encrypting Solid State Drive
(THNSB8 model)



TOSHIBA CORPORATION

Rev 1.0.3

TOSHIBA

OVERVIEW	3
ACRONYMS	3
SECTION 1 – MODULE SPECIFICATION.....	5
SECTION 1.1 – PRODUCT VERSION	5
SECTION 2 – ROLES SERVICES AND AUTHENTICATION.....	5
SECTION 2.1 – SERVICES	6
SECTION 3 – PHYSICAL SECURITY	8
SECTION 4 – OPERATIONAL ENVIRONMENT.....	9
SECTION 5 – KEY MANAGEMENT.....	10
SECTION 6 – SELF TESTS.....	10
SECTION 7 – DESIGN ASSURANCE.....	11
SECTION 8 – MITIGATION OF OTHER ATTACKS.....	11
APPENDIX A – EMI/EMC	11

TOSHIBA

Overview

The Toshiba TCG Enterprise SSC Self-Encrypting Solid State Drive (listed in Section 1.1 Product Version) is used for solid state 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 multiple-chip embedded, and the physical boundary of the CM is the entire SSD. The logical boundary is SATA interface (same as the physical boundary). The physical interface for power-supply and for communication is one SATA connector. The CM is connected with host system by SATA cable. The logical interface is the SATA, 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.

The CM is intended to meet the requirements of FIPS140-2 Security Level 2 Overall. The Table below shows the security level detail.

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	SATA connector
Control Input	SATA connector
Data Output	SATA connector
Status Output	SATA connector
Power Input	Power connector

Table 1-1 - Physical/Logical Port Mapping

This document is non-proprietary and may be reproduced in its original entirety.

Acronyms

AES	Advanced Encryption Standard
CM	Cryptographic Module
CSP	Critical Security Parameter
DRBG	Deterministic Random Bit Generator

TOSHIBA

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

TOSHIBA

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 following models are validated with the following FW version and HW version:

HW version: A0 with THNSB8480PCSE

A0 with THNSB8800PCSE

A0 with THNSB8960PCSE

A0 with THNSB81Q60CSE

A0 with THNSB81Q92CSE

FW version: 8EEF7101

“xxxx” in “THNSB8xxxxCSE” expresses the device capacity.

THNSB8480PCSE: 480GBytes, THNSB81Q60CSE: 1.60TBytes

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	$1/2^{48} < 1/1,000,000$	$15,000 / 2^{48} < 1 / 100,000$
Master	User	Role	PIN	$1/2^{48} < 1/1,000,000$	$15,000 / 2^{48} < 1 / 100,000$
User	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 $1/2^{48} < 1/1,000,000$ (the CM accepts any value (0x00-0xFF) as each byte of PIN). The CM waits 4msec when authentication attempt fails, so the maximum number of authentication attempts is 15,000 times in 1 min. Therefore the probability that random attempts in 1min will succeed is $15,000 / 2^{48} < 1 / 100,000$. Even if TryLimit¹ is infinite, the probability that random attempts is same.

¹ TryLimit is the upper limit of failure of authentication of each role.

TOSHIBA

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 (LockingSP is active)	BandMaster0 ... BandMaster8	Table MAC Key	X	HMAC-SHA256 (#2543)	-TRUSTED SEND (TCG Set Method Result)
Lock/Unlock	Block or allow read (decrypt) / write (encrypt) of user data. Unlocking also requires read/write unlocking to be enabled. User data locked in Power On Reset when set User PIN. (ATA Security is enable)	Master ² User	N/A	N/A	N/A	-ATA SECURITY UNLOCK
Cryptographic Erase	Erase user data (in cryptographic means) by changing the data encryption key	EraseMaster	MEK(s) RKey Table MAC Key PIN	W X X W	Hash_DRBG(#1127) AES256-CBC(#3900) HMAC-SHA256 (#2543)	-TRUSTED SEND (TCG Erase Method Result),
Data read/write(decrypt/encrypt)	Encryption / decryption of unlocked user data to/from band	None ³	MEKs	X	AES256-XTS(#3899)	-ATA 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 Master ² User	PubKey Table MAC Key (Only TCG)	X X	RSASSA-PKCS #1-v1_5(#1998) HMAC-SHA256 (#2543)	-TRUSTED SEND (TCG Set Method Result), -ATA DOWNLOAD MICROCODE(DMA) -ATA SECURITY UNLOCK
RandomNumber generation	Provide a random number generated by the CM	None ⁴	Seed	R	Hash_DRBG(#1127)	-TRUSTED SEND (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	Table MAC Key	X	HMAC-SHA256 (#2543)	-TRUSTED SEND (TCG Set Method Result)
Set PIN	Setting PIN (authentication data)	EraseMaster, SID, BandMaster0 ... BandMaster8, Master, User ⁵	RKey Table MAC Key PIN	X X W	AES256-CBC(#3900) HMAC-SHA256 (#2543) SHA256(#3213)	-TRUSTED SEND (TCG Set Method Result) -ATA SECURITY SET PASSWORD
Show Status	Report status of the CM	None	N/A	N/A	N/A	Read STATUS REGISTER (50/51h)
Zeroization	Erase user data in all bands by changing the data encryption key, initialize range settings, and reset PINs for TCG	None ⁶	MEKs RKey Table MAC Key PIN	W X,W X,W W	Hash_DRBG(#1127) AES256-CBC(#3900) HMAC-SHA256 (#2543)	-TRUSTED SEND (TCG RevertSP Method Result)
Zeroization with Authentication	Erase user data by changing the data encryption key and reset Master/User PINs, after authenticated by Master or User	Master User	MEKs RKey Table MAC Key	W X X,W	Hash_DRBG(#1127) AES256-CBC(#3900) HMAC-SHA256 (#2543)	-ATA SECURITY ERASE PREPARE + ATA SECURITY ERASE UNIT

² When Master is set in “High” by User.

³ The band has to be unlocked by corresponding BandMaster beforehand.

⁴ Except Master and User.

⁵ For PIN of themselves.

⁶ Need to input PSID, which is public drive-unique value used for the TCG RevertSP method. The PSID is printed on identification label of the module.

			PIN	W		
--	--	--	-----	---	--	--

Table 3 - FIPS Approved services

Algorithm	CAVP Certification Number
AES256-CBC	#3900
AES256-XTS	#3899
Firmware SHA256	#3213
Hardware SHA256	#3308
Firmware HMAC-SHA256	#2543
Hardware HMAC-SHA256	#2625
RSASSA-PKCS#1-v1_5	#1998
Hash_DRBG	#1127

Table 4 - FIPS Approved Algorithms

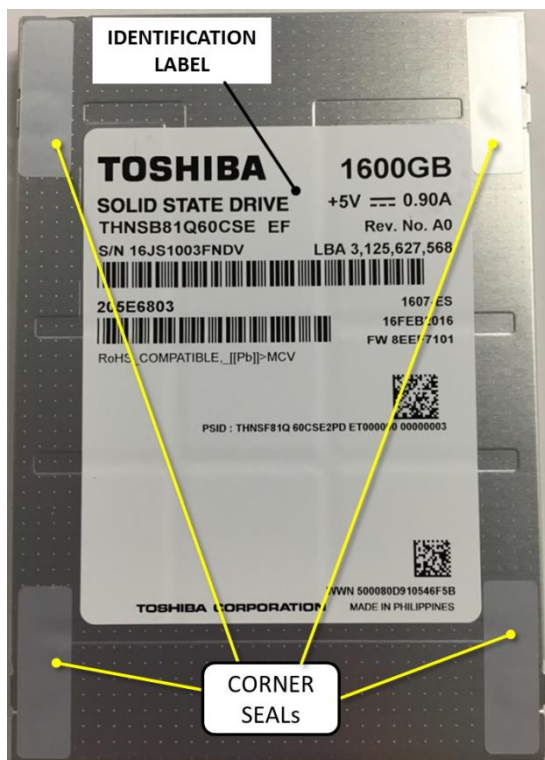
Algorithm	Description
NDRNG	Hardware RNG used to seed the approved Hash_DRBG. Minimum entropy of 8 bits is 7.58.

Table 4-1 - Non-FIPS Approved Algorithms

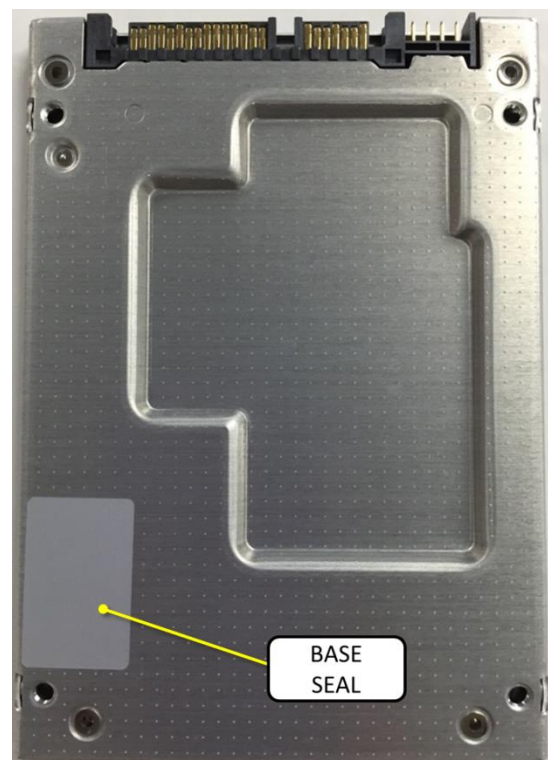
Section 3 – Physical Security

The CM has the following physical security:

- Production-grade components with standard passivation
- Exterior of the drive is opaque
- Five tamper-evident security seals are applied to the CM in factory
 - Four opaque and tamper-evident security seals (CORNER SEALS) are applied to top cover of the CM. These seals prevent top cover removal.
 - One opaque and tamper-evident security seal (BASE SEAL) are applied to base plate of the CM. This seal prevents an attacker to access the PCB.
- The tamper-evident security seals cannot be penetrated or removed and reapplied without tamper-evidence



Top cover side



Base plate side



CORNER SEAL

BASE SEAL

The operator is required to inspect the CM periodically (every month or every two months) 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 the CM
- A scratch on security seals covered screws
- Security seal cutouts do not match original



CORNER SEAL

BASE SEAL

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.

TOSHIBA

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
Master/User PINs			Zeroization with Authentication service			
MEKs	512	Symmetric	Zeroization service Zeroization with Authentication 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 instantiation (Minimum entropy of 8 bits: 7.58)	No	Plain/RAM
Table MAC Key	256	HMAC Key	Zeroization service Zeroization with Authentication service	DRBG	No	Encrypted by RKey / System Area

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	Failure Behavior
Firmware Integrity Check	Power-On	HMAC 256bit	Enters Boot Error State.
SHA256(F.E CPU)	Power-On	Digest KAT	Enters Boot Error State.
HMAC-SHA256(F.E CPU)	Power-On	Digest KAT	Enters Boot Error State.
AES256-CBC (F.E CPU)	Power-On	Encrypt and Decrypt KAT	Enters Boot Error State.
AES256-XTS	Power-On	Encrypt and Decrypt KAT	Enters Boot Error State.
Hash_DRBG	Power-On	DRBG KAT	Enters Boot Error State.
RSASSA-PKCS#1-v1_5	Power-On	Signature verification KAT	Enters Boot Error State.
Hash_DRBG	Conditional	Verify newly generated random number not equal to previous one	Enters Error State.
NDRNG	Conditional	Verify newly generated random	Enters Error State.

TOSHIBA

		number not equal to previous one	
Firmware load test	Conditional	Verify signature of downloaded firmware image by RSASSA-PKCS#1-v1_5, and run firmware integrity check	Incoming firmware image is not loaded and is not saved.

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.

Appendix A – EMI/EMC

FIPS 140-2 requires the Federal Communications Commission (FCC) ID, but this CM does not have FCC ID. Because this CM is a device described in Subpart B, Class A of FCC 47 Code of Federal Regulations Part 15. However, all systems using this CM and sold in the United States must meet these applicable FCC requirements.