# TOSHIBA

FIPS 140‐2 Non‐Proprietary Security Policy for:

# Toshiba TCG Enterprise SSC Self‐Encrypting Solid State Drive (PX04S model) Type B



TOSHIBA CORPORATION

Rev 1.1.0

# TOSHIBA

**TOSHIBA**

### Overview

The Toshiba TCG Enterprise SSC Self-Encrypting Solid State Drive (listed in Section1.1 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 SAS interface (same as the physical boundary). The physical interface for power-supply and for 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.

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 | 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

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 PX04SVQ080B, PX04SVQ160B
FW version: ZW00

## 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 $1/2^{48} < 1/1,000,000$ (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 TryLimit[1] is infinite, the probability that random attempts is same.

---

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

### 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 | Table MAC Key | X | HMAC-SHA256 (#2231) | 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 Table MAC Key | W X X | Hash_DRBG(#867) AES256-CBC(#3485) HMAC-SHA256 (#2231) | 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-R( #3487) AES256-XTS-W (#3486) | 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 Table MAC Key | X X | RSASSA-PKCS #1-v1_5(#1795) HMAC-SHA256 (#2231) | 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(#867) | 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 | Table MAC Key | X | HMAC-SHA256 (#2231) | SECURITY PROTOCOL IN(TCG Set Method Result) |
| Set PIN | Setting PIN (authentication data) | All for their PIN | RKey Table MAC Key | X X | AES256-CBC(#3485) HMAC-SHA256 (#2231) SHA256(#2879) | 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[2] | RKey Table MAC KEY MEKs PIN | X,W X,W W W | AES256-CBC(#3485) HMAC-SHA256 (#2231) Hash_DRBG(#867) | SECURITY PROTOCOL IN(TCG RevertSP Method Result) |

Table 3 - FIPS Approved services

| Algorithm | CAVP Certification Number |
|---|---|
| AES256-CBC | #3485 |
| AES256-XTS-R | #3487 |
| AES256-XTS-W | #3486 |
| SHA256 (SEC CPU) | #2879 |
| HMAC-SHA256 (SEC CPU) | #2231 |
| RSASSA-PKCS#1-v1_5 | #1795 |
| Hash_DRBG | #867 |

Table 4 - FIPS Approved Algorithms

---

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

| Algorithm | Description |
|-----------|-------------|
| NDRNG | Hardware RNG used to seed the approved Hash_DRBG. Minimum entropy of 8 bits is 7.53. |

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
  - Three opaque and tamper-evident security seals (VOID LABEL H, VOID LABEL J and VOID LABEL K) are applied to side of the CM and edge of OUTER SHEET[3]. These seals prevent cover removal and an attacker to access the PCB
  - Two opaque and tamper-evident security seals (VOID LABEL F and VOID LABEL G) are applied to side of the CM. These seals prevent cover removal
- The tamper-evident security seals cannot be penetrated or removed and reapplied without tamper-evidence



---
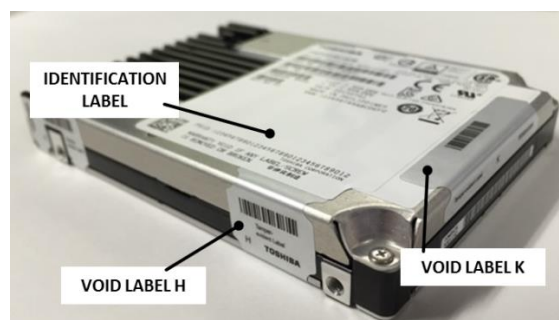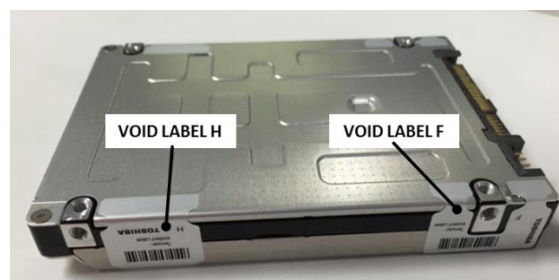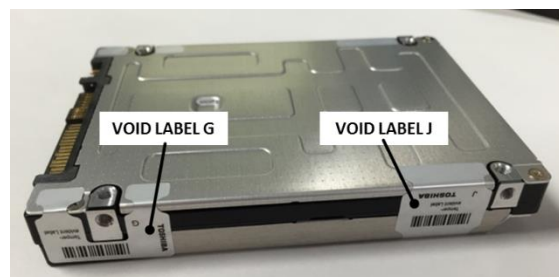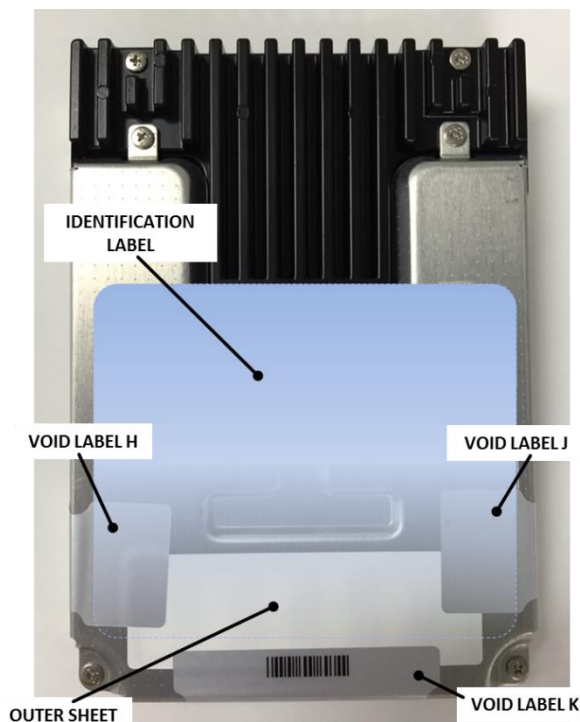
[3] OUTER SHEET is an opaque seal covering some holes of the top cover. It cannot leave "VOID" message, but leaves the evidence of the cut.

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
- Text on security seals do not match original
- Cutting line on security seal or OUTER SHEET
- Security seal cutouts do not match original



**Mark of alphabetic character(s) which constitute a word "VOID"**



**Cutting line (Security seals and OUTER SHEET)**

### 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 instantiation (Minimum entropy of 8 bits: 7.53) | No | Plain/RAM |
| Table MAC Key | 256 | HMAC Key | Zeroization 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 |
|---|---|---|
| Firmware Integrity Check | Power-On | EDC 32-bit |
| SHA256 (F.E CPU) | Power-On | Digest KAT |
| SHA256 (SEC CPU) | Power-On | Digest KAT |
| HMAC-SHA256 (F.E CPU) | Power-On | Digest KAT |
| HMAC-SHA256 (SEC CPU) | Power-On | Digest KAT |
| AES256-CBC | Power-On | Encrypt and Decrypt KAT |
| AES256-XTS-R | Power-On | Decrypt KAT |
| AES256-XTS-W | Power-On | Encrypt KAT |
| Hash_DRBG | Power-On | DRBG KAT |
| RSASSA-PKCS#1-v1_5 | Power-On | Signature verification KAT |
| 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#1-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

Initial operations to setup this module are following:

1. Get MSID from SAS interface.

2. Set range configurations with BandMaster(s) authority by using MSID as PIN.

3. Change BandMaster(s)/EraseMaster/SID PINs.

4. Set PortLocked in Download port to "TRUE".


To get more details, 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

This CM is a "Class B" device and was tested and verified to conform to the EMI/EMC requirements found in the following regulation:

- FCC Subpart 15B