

FIPS 140 - 2 Security Policy for:

Toshiba TCG Enterprise SSC Self-Encrypting Solid State Drive  
(PX model NA02)



TOSHIBA CORPORATION

Rev 2.0

# TOSHIBA

---

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

# 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 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.

| 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      |
| <b>Overall Level</b>                         | <b>2</b> |

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 |
| EDC  | Error Detection Code               |
| FW   | Firmware                           |

# TOSHIBA

---

|       |   |
|-------|---|
| 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 Solid State Drive has been validated:

HW version: A0 with PX02SMU020, PX02SMU040, PX02SMU080, or PX02SMQ160

FW version: NA02, NA04

The PX02SMU080 with NA02 and NA04 varies “Product ID” value of INQUIRY command according to customer requirements. These “Product ID” values are X440\_PHM2800MCTO and X577\_PHM2800MCTO.

## 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

# TOSHIBA

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  $15,000 / 2^{48} < 1 / 100,000$ .

## 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 (#1611)  | SECURITY PROTOCOL IN(TCG Set Method Result)      |
| Cryptographic Erase              | Erase user data (in cryptographic means) by changing the data encryption key   | EraseMaster                            | MEK(s)<br>RKey<br>Table MAC Key      | W<br>X<br>X             | Hash_DRBG(#397)<br>AES256CBC(#2598)<br>HMAC-SHA256 (#1611) | SECURITY PROTOCOL IN(TCG Erase Method Result)    |
| Data read/write(decrypt/encrypt) | Encryption / decryption of unlocked user data to/from band   | None                                   | MEKs                                 | X                       | XTS-AES256(#2598)  | SCSI READ/WRITE Commands                         |
| Download Port Lock/Unlock        | Enable / Disable Firmware Download service   | SID                                    | Table MAC Key                        | X                       | HMAC-SHA256 (#1611)  | SECURITY PROTOCOL IN(TCG Set Method Result)      |
| Firmware Download                | Load complete firmware image. The device is reset and will run with the new code   | None                                   | PubKey                               | X                       | RSASSA-PKCS-v1_5(#1331)                                    | SCSI WRITE BUFFER                                |
| RandomNumber generation          | Provide a random number generated by the CM  | None                                   | Seed                                 | R                       | Hash_DRBG(#397)  | 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 (#1611)  | SECURITY PROTOCOL IN(TCG Set Method Result)      |
| Set PIN                          | Setting PIN (authentication data)  | All for their PIN                      | RKey<br>Table MAC Key                | X<br>X                  | AES256CBC(#2598)<br>HMAC-SHA256 (#1611)<br>SHA256(#2183)   | 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            | AdminSP.PSID(using PSID <sup>1</sup> ) | RKey<br>Table MAC KEY<br>MEKs<br>PIN | X,W<br>X<br>W<br>W      | AES256CBC(#2598)<br>HMAC-SHA256 (#1611)<br>Hash_DRBG(#397) | SECURITY PROTOCOL IN(TCG RevertSP Method Result) |

**Table 3 - FIPS Approved services**

| Algorithm        | CAVP Certification Number |
|------------------|---------------------------|
| AES256CBC        | #2598                     |
| XTS-AES256       | #2598                     |
| SHA256           | #2183                     |
| HMAC-SHA256      | #1611                     |
| RSASSA-PKCS-v1_5 | #1331                     |
| Hash_DRBG        | #397                      |

<sup>1</sup> PSID (Printed SID) is public drive-unique value which is used for the TCG Revert AdminSP method.

### Section 3 – Physical Security

The CM has the following physical security:

- Production-grade components with standard passivation
- Exterior of the drive is opaque
- In PX02SMU020/040/080 : Four tamper-evident security seals (CORNER SEAL A, CORNER SEAL B, CORNER SEAL C, and CORNER SEAL D) are applied to the CM in factory. These opaque and tamper-evident security seals are applied to top cover of the CM. These seals prevent top cover removal
- In PX02SMQ160: Three tamper-evident security seals are applied to the CM in factory
  - One opaque and tamper-evident security seal (BASE SEAL) is applied to base of the CM. This seal prevents an attacker to access the PCB
  - Two opaque and tamper-evident security seals (SIDE SEAL A and SIDE SEAL B) is 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



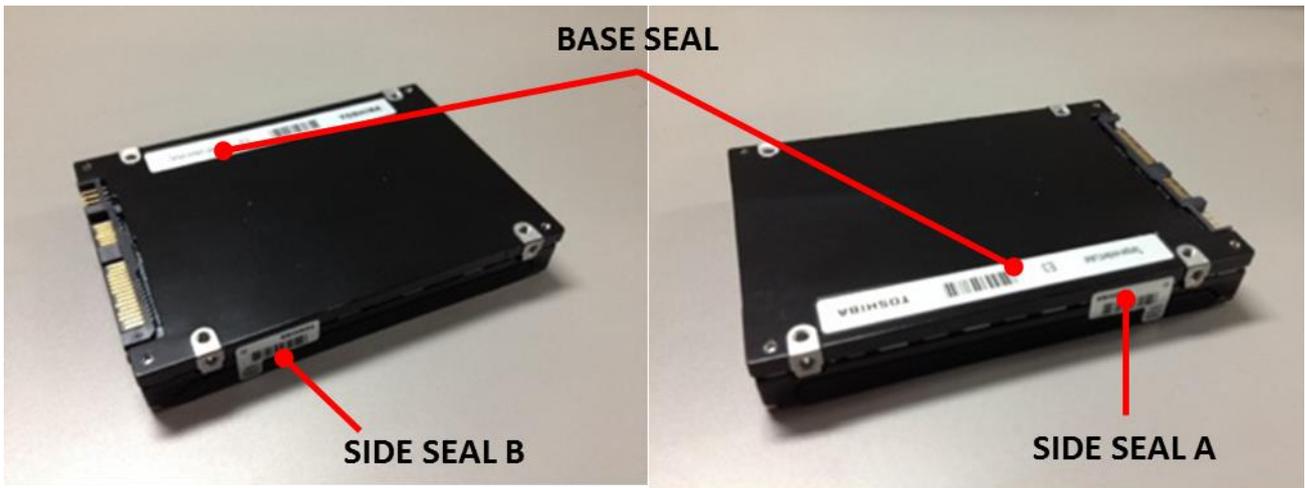


OVERVIEW OF TOP COVER  
(PX02SMU020/040/080)



SIDE SEAL A      SIDE SEAL B  
(PX02SMQ160)

# TOSHIBA



OVERVIEW OF BASE  
(PX02SMQ160)

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 enclosure
- 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.

# TOSHIBA

| Key/CSP                             | Length | Type      | Zeroize Method      | Establishment                                       | Output                       | Persistence/Storage                              |
|-------------------------------------|--------|-----------|---------------------|---|------------------------------|--|
| BandMaster/Erase<br>Master/SID PINs | 256    | PIN       | Zeroization service | Electronic input                                    | No                           | SHA digest/System Area                           |
| MEKs                                | 512    | Symmetric | Zeroization service | DRBG  | No                           | Encrypted by RKey /<br>System Area               |
| MSID                                | 256    | Public    | N/A(Public)         | Manufacturing                                       | Output: Host can<br>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<br>means) / System Area |
| Seed                                | 440    | DRBG seed | Power-Off           | Entropy collected<br>from NDRNG at<br>instantiation | No                           | Plain/RAM  |
| Table MAC Key                       | 256    | HMAC Key  | Zeroization service | DRBG  | No                           | Encrypted by RKey /<br>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                   | Power-On       | Digest KAT   |
| FW HMAC 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 |

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 authority by using MSID as PIN.

3. Change BandMaster(s)/EraseMaster PINs.

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.