# iStorage Ltd.
# iStorage datAshur PRO$^2$ Level 3 Secure Storage Drive

FIPS 140-2 Non-Proprietary Security Policy

Document Version *1.4*

## TABLE OF CONTENTS

# INTRODUCTION

The iStorage datAshur PRO$^2$ Level 3 Secure Storage Drive (datAshur PRO$^2$) is an encrypted storage device that provides a secure way to store and transfer data. User authentication is self-contained via an on-board keypad. User data is protected by hardware-based 256-bit AES encryption to secure sensitive information in the event that the drive is lost or stolen.

The data encryption key (DEK) and other cryptographic parameters are generated within the module through a NIST approved DRBG (ref: SP 800-90A). The seed for the DRBG is also produced within the module from a hardware-based entropy generator.

**Table 1 - All iStorage datAshur PRO$^2$ Level 3 Versions**

| Capacity | Hardware Version | EC Firmware Version | SC Firmware Version |
|---|---|---|---|
| 4 GB | IS-FL-DP2-256-4 | IS_EC_FW_505_1X | 2.5 |
| 8 GB | IS-FL-DP2-256-8 | | |
| 16 GB | IS-FL-DP2-256-16 | | |
| 32 GB | IS-FL-DP2-256-32 | | |
| 64 GB | IS-FL-DP2-256-64 | | |
| 128 GB | IS-FL-DP2-256-128 | | |
| 256 GB | IS-FL-DP2-256-256 | | |
| 512 GB | IS-FL-DP2-256-512 | | |

# 1. CRYPTOGRAPHIC MODULE SPECIFICATION

## 1.1 Security Level

The module meets the overall requirements of FIPS 140-2 Level 3.

**Table 2 - Module Security Level**

| FIPS Area | FIPS Security Requirement | Level |
|---|---|---|
| 1 | Cryptographic Module Specification | 3 |
| 2 | Module Ports and Interfaces | 3 |
| 3 | Roles, Services, and Authentication | 3 |
| 4 | Finite State Model | 3 |
| 5 | Physical Security | 3 |
| 6 | Operational Environment | N/A |
| 7 | Cryptographic Key Management | 3 |
| 8 | EMI/EMC | 3 |
| 9 | Self-Tests | 3 |

|  |  |  |
|---|---|---|
| 10 | Design Assurance | 3 |
| 11 | Mitigation of Other Attacks | N/A |

## 1.2 Modes of Operation

The iStorage datAshur PRO$^2$ Module operates only in a FIPS Approved mode. There does not exist a non-Approved mode of operation. The module indicates that it is in an approved mode of operation by displaying a solid red LED.

## 1.3 Specifications

The datAshur PRO$^2$ is a multi-chip standalone cryptographic module as defined by FIPS 140-2. It consists of a USB 3.0 capable encryption controller, eMMC memory, a security controller, a non-replaceable battery, a keypad controller, a 5V DC Input, and a user interface with three (3) LED status indicators and a user-interface alphanumeric keypad with twelve (12) buttons. The module is encapsulated within an opaque, production grade integrated circuit package. The security components are protected by epoxy against physical tamper attacks. The cryptographic boundary is defined by the datAshur PRO$^2$ entire device, which contains all the components.

# 2. MODULE PORTS AND INTERFACES

The cryptographic module exposes the following physical ports and logical interfaces:

**Table 3 - Physical Ports and Logical Interfaces**

| Physical Port | Logical Interface | Description |
|---|---|---|
| USB Port | Data input<br>Data output<br>Control input<br>Status output | The USB port connects the module to the host computer and is used to exchange decrypted user data as well as control and status information for the USB protocol. There is no direct connection between the USB port and the security controller. |
|  | External power | The USB VBUS (+5) charges the battery and will power the module when it is available. |
| Alphanumeric Keypad (0-9) | Data input | The ten (10) alphanumeric labelled keypad buttons, connected to keypad controller button inputs, are used to enter User PINs. |
| Key and Shift Buttons | Control input | The two (2) buttons are connected to the keypad controller button inputs, and are used to control UI flow, including selecting the role. The Key button is also used to awaken the module from idle state. |
| Red, Green and Blue LEDs | Status output | Refer to Table 4. |
|  |  |  |

Table 4 - LED Status Output

| LED Behaviour | Module State | Status Description |
|---|---|---|
| LEDs off | Locked | The module is in idle state requiring wake by connecting to a powered USB port or pressing SHIFT button. |
| Red LED solid | Locked | Standby State. Waiting for keypad commands to start Admin or User PIN entry process. |
| Red LED solid | Reset | Reset State. Waiting for setting up an Administrative User PIN. |
| GREEN and BLUE LEDs blinking together | Locked | Waiting for Admin PIN entry. |
| All three LEDs solid | Locked | Waiting for obtaining additional 3 Admin PIN attempts |
| All three LEDs blink alternately when pressing KEY button | Locked | Waiting for obtaining additional 2 Admin PIN attempts |
| GREEN and RED LEDs blinking together | Locked | Waiting for OTR PIN entry. |
| All three LEDs blink simultaneously | Locked | Waiting for Standard User/Self-destruct PIN to unlock. Administrative User PIN is set. |
| RED and GREEN solid | Locked | Initial Shipment. Waiting for configuration of an Admin PIN |
| Red Green and Blue blink alternatively when pressing "0" button | Locked | Factory reset is initiated. Module waiting for confirmation code. |
| Blue LED solid | Locked | Administrative User Mode. Ready to accept Administrator commands. |
| The LEDs illuminate alternately from Red to Green and then to Blue, followed by Red LED blinking two seconds, same pattern repeats | Failed | SC KATs fail |
| A faded illumination of Red and Blue LEDs | Failed | SC Firmware Integrity Test fail |
| The LEDs illuminate alternately from Red to Green to Blue, then the flashing Green LED, same pattern repeats | Failed | NDRNG tests fail |
| Green LED blinks constantly when a valid Admin PIN is entered and the device is not connected to a powered USB port | Unlocked | Unlocked by a valid Admin PIN and not connected to a powered USB port. |
| Green LED blinking quickly | Locked | Adding Standard User/Self-Destruct PINs in progress |
| Blue LED blinking quickly | Locked | Adding Administrative User PIN in progress |

| LED Behaviour | Module State | Status Description |
|---|---|---|
| Blue LED solid and Green Blinking | Locked | Ready to accept new PIN. |
| Green and Blue LEDs blink alternately | Locked | Unlocking in progress |
| Green LED solid | Unlocked | Unlocked and connected. No communication or data transfer or via USB |
| Green LED blinks | Unlocked | Unlocked. Communicating or transferring data in progress |
| RED blinks 3 times and off | Locked | Low Battery Level. Charge on a powered USB port for 15-30 minutes |
| RED - Fade Out | Locked | Device turning off to the Idle State |
| BLUE blinking every 5 seconds | Locked | Battery starts charging after 30 seconds when device is locked and connected to a USB port |

# 3. ROLES, SERVICES, AND AUTHENTICATION

## 3.1 Roles and Services

The iStorage datAshur PRO$^2$ supports three distinct and separate identities and roles: Standard User, Administrative User, and OTR User. All three users can access the private partition and user data stored in the device when they are authenticated successfully.

The role is explicitly selected during authentication (refer to Table 6).

Table 5 defines all services and operations that can be performed by the datAshur PRO$^2$ module. CSP access refers to CSP access by the module, not the operator. No CSPs are output by the module.

**Table 5 - Services Authorized for Each Role**

| Operator | Services | Accessible CSP | CSP Access by Module |
|---|---|---|---|
| Standard User Role | Open private partition for read/write access of user data | Standard User PIN<br>Standard User KEK<br>Standard User PBKDF SALT<br>DEK | READ |
| | Read or write private partition with user data | | |
| | Configure the partition as write-protect | | |
| | Check Firmware Version | | |

| Operator | Services | Accessible CSP | CSP Access by Module |
|---|---|---|---|
| | Change User PIN | Standard User PIN<br>SP 800-90A state variables<br>Standard User KEK<br>Standard User PBKDF SALT<br>DEK | READ/WRITE |
| | Lock private partition to prevent read/write access to user data | N/A | N/A |
| Administrative User Role | Open private partition for read/write access of user data | Administrative User PIN<br>Administrative User KEK<br>Administrative User PBKDF SALT<br>DEK | READ |
| | Read or write private partition with user data | | |
| | Configure the partition as write-protect | | |
| | Check Firmware Version | | |
| | Set unattended auto-lock time | | |
| | Check unattended auto-lock time | | |
| | Set User PIN policy | | |
| | Check User PIN policy | | |
| | Set User PIN Brute Force Limitation | | |
| | Check User PIN Brute Force Limitation | | |
| | Configure datAshur PRO$^2$ as Bootable | | |
| | Disable the datAshur PRO$^2$ Bootable feature | | |
| | Check the Bootable setting | | |
| | Change Admin/User/SD/OTR PIN | Standard User PIN<br>Administrative User PIN<br>SD PIN | READ/WRITE |

| Operator | Services | Accessible CSP | CSP Access by Module |
|---|---|---|---|
|  | Add User/SD/OTR PIN | OTR PIN<br>SP 800-90A state variables<br>Standard User KEK<br>Standard User PBKDF SALT<br>Administrative User KEK<br>Administrative User PBKDF SALT<br>SD KEK<br>SD PBKDF SALT<br>OTR KEK<br>OTR PBKDF SALT<br>DEK |  |
|  | Delete User/SD/OTR PIN |  |  |
|  | Lock private partition to prevent read/write access to user data | N/A | N/A |
| OTR User | One-time recovery | OTR PIN<br>OTR KEK<br>OTR PBKDF SALT<br>SP 800-90A state variables<br>Standard User PIN<br>Standard User KEK<br>Standard User PBKDF SALT | READ/WRITE |
|  |  | DEK | READ |
| Unauthenticated Services (no authenticated role required) | Show locked/unlocked status | N/A | N/A |
|  | Show whether an Administrative User PIN has been set |  |  |
|  | Run test functions |  |  |
|  | Self-destruct | SD PIN<br>SD KEK<br>SD SD PBKDF SALT | READ |

| Operator | Services | Accessible CSP | CSP Access by Module |
|---|---|---|---|
| | | Standard User PBKDF SALT<br>Administrative User PBKDF SALT<br>SD PBKDF SALT<br>OTR PBKDF SALT<br>DEK | WRITE |
| | Factory reset to clear all Critical Security Parameters (CSPs) | Standard User KEK<br>Standard User PBKDF SALT<br>Administrative User KEK<br>Administrative User PBKDF SALT<br>SD KEK<br>SD PBKDF SALT<br>OTR KEK<br>OTR PBKDF SALT<br>Standard User PIN<br>Administrative User PIN<br>OTR PIN<br>SD PIN<br>DEK<br>SP 800-90A state variables | WRITE |

## 3.2 AUTHENTICATION

The datAshur PRO$^2$ supports identity-based authentication. The module supports a single Administrative User, a single Standard User, and a single OTR User who are authenticated via the module's keypad interface. The module does not output authentication data outside of the cryptographic boundary.

From the factory, the datAshur PRO$^2$ drive is supplied in the 'Initial Shipment State' with no pre-set Admin PIN. A 7-15 digit Admin PIN must be configured before the drive can be used. The procedure for configuring an Admin PIN under 'Initial Shipment State' is specified in the User Manual. Once an Admin PIN has been successfully configured, it is then not possible to switch the drive back to the 'Initial Shipment State'.

**Table 6 - Authentication for IDs**

| Identity | Identification | Authentication | Description |
|---|---|---|---|
| Administrative User | Identified by pressing the KEY button | Enters 7 to 15 digit PIN | This identity has full access to all Administrative User services. |

| Identity | Identification | Authentication | Description |
|---|---|---|---|
| Standard User | Identified by entering the KEY + SHIFT buttons combination | Enters 7 to 15 digit PIN | This identity has full access to all Standard User services. |
| OTR User | Identified by entering the KEY + 4 buttons combination | Enters 7 to 15 digit PIN | This identity has full access to the OTR User services |

### 3.2.1 Initialization

After zeroization such as a factory reset, the module must be initialized before it can operate in an approved mode. The procedure is initiated differently for first time use and for initialization after factory reset. Additional detail on all procedures is specified in the User Manual.

- *On first time use:*
  - *Press and hold "SHIFT" button for one second until solid red and green LEDs display*
  - *Press and hold "Key + 1" buttons*
- *To initialize after factory reset:*
  - *In Standby state, press and hold "Shift + 1" buttons until solid red LED changes to blinking green LED and solid blue LED.*
- *Enter new Admin PIN and press the "key" button. Module displays solid blue LED and blinking green LED.*
- *Reenter new Admin PIN and press the "key" button again. Module displays a blinking green LED (first time use) or solid blue LED (after factory reset).*

### 3.2.2 Strength of Authentication

Authentication strength is determined by PIN which must be between 7 (minimum) and 15 (maximum) digits long. The PIN is comprised of numeric digits (0-9). The SHIFT key can be used for additional combinations, "SHIFT+1" is a separate value than just "1". Therefore, the probability of a successful, random guess of a PIN is approximately one in 20^7 or 1: 1,280,000,000.

The Standard User will be locked out of the module after ten (10) consecutive failed authentication attempts. If the Administrative User makes ten (10)[1] consecutive failed authentication attempts, zeroization will be triggered (refer to Section 6.1.1). The OTR User can also authenticate an OTR PIN and set up a new User PIN to access the data. Maximum five (5) attempts is allowed for authenticating an OTR PIN. In the unlikely event that an attacker makes 25 attempts in one minute, the probability of successfully guessing any PIN before the drive disables the roles or is zeroized is 1: 51,200,000. Furthermore, identity-based authentication further decreases the rate of false acceptance and the probability of a successful random attempt.

The Standard User PIN strength can be enhanced via a policy set by the Administrative User. The policy mandates a specific minimum length (from 7 to 15 digits) to be set, as well as the option to require the input of one or more "Special Characters". The "Special Character" functions as "SHIFT + digit".

[1] After five incorrect attempts, and also after eight incorrect attempts, the Administrative User must enter "47867243" and press the "KEY" button to continue attempting to authenticate

### 3.2.3 One-Time Recovery Feature

The datAshur PRO² has been designed with a one-time recovery feature that offers the user a way to access the data in case they forget the User PIN. The Administrative User creates an additional OTR PIN in Admin mode. When the OTR PIN is authenticated, the module will require users to set up a new User PIN. The creation of a new User PIN must comply with the 'User PIN Policy' if one has been configured. Upon successful creation of a new User PIN, the module will overwrite all CSPs related to the previous User PIN. The encryption key is not changed and all data stored in the drive remains intact.

To trigger the one-time recovery function, the user is required to press "KEY+4" buttons before entering the OTR PIN. The strength requirements for Admin/User PINs are also applicable to the OTR PIN. The administrator is entitled to set up or remove this feature.

### 3.2.4 Self-Destruct Feature

The datAshur PRO² has been designed with a self-destruct feature that zeroizes all plaintext secret keys and CSPs. The Administrative User creates an additional self-destruct PIN (SD PIN) in administrative mode. When the self-destruct PIN is authenticated, the module will delete the encryption key, all data, and Admin/User PINs, it will generate a new encryption key and unlock the drive. Activating this feature will cause the self-destruct PIN to become the new Standard User PIN and the datAshur PRO² will need to be partitioned and formatted before any new data can be added to the drive.

To trigger the self-destruct function, the user is required to press "Shift and Key" buttons before entering the self-destruct PIN, similar to the process for authenticating a user PIN. The strength requirements for Admin/User PINs are also applicable to self-destruct PIN. The administrator is entitled to set up or remove this feature.

## 3.3 Security Rules

This section documents the security rules enforced by the cryptographic module to implement the security requirements of FIPS 140-2 Level 3:

- The cryptographic module provides three distinct roles: Standard User, Administrative User, and OTR User.
- The cryptographic module provides identity-based authentication.
- When the module has not been placed in a valid role or is in an error state, the operator shall not have access to any cryptographic service.
- The operator can command the module to perform the power-up self-test at any time.
- Data output is inhibited during self-tests, zeroization, key generation, authentication and error states.
- No CSPs are output from the module in any form.
- The module uses a solid red LED to indicate that it is in an approved mode of operation.

# 4. PHYSICAL SECURITY

The datAshur PRO² Module is a multi-chip standalone device whose cryptographic boundary is defined as the perimeter of the outer enclosure. The opaque outer enclosure provides tamper evidence in the event the enclosure is opened. Regular inspections of the outer enclosure should be conducted for evidence of tampering.

To prevent the security integrity circuits from being physically attacked, all critical components are covered by an epoxy resin. Trying to access any component through the resin will cause critical damage. The epoxy also adds another layer of tamper-evidence to the products. Epoxy hardness was tested at ambient temperature and over the module’s documented operating temperature range from 0 ˚C to 45 ˚C.

# 5. OPERATIONAL ENVIRONMENT

The FIPS 140-2 Area 6 (Operational Environment) requirements for the module are not applicable because the device does not contain a modifiable operational environment.

# 6. CRYPTOGRAPHIC KEY MANAGEMENT

## 6.1 CSPs and Keys

No secret keys or CSPs are established or output by the module. PINs are entered into the module in plaintext via the keypad, but no secret keys or other CSPs are entered into the module. KEKs are derived from a PBKDF and may only be used in storage applications.

**Table 7 - Secret Keys and Critical Security Parameters**

| CSP/Key | Use | Generation or Establishment | Storage | Zeroization | |
|---|---|---|---|---|---|
| | | | | **All CSPs** | **Additional Zeroization** |
| Standard User PIN<br>(7-15 digits) | Input to PBKDF to allow generation of Standard User KEK | Created by Standard User | RAM<br>(plaintext during input and processing, deleted immediately after use) | Factory Reset, or sufficient failed authentication attempts | Lock, unlock, timeout, power-off |
| Administrative User PIN<br>(7-15 digits) | Input to PBKDF to allow generation of Administrative User KEK | Created by Administrative User | RAM<br>(plaintext during input and processing, deleted immediately after use) | | Lock, unlock, timeout, power-off |
| SD PIN<br>(7-15 digits) | Input to PBKDF to allow generation of SD KEK | Created by Administrative User | RAM<br>(plaintext during input and processing, deleted immediately after use) | | Lock, unlock, timeout, power-off |

| CSP/Key | Use | Generation or Establishment | Storage | Zeroization | |
|---|---|---|---|---|---|
| | | | | All CSPs | Additional Zeroization |
| OTR PIN<br>(7-15 digits) | Input to PBKDF to allow generation of OTR KEK | Created by Administrative User | RAM<br>(plaintext during input and processing, deleted immediately after use) | | Lock, unlock, timeout, power-off |
| Standard User KEK<br>(AES 256 KW) | AES key used to wrap the XTS-AES data encryption key (DEK) | Derived by the PBKDFv2 algorithm which uses the Standard User PIN along with Standard User Salt data | RAM<br>(plaintext, temporarily available during execution) | | Lock, unlock, timeout, power-off |
| Standard User PBKDF SALT<br>(256 bits) | Input to PBKDF to allow generation of Standard User KEK | Generated by internal SP 800-90A CTR-DRBG | Plaintext in NVM | | PIN changed/ deleted, SD PIN verified, User PIN policy changed |
| Administrative User KEK<br>(AES 256 KW) | AES key used to wrap the XTS-AES data encryption key (DEK) | Derived by the PBKDFv2 algorithm which uses the Administrative User PIN along with Administrative User Salt data | RAM<br>(plaintext, temporarily available during execution) | | Lock, unlock, timeout, power-off |
| Administrative User PBKDF SALT<br>(256 bits) | Input to PBKDF to allow generation of Administrative User KEK | Generated by internal SP800-90A CTR-DRBG | Plaintext in NVM | | PIN changed/ deleted, SD PIN verified, User PIN policy changed |
| SD KEK<br>(AES 256 KW) | AES key used to wrap the XTS-AES data encryption key (DEK) | Derived by the PBKDFv2 algorithm which uses PIN created by an Administrative User in addition to SD PBKDF Salt | RAM<br>(plaintext, temporarily available during execution) | | Lock, unlock, timeout, power-off |
| SD PBKDF SALT<br>(256 bits) | Input to PBKDF to allow generation of SD KEK | Generated by internal SP800-90A CTR-DRBG | Plaintext in NVM | | PIN changed/ deleted, SD PIN verified, User PIN policy changed |

| CSP/Key | Use | Generation or Establishment | Storage | Zeroization | |
|---|---|---|---|---|---|
| | | | | All CSPs | Additional Zeroization |
| OTR KEK<br>(AES 256 KW) | AES key used to wrap the XTS-AES data encryption key (DEK) | Derived by the PBKDFv2 algorithm which uses PIN created by an Administrative User in addition to OTR PBKDF Salt | RAM (plaintext, temporarily available during execution) | | Lock, unlock, timeout, power-off |
| OTR PBKDF SALT<br>(256 bits) | Input to PBKDF to allow generation of OTR KEK | Generated by internal SP800-90A CTR-DRBG | Plaintext in NVM | | PIN changed/ deleted, OTR PIN verified, User PIN policy changed |
| DEK<br>(XTS-AES 256) | XTS-AES Data Encryption Key (DEK) used to encrypt/ decrypt data to be stored/ retrieved from storage device | Generated by internal SP800-90A CTR-DRBG | RAM (plaintext, temporarily available during execution), wrapped with each authorized user's KEK | | Lock, unlock, timeout, power-off |
| SP 800-90A CTR-DRBG state variables (seed, V, and key) | State variables for SP 800-90A CTR - DRBG | Generated internally by the module's NDRNG | RAM (plaintext, temporarily available during execution) | | Lock, unlock, timeout, power-off |

### 6.1.1 Zeroization

Zeroization is the erasure of CSPs from volatile and non-volatile storage. The security controller firmware will erase any temporary variables as soon as they are not required. For example, the PIN buffer is immediately cleared when the authentication is done.

All values stored in the security controller NVM provide no clues to the PIN, the DEK, or the KEK values. When resetting the device or deleting a user, the related NVM values will be sanitized to guarantee there is no possibility of restoring the accounts. More specifically, the zeroization involves two rounds of complete overwrites of the memory content.

There is no non-volatile memory available in the encryption controller, thus any sensitive data passed to the encryption controller will not be stored. The temporary variables are erased as soon as no longer required.

Factory reset (zeroization) is initiated by the following procedure:

- *In Standby state, press and hold "0" button until all LEDs blink alternatively on and off*

- *Press and hold down “2 + 7” buttons until all LEDs become solid for a second and then to a solid RED LED*

In addition, if an incorrect Admin PIN is entered ten (10) consecutive times, the module’s Brute Force Defense Mechanism (zeroization) is activated, and then all data including, Admin/User/SD/OTR PINs, the encryption key and all CSPs will be deleted and lost forever.

## 6.2 Algorithms

### 6.2.1 FIPS Approved Algorithms

Table 8 lists all the approved algorithms used in the module.

**Table 8 - FIPS Approved Algorithms**

| Certificate | Algorithm | Standard(s) | Modes/Methods | Key Lengths, Curves, or Moduli | Use |
|---|---|---|---|---|---|
| 4756 | AES | FIPS 197,<br>NIST SP 800-38A<br>SP 800-38E | CBC, ECB, XTS | 256 bits[2] | Encryption Controller:<br>User data encryption and decryption |
| 5179 | AES | FIPS 197,<br>NIST SP 800-38A<br>NIST SP 800-38F | CTR, ECB, KW | 256 bits | Security Controller:<br>ECB and CTR modes are used as the basis of the CTR-DRBG and the KW mode. KW mode is implemented to wrap and recover the data key and for user authorization. |
| Vendor affirmed | CKG | SP 800-133 | | | The unmodified output of the DRBG is used for symmetric key generation |
| 1954 | DRBG | NIST SP 800-90A | AES-256 based CTR-DRBG | 256 bits | Security Controller:<br>Random number generator for encryption keys and salts. |
| 3435 | HMAC | FIPS 198-1 | HMAC-SHA-256 | 256 bits | Security Controller:<br>Algorithmic basis of PBKDF. |
| Vendor Affirmed | PBKDF | RFC 2898,<br>NIST SP 800-132 (supports option 2a of section 5.4) | HMAC-SHA-256 (Cert. 3435) | 256 bits | Security Controller:<br>This algorithm accepts the user's PIN as input and generates the KEK (only used in storage applications). |
| 4183 | SHS | FIPS 180-4 | SHA-256 | 256 bits | Security Controller:<br>Algorithmic basis of PBKDF. |

### 6.2.2 FIPS Allowed Algorithms

Table 9 lists all the non-approved algorithms used in the module.

[2] 128-bit AES is included in the CAVS certificate, but is not used by any of the module’s services

Table 9 - FIPS Allowed Algorithms

| Algorithm | Use | Strength |
|---|---|---|
| NDRNG | Security Controller:<br>Entropy source for seed to CTR-DRBG | The NDRNG generates a minimum of 283 bits of entropy as entropy input for the module's 256-bit CTR-DRBG. |

## 7. EMI/EMC

The module conforms to the EMI/EMC requirements specified by 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class B (i.e., for home use).

## 8. SELF-TESTS

When the module is powered on, it performs initialization and runs a sequence of self-tests. If any of these tests fails, the module transitions to an error state. In this state, the module cannot perform any cryptographic services and is not usable. Table 10 summarizes the power-up self-tests.

Table 10 - Power-Up Self-Tests

| Tested Function | Self-Test | Error State | Error Indicator | Access | Resolving Error |
|---|---|---|---|---|---|
| **Firmware Integrity Tests** | | | | | |
| SC Firmware Integrity Test | Cyclic Redundancy Check - CRC-32 | Power-Up Self-Test Failed | A faded illumination of Red and Blue LEDs | All SC cryptographic operations and data output are inhibited | Power cycle the device to reinitiate the power-up self-tests. Module can be used if tests are successful. |
| EC Firmware Integrity Test | Cyclic Redundancy Check - CRC-16 | Power-Up Self-Test Failed | Green LED blinks constantly when a valid PIN is entered and the device is connected to a powered USB port | All EC cryptographic operations and data output are inhibited | Power cycle the device to reinitiate the power-up self-tests. Module can be used if tests are successful. |
| **Entropy Source Power-Up Self-Tests** | | | | | |

| Tested Function | Self-Test | Error State | Error Indicator | Access | Resolving Error |
|---|---|---|---|---|---|
| NDRNG | NDRNG power-up tests include:<br>• Repetition Count Test (RCT) per SP 800-90B<br>• Adaptive Proportion Test (APT) per SP 800-90B | Power-Up Self-Test Failed | The LEDs illuminate alternately from Red to Green to Blue, then the flashing Green LED, same pattern repeats, and the device is securely reset | All SC cryptographic operations and data output are inhibited | Power cycle the device to reinitiate the power-up self-tests. Module can be used if tests are successful. |
| **Known Answer Tests (KATs)** | | | | | |
| CTR-DRBG[3] | DRBG KATs include the following:<br>• Instantiate<br>• Generate<br>• Reseed | Power-Up Self-Test Failed | The LEDs illuminate alternately from Red to Green and then to Blue, followed by Red LED blinking two seconds, same pattern repeats | All SC cryptographic operations and data output are inhibited | Power cycle the device to reinitiate the power-up self-tests. Module can be used if tests are successful. |
| PBKDF | PB KDF KAT includes:<br>• SHA-256 KAT<br>• HMAC-SHA-256 KAT | Power-Up Self-Test Failed | | All SC cryptographic operations and data output are inhibited | Power cycle the device to reinitiate the power-up self-tests. Module can be used if tests are successful. |
| AES (Cert. #5179) | AES ECB SC Encrypt KAT | Power-Up Self-Test Failed | | All SC cryptographic operations and data output are inhibited | Power cycle the device to reinitiate the power-up self-tests. Module can be used if tests are successful. |
| | AES ECB SC Decrypt KAT | | | | |
| AES Key Wrap (Cert. #5179) | KW-AE KAT | Power-Up Self-Test Failed | | All SC cryptographic operations and data output are inhibited | Power cycle the device to reinitiate the power-up self-tests. Module can be used if tests are successful. |
| | KW-AD KAT | | | | |
| AES (Cert. #4756) | XTS-AES EC Encrypt KAT | Power-Up Self-Test Failed | GREEN LED Blinks constantly | All EC cryptographic operations and data output are inhibited | Power cycle the device to reinitiate the power-up self-tests. Module can be used if tests are successful. |
| | XTS-AES EC Decrypt KAT | | | | |

[3] Per IG 9.8, the SP 800-90A-compliant DRBG does not perform the test described in AS.09.42-AS.09.43

Table 11 - Conditional Self-Tests

| Tested Function | Self-Test | Initiation | Error State | Error Indicator | Access | Resolving Error |
|---|---|---|---|---|---|---|
| **Conditional Tests** | | | | | | |
| NDRNG | NDRNG power-up tests include:<br>• Repetition Count Test (RCT) per SP 800-90B<br>• Adaptive Proportion Test (APT) per SP 800-90B | Initiated on every call to instantiate/ reseed [SP 800-90A] CTR-DRBG | Conditional Self-test failed | The LEDs illuminate alternately from Red to Green to Blue, then the flashing Green LED, same pattern repeats, and the device is securely reset | All cryptographic operations and data output are inhibited | Power cycle the device to reinitiate it. Module can be used if power-up and conditional self-tests are successful. |
| AES-XTS-256 | FIPS 140-2 implementation guidance A.9 XTS-AES Key Generation test | Initiated on every call to generate a DEK | Conditional Self-test failed | Green LED blinks constantly when a valid PIN is entered and the device is connected to a powered USB port | All EC cryptographic operations and data output are inhibited | Power cycle the device to reinitiate it and initiate another call to re-generate an XTS-AES Key |

# 9. APPENDIX A: REFERENCES

Table 12 – References

| Reference Number | Reference Title | Publishing Entity | Publication Date |
|---|---|---|---|
| [1] | Implementation Guidance for FIPS 140-2 and the Cryptographic Module Validation Program. | NIST | December 2019 |
| [2] | SP 800-90B: Recommendation for the Entropy Sources Used for Random Bit Generation. | NIST | January 2018 |
| [3] | Annex C: Approved Random Number Generators for FIPS PUB 140-2, Security Requirements for Cryptographic Modules. | NIST | June 2019 |
| [4] | FIPS 197: Specification for the ADVANCED ENCRYPTION STANDARD (AES). | NIST | November 2001 |
| [5] | SP 800-38A: Recommendation for Block Cipher Modes of Operation. | NIST | December 2001 |
| [6] | SP 800-38E: Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices. | NIST | January 2010 |
| [7] | SP 800-38F: Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping. | NIST | December 2012 |
| [8] | SP 800-90A Revision 1: Recommendation for Random Number Generation Using Deterministic Random Bit Generators. | NIST | June 2015 |
| [9] | FIPS 180-4: Secure Hash Standard (SHS). | NIST | August 2015 |
| [10] | FIPS PUB 198-1: The Keyed-Hash Message Authentication Code (HMAC). | NIST | July 2008 |
| [11] | SP 800-132: Recommendation for Password-Based Key Derivation Part 1: Storage Applications. | NIST | December 2010 |

# 10. APPENDIX B: ABBREVIATIONS AND DEFINITIONS

Table 13 – Abbreviations and Definitions

| Term | Definition |
|---|---|
| ADMIN | Administrative User |
| AES | Advanced Encryption Standard |
| CRC | Cyclic Redundancy Check |
| CSP | Critical Security Parameter |
| DEK | Data Encryption Key |
| DRBG | Deterministic Random Bit Generator |
| EC | Encryption Controller |
| ECB | Electronic Code Book |
| EMC | Electromagnetic Compatibility |
| EMI | Electromagnetic Interference |
| FIPS | Federal Information Processing Standard |
| FSM | Finite State Model |
| HDD | Hard Disk Drive |
| HMAC | Hash-Based Message Authentication Code |
| KAT | Known Answer Test |
| KC | Keypad Controller |
| KEK | Key Encryption Key |
| KW | Key Wrap |
| LED | Light Emitting Diode |
| NDRNG | Non-Deterministic Random Number Generator |
| NVM | Non-Volatile Memory |
| OTR | One-Time Recovery |
| PBKDF | Password Based Key Derivation Function |
| PIN | Personal Identification Number |
| SALT | Random value used to improve security of cryptographic algorithms |
| SC | Security Controller |
| SD | Self-Destruct |
| SHA | Secure Hash Algorithm |
| SSD | Solid State Drive |
| USB | Universal Serial Bus |