SECUREDATA, Inc.
SecureDrive KP

FIPS 140-2 Non-Proprietary Security Policy
Version 1.2

Table of Contents

List of Tables

List of Figures

1 Cryptographic Module Specification

1.1 Overview

The SECUREDATA, Inc. SecureDrive KP is a multi-chip, stand-alone, cryptographic module that provides hardware-encrypted storage of user data with a USB 3.0 interface. Access to encrypted data is authenticated with user input via the built-in keypad. User data is protected by 256-bit XTS-AES encryption that secures sensitive information from unauthorized disclosure in the event that the module is lost or stolen. The custom electronics within the module are encapsulated within an opaque, production grade epoxy. The module's enclosure defines the cryptographic boundary.

The data encryption key (DEK) and other critical security parameters (CSPs) are generated by a NIST approved DRBG[1] within the module when it is first used. The seed for the DRBG is also produced within the module from a hardware-based, entropy generator.

The user interface for the module is an alphanumeric keypad with eleven (11) buttons and three (3) status-indicator LEDs. The LEDs are each a different color, red green and blue, and in distinct locations. The keypad accepts the User or CO PIN/Password when creating new credentials and when authenticating to unlock the module. The LEDs provide status information while entering authentication credentials and using the module.

---

[1] *SP 800-90Ar1 – Recommendation for Random Number Generation Using Determinstic Random Bit Generators*. NIST. (June 2015).

Figure 1: SecureDrive KP   .

Hardware Part Numbers	Firmware Versions
SD-KP-12-BL-1TB SD-KP-12-BL-2TB SD-KP-20-BL-1TB SD-KP-20-BL-2TB SD-KP-20-BL-4TB SD-KP-20-BL-5TB SD-KP-12-BL-250GB-SSD SD-KP-12-BL-500GB-SSD SD-KP-12-BL-1TB-SSD SD-KP-12-BL-2TB-SSD SD-KP-12-BL-4TB-SSD SD-KP-12-BL-8TB-SSD	CLEVX_3637E_USB_V0313 CLEVX_3637E_USB_V0314 CLEVX_SATA-KP_v2.2

Table 1: Module Hardware and Firmware Versions

1.2 FIPS Security Level

The module meets the overall requirements for FIPS 140-2[2] Level 3.

FIPS Area	FIPS Security Requirement	Level
1	Cryptographic Module Specification	3
2	Module Ports and Interfaces	3
3	Rôles, 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*

Table 2: FIPS Security Level

---

[2]   *FIPS 140-2 – Security Requirements for Cryptographic Modules*. NIST. (December 2002).

1.3 Mode of Operation

The module operates only in a FIPS approved mode. Approved mode is indicated by the three status-indicator LEDs blinking once simultaneously when the module is powered on.

To meet the requirements for FIPS 140-2 Level 3, the module enforces the following security rules:

- The cryptographic module provides two distinct operator rôles: User and Cryptographic Officer (CO).
- The cryptographic module provides identity-based authentication.
- When the module has not been placed in a valid rôle or is in an error state, the operator shall not have access to any cryptographic service.
- The operator is capable of commanding the module to perform self-tests at any time by cycling the power.
- Data output is inhibited during self-test, zeroization, key generation, and authentication.
- No CSPs are output from the module in any form.

2 Module Ports and Interfaces

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

Physical Port	Logical Interface	Description
USB Data	Data input Data output Control input Status output	The USB Data port connects the module to the host computer. It is used to exchange decrypted user data as well as control and status information for the USB protocol. When the drive is locked the USB interface is disabled.
Alphanumeric Keypad (0-9)	Data input	The keypad with ten (10) alphanumeric labeled buttons is connected to button inputs. The keypad is used to enter User or CO PIN/Password.
KEY button	Control input	The KEY button is connected to a button input. It is used to awaken the module from low-power sleep and to control UI flow including selection of the rôle.
Red, green and blue LEDs	Status output	Refer to Table 4 for details.
USB Power	External power	The USB VBUS (+5VDC) powers the module and embedded storage component.

Table 3: Module Ports and Interfaces

LED Behavior	Module State	Status Description
All three LEDs blink once simultaneously	Connected to USB power	Module powered-on with all LEDs operational. Firmware integrity tests and KATs have passed.
LEDs illuminate two times in circling pattern, red then green then blue. Red LED illuminates, fades out, and then red illuminates steadily.	Failed	Module in error state.
Red LED blinking	Locked	Waiting for User PIN/Password to unlock
Red and blue LEDs blinking	Locked	Waiting for User PIN/Password to unlock. CO PIN/Password is set.
Red LED on solidly	Locked	Module verifying User PIN/Password
Green LED on solidly	Disconnected	Unlocked and ready to connect to PC
Green LED on solidly and blue LED blinking	Connected	Unlocked, connected to PC via USB, and communicating or transferring data
Green and blue LEDs on solidly	Connected	Unlocked and connected to PC via USB
Green LED on with single blink every 2 seconds and blue LED blinking	Connected	Unlocked, connected to PC via USB, and communicating or transferring data. Drive configured in read-only mode
Green LED on with single blink every 2 seconds and blue LEDs on solidly	Connected	Unlocked and connected to PC via USB. Drive configured in read-only mode.
Red LED blinking and green LED on solidly.	UI	User authenticated and module configuration UI is active.
Red LED blinking and green LED blinking quickly.	UI	CO authenticated and module configuration UI is active.
Red LED blinks very slowly.	Locked and disconnected	Module is awake and there is neither User nor CO PIN/Password defined after reset.
Blue LED blinking	Disconnected	Ready to accept new User PIN/Password
Green LED blinking after entering new User/CO PIN/Password	Disconnected	Ready to accept new PIN/Password a second time as confirmation
Red and blue LEDs blinking	Disconnected	Ready to accept new CO PIN/Password
Red and green LEDs blinking	Locked	Waiting for CO PIN to unlock. User PIN/Password is set.
Blue LED blinking	Locked	No User PIN/Password
Red and green LEDs blinking alternately	Disconnected	Factory reset initiated. Module waiting for confirmation code.
Red LED illuminates and then fades out and then illuminates solidly	Disconnected	Module locked and disconnected

Table 4: LED Status Indications

To verify that the module is in good working order when it is first powered-on, observe that the three status-indicator LEDs blink once simultaneously. Then, press KEY to make sure the module does not enter the ERROR state.

3   Rôles, Services, Authentication, and Identification

3.1 Rôles and Identification

The module implements level 3, identity-based authentication with two distinct identities User and Crypto-Officer.

Identity	Identification	Authentication Data	Description
User[3]	Identifies as User by pressing 'KEY' button	7-15 digit PIN/Password	User has full access to all User services.
CO	Identifies as CO by pressing '1' and 'KEY' buttons	7-15 digit PIN/Password	CO has full access to all CO services.

Table 5: Module Rôles

The rôle is explicitly selected during authentication:

- User
  1. Press and release KEY button to identify as User
  2. Enter correct User PIN/Password
  3. Press and release KEY button

- CO
  1. Press and hold '1' button
  2. Press and release KEY button
  3. Release '1' to identify as CO
  4. Enter correct CO PIN/Password
  5. Press and release KEY button

---

3   In the case where the User PIN is defined but no CO PIN is defined, the User identity behaves as a combined User/CO identity.

3.2 Module Initialization

A new module comes from the factory initialized with a default User PIN/Password of '11223344'. No CO PIN/Password is defined for a factory initialized module. In this configuration, the module is ready for operation in a FIPS approved mode.

If the module is zeroized, there will be neither a User PIN/Password nor a CO PIN/Password defined and there will be no DEK. The module must be initialized before it will operate in an approved mode. From this state, either a User or a CO PIN/Password may be defined first.

To create an initial User PIN/Password on a zeroized module:

1. Connect the Drive to a computer with the USB cable.
2. Verify that all LEDs illuminate simultaneously and then the red LED remains lit.
3. Press KEY. Red LED will blink slowly.
4. Press KEY twice. Blue LED blinks.
5. Enter new User PIN/Password. Press KEY twice. Green LED blinks.
6. Enter new User PIN/Password a second time. Press KEY twice.
7. Red LED illuminates while the credentials are saved.
8. Green LED illuminates when complete. The module is unlocked as the User.

To create an initial CO PIN/Password on a zeroized module:

1. Connect the Drive to a computer with the USB cable.
2. Verify that all LEDs illuminate simultaneously and then the red LED remains lit.
3. Press KEY. Red LED will blink slowly.
4. Press and hold '1' button. Press and release KEY twice. Release '1' button. Blue and red LEDs blink together.
5. Enter new CO PIN/Password. Press KEY twice. Green LED blinks.
6. Enter new CO PIN/Password a second time. Press KEY twice.
7. Red LED illuminates while the credentials are saved.
8. Green LED blinks fast when complete. The module is unlocked as the CO.

3.3 Services

Identity	Service	CSP Access
CO	Set CO PIN/Password	<u>Read and Write</u> Change CO PIN/Password, CO salt, and CO KEK. Create DEK using CTR-DRBG state (seed, V, key) if one is not defined.
	Set User PIN/Password	<u>Read and Write</u> Change User PIN/Password, User salt, and User KEK.
	Zeroize User PIN/Password	<u>Zeroize</u> Zeroize User salt and User KEK.
	Erase private partition data	<u>Read and Write</u> Change CO salt and CO KEK. Create DEK using CTR-DRBG state (seed, V, key). <u>Zeroize</u> Zeroize User salt and KEK.
	Open private partition for read/write access to user data	<u>Read</u> Read CO salt and CO KEK. Decrypt DEK.
	Lock private partition to prevent read/write access to user data	<u>Zeroize</u> Zeroize DEK in RAM.
	Read or write private partition with user data	<u>Read</u> Use DEK to encrypt and decrypt user data.
	Configure idle timeout lock	None
User	Set CO PIN/Password when none exists	<u>Read and Write</u> Change CO PIN/Password, CO salt, and CO KEK.
	Set User PIN/Password	<u>Read and Write</u> Change User PIN/Password, User salt, and User KEK. Create DEK using CTR-DRBG state (seed, V, key) if one is not defined.
	Open private partition for read/write access to user data	<u>Read</u> Read CO salt and CO KEK. Decrypt DEK.
	Lock private partition to prevent read/write access to user data	<u>Zeroize</u> Zeroize DEK in RAM.
	Read or write private partition with user data	<u>Read</u> Use DEK to encrypt and decrypt user data.
	Configure idle timeout lock	None

Identity	Service	CSP Access
Unauthenticated	Show locked/unlocked status	None
	Show whether or not drive is initialized	Read Verify validity of either User salt or CO salt.
	Show whether or not User PIN/Password is defined	Read Verify validity of User salt.
	Show whether or not CO PIN/Password is defined	Read Verify validity of CO salt.
	Run self-tests	None
	Factory reset (zeroize) module and erase private partition data	Zeroize Zeroize all CSPs.

Table 6: Services Available in FIPS Approved Mode

3.4 Authentication

The Crypto Officer and User rôles authenticate via the module's keypad interface. The module does not output CO or User authentication data outside of the cryptographic boundary.

The PIN/Password, from either the User or the CO, is an input to PBKDFv2 that produces the Key Encryption Key (KEK) for that rôle. The KEK is used by the Synthetic Initialization Vector[4] (SIV) algorithm to encrypt or wrap the DEK. SIV is constructed using AES CTR (Cert. #5366) and AES CMAC (Cert. #5366). Decrypting (sometimes called unwrapping) an encrypted DEK requires the same PIN/Password that was given to PBKDFv2 when the DEK was encrypted.

The authentication strength for the module is determined by the PIN/Password. The PIN/Password is composed of a sequence of decimal digits 0-9, as marked on the keypad buttons, selected by the User or CO. Most of the buttons also bear alphabetic letters (see Figure 1). The minimum PIN/Password length is seven (7) digits. The maximum PIN/Password length is 15 digits. The probability of a successful, random guess of a minimum length PIN/Password is approximately 10^{-7} or 1 chance in 10,000,000[5].

The module protects against brute-force attempts to guess a rôle's PIN/Password by permitting no more than ten (10) consecutive incorrect guesses before locking out that rôle. Incorrect PIN/Password attempts are counted independently for each rôle. The probability of an attacker correctly guessing a PIN/Password is 10^{-6} or 1 chance in 1,000,000.

---

4   Harkins, D. *Synthetic Initialization Vector (SIV) Authenticated Encryption Using the Advanced Encryption Standard (AES)*. IETF. (October 2008)

5   Sequential and repeating PINs are not allowed. For example, the module will reject a PIN of 1-2-3-4-5-6-7 or 6-5-4-3-2-1-0. Attempts to create such a PIN will cause the module to indicate an error. There are 270 such combinations.

4 Physical Security

The multi-chip standalone cryptographic module includes the following physical security mechanisms, conforming to FIPS 140-2 Level 3 requirements:

1. Production grade components
2. Hard, opaque, tamper-evident enclosure with embedded, hard epoxy covering all security relevant components
3. Memory protection enabled to prevent read-out of firmware, RAM, or NVRAM

The operator should periodically inspect the module for evidence of tampering.

5 Operational Environment

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

6 Cryptographic Key Management

6.1 Cryptographic Algorithms

Algorithm	Modes	Key Sizes	Reference	CAVP Cert.	Use
AES	XTS[6]	256	NIST SP 800-38E[7]	4642	Encryption of user data within storage application only
AES	ECB CMAC CTR	128 256 (ECB only)	FIPS 197[8] NIST SP 800-38A[9]	5366	Block cipher basis of CTR-DRBG.
CKG	-	256	NIST SP-800-133[10]	Vendor Affirmed	The unmodified output of the DRBG is used for generating symmetric keys
DRBG	AES-CTR	256	NIST SP 800-90A[11]	2077	Random number generator for encryption keys and salts
HMAC	HMAC-SHA-1	160	FIPS 198-1[12]	3554	Algorithmic basis of PBKDFv2
PBKDFv2	HMAC-SHA-1	-	NIST SP 800-132[13]	Vendor Affirmed	KEK generation. Password is the same as the User/CO PIN/Password with a minimum length of 7 digits 0-9. Algorithm conforms to FIPS 140-2 Implementation Guidance (IG) D.6: the module supports option 2a as documented in SP 800-132 § 5.4.
SHS	SHA-1	-	FIPS 180-4[14]	4308	Algorithmic basis of HMAC-SHA1

Table 7: FIPS Approved Algorithms

Algorithm	Caveats	Use
NDRNG	Module generates cryptographic keys with a minimum security strength of 256 bits.	Entropy source for seed to CTR-DRBG

Table 8: FIPS Allowed Algorithms

---

6   ECB and CBC modes as well as 128 bit AES are included in the CAVS certificate, but are used by no services in the module.
7   *SP 800-38E – Recommendation for Block Cipher Modes of Operation: the XTS-AES Mode for Confidentiality on Storage Devices*. NIST. (January 2010).
8   *FIPS 197 – Advanced Encryption Standard (AES)*. NIST. (November 2001).
9   *SP 800-38A – Recommendation for Block Cipher Modes of Operation: Methods and Techniques*. NIST. (December 2001).
10   *SP 800-133 – Recommendation for Cryptographic Key Generation*. NIST. (December 2012).
11   *SP 800-90Ar1 – Recommendation for Random Number Generation Using Determinstic Random Bit Generators*. NIST. (June 2015).
12   *FIPS 198-1 – The Keyed-Hash Message Authentication Code (HMAC)*. NIST. (July 2008).
13   *SP 800-132 – Recommendation for Password-Based Key Derivation: Part 1: Storage Applications*. NIST. (December 2010).
14   *FIPS 180-4 – Secure Hash Standard (SHS)*. NIST. (August 2015).

6.2 Critical Security Parameters

The module does not output or establish CSPs--either by key agreement or key transport. The only CSPs entered in into the module are plaintext PIN/Passwords via the keypad. KEKs are derived using PBKDFv2 and are only used as part of the module's data storage application.

Parameter	Use	Source	Storage	Creation / Destruction
CTR-DRBG state (seed, V, key)	Generating random values for CSPs	NDRNG and CTR-DRBG	RAM	Created when DRBG is seeded which is every time the module initializes
				Destroyed on lock, connect, successful generation of CSPs, power-off, and zerization
User PIN/Password	Input to PBKDFv2 to allow generation of the User KEK.	Keypad entry	RAM	Created by User
				Destroyed on lock, unlock, timeout, power-off
CO PIN/Password	Input to PBKDFv2 to allow generation of the CO KEK.	Keypad Entry	RAM	Created by CO
				Destroyed on lock, unlock, timeout, power-off
User Salt	Input to PBKDFv2 to generate key to wrap DEK.	CTR-DRBG	NVRAM	Created when User changes PIN/Password
				Destroyed on PIN/Password change, zeroization
CO Salt	Input to PBKDFv2 to generate key to wrap DEK.	CTR-DRBG	NVRAM	Created when CO changes PIN/Password
				Destroyed on PIN/Password change, zeroization
XTS-AES DEK	Encryption and decryption of user data	CTR-DRBG	RAM	Created when first PIN/Password, either User or CO, is set
				Destroyed on lock, timeout, entering low-power mode, power-off, and zeroization
User KEK	Encryption (wrapping) and decryption (unwrapping) of DEK	User PIN/Password, User Salt, and PBKDFv2	RAM	Created before encrypting or decrypting the DEK.
				Destroyed immediately after use
CO KEK	Encryption (wrapping) and decryption (unwrapping) of DEK	CO PIN/Password, CO Salt, and PBKDFv2	RAM	Created before encrypting or decrypting the DEK.
				Destroyed immediately after use

Table 9: Critical Security Parameters

6.3 Zeroization of Critical Security Parameters

Zeroization is the erasure of CSPs from volatile and non-volatile storage. The module initiates an erase cycle to zeroize CSPs stored in NVRAM. Copies of CSPs in RAM are erased by setting the memory to zeros. This process occurs when the module is factory reset or when the module detects a brute-force attack.

Factory reset is initiated by the following procedure:

1. Disconnect and reattach USB connection to the module. The red LED will be on steady indicating that the drive is locked.
2. Press and hold '7' button.
3. Press and release KEY button to awaken drive.
4. Observe red and green LEDs are illuminating alternately.
5. Enter confirmation code 9-9-9.
6. Press and hold '7' button.
7. Press and release KEY button to confirm factory reset.
8. Release '7' button.
9. Observe red and green LEDs on steadily for several seconds while CSPs are zeroized.

There are two kinds of brute-force attacks. Ten consecutive failed attempts to unlock the module as the User is the first type of brute-force attack and will zeroize the User CSPs. After this type of attack, the CO will be able to unlock the module, recover user data, and permit the setup of a new User PIN/Password. However, if there is no CO PIN/Password, the user data partition will be erased leaving the module in the factory reset state with an erased use data partition.

The second kind of brute-force attack is against the CO PIN/Password. Ten consecutive failed attempts to unlock the module as CO will zeroize all CSPs for both the CO and User rôles, including the DEK. The module will be left in the factory reset state with an erased user data partition.

7   EMI/EMC Regulatory Compliance

This module conforms to the EMI/EMC requirements specified by Title 47 of the 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 powers on, it performs initialization and runs a sequence of self-tests. If any of these tests fails, the drive will enter an error state. The module cannot perform any cryptographic services and is not usable in this state. The module also performs continuous self-tests. The only way to clear a module error state is to cycle the power. Self-tests are summarized in Table 10.

Test Category	Test Name	When Executed	Error Indication
Firmware Integrity	Firmware CRC-32	Module power-on	Module illuminates no LEDs and does not respond to button presses.
	Firmware CRC-16	Module power-on	Module fails to mount to host PC after successful unlock and returns to locked state.
Known Answer	DRBG Cert. #2077 KATs CTR-DRBG Instantiate CTR-DRBG Generate	Module power-on	LEDs illuminate two times in circling pattern, red then green then blue. Red LED illuminates, fades out, and then red illuminates steadily.
	PBKDFv2 combined KATs HMAC SHA-1 Cert. #3554 SHA-1 Cert. #4308	Module power-on	LEDs illuminate two times in circling pattern, red then green then blue. Red LED illuminates, fades out, and then red illuminates steadily.
	SIV KATs AES ECB encrypt Cert. #5366 AES ECB decrypt Cert. #5366 AES CMAC Cert. #5366	Module power-on	LEDs illuminate two times in circling pattern, red then green then blue. Red LED illuminates, fades out, and then red illuminates steadily.
	XTS-AES Cert. #4642 KATs AES-XTS encrypt AES-XTS decrypt	Module power-on	Module fails to mount to host PC after successful unlock.
Conditional	NDRNG Conditional Test	Use of NDRNG	LEDs illuminate two times in circling pattern, red then green then blue. Red LED illuminates, fades out, and then red illuminates steadily.
	AES-XTS Cert. #4642 Conditional FIPS 140-2 IG A.9 AES-XTS Key Generation Test	Creation of DEK	Module fails to mount to host PC after successful unlock.

Table 10: Module Self-Tests

9   Mitigation of Other Attacks

The module has not been designed to mitigate attacks not addressed by the security requirements of FIPS 140-2.

10 Glossary of Terms and Acronyms

Term	Definition
AES	Advanced Encryption Standard
CO	Cryptographic Officer
CRC	Cyclic Redundancy Check
CSP	Critical Security Parameter
CTR-DRBG	Counter-Mode Deterministic Random Byte Generator
DEK	Data Encryption Key
DRBG	Deterministic Random Byte Generator
ECB	Electronic Code Book
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FIPS	Federal Information Processing Protocol
HMAC	Keyed-Hash Message Authentication Code
KAT	Known Answer Test
KEK	Key Encryption Key
LED	Light Emitting Diode
NDRNG	Non-deterministic Random Number Generator; module entropy source
NIST	National Institute of Standards and Technology
NVRAM	Non-volatile Random Access Memory
PBKDFv2	Password Based Key Derivation Algorithm Version 2
PIN	Personal Identification Number; synonym for password
RAM	Random Access Memory
Salt	Random value used to improve security of cryptographic algorithms
SATA	Serial AT Attachment
SHA-1	Secure Hash Algorithm 1
SHS	Secure Hash Standard

SIV	Synthetic Initialization Vector
USB	Universal Serial Bus
XTS-AES	AES cipher mode used to encrypt user data in mass storage
Zeroization	The process of erasing cryptographic security keys and parameters