LOK-IT
SECURE FLASH DRIVE®

FIPS 140-2 SECURITY POLICY V.15.4
For
LOK-IT® 10 KEY (Series SDG003FM)

TABLE OF CONTENTS

MODULE OVERVIEW

LOK-IT® 10 Key (Series SDG003FM) Revisions

Hardware revision:	HW003-32 Rev:01	32GB
	HW003-16 Rev:04	16GB
	HW003-16 Rev:03	16GB
	HW003-08 Rev:03	8GB
	HW003-08 Rev:02	8GB
	HW003-04 Rev:03	4GB
	HW003-04 Rev:02	4GB
USB controller firmware revision:	V01.12A14-F05	32GB
	V01.12A14-F05	16GB
	V01.12A12-F01	16GB
	V01.12A14-F05	8GB
	V01.12A12-F01	8GB
	V01.12A14-F05	4GB
	V01.12A12-F01	4GB
Security controller firmware revision:	SDG003FM-010	32GB
	SDG003FM-010	16GB
	SDG003FM-010	8GB
	SDG003FM-010	4GB

SDG provides FIPS 140-2 approved security functionality to the LOK-IT®USB flash drive[1]. The LOK-IT® module employs FIPS compliant encryption and key management functionality to ensure the protection of data stored on internal LOK-IT® flash memory.

The module is a multi-chip standalone cryptographic module, as defined by FIPS 140-2 and consists of an Initio 1861 USB controller, NAND Flash memory and a Microchip PIC16LF1825 security controller. All components are encased in hard, opaque, production grade integrated circuit packaging. The cryptographic boundary is defined as the boundary of the module's PCB and hard epoxy coating.

Figure 1

Component Side of PCB

[1] Based upon *DataLock®,* licensed technology from ClevX, LLC – Patents Pending

SECURITY LEVEL

The cryptographic module meets the overall requirements applicable to Level 3 Security of FIPS 140-2.

Security Requirements Section	Level
Cryptographic Module Specification	3
Roles, Services, and Authentication	3
Module Ports and Interfaces	3
Finite State Model	3
Physical Security	3
Operational Environment	N/A
Cryptographic Key Management	3
EMI/EMC	3
Self-Tests	3
Design Assurance	3
Mitigation of Other Attacks	N/A
Overall	3

Table 1

Module Security Level Specification

MODES OF OPERATION

Approved Modes of Operation

The LOK-IT® module supports a FIPS approved mode of operation. The module is locked and is inaccessible to a connected host computer until the user enters a valid PIN that authenticates to a particular role.

Drives are configured in manufacturing with a single private partition. The partition is not accessible until the user or CO has set a valid PIN.

Non-Approved Modes of Operation

LOK-IT® does not support any non-approved modes of operation.

Approved Algorithms

AES 256 bit (CBC), NIST Certification #1514

SHA-256, NIST Certification #1682

Hash_DRBG, NIST Certification #164

Non-Approved Algorithms

NDRNG.

Encryption Keys

SDG003FM uses a NDRNG as input to a Hash_DRBG algorithm specified in NIST special publication SP800-90 to generate a random 256 bit encryption key. The AES key has 256 bits of entropy.

CRYPTOGRAPHIC KEY MANAGEMENT

A new encryption key is generated when a PIN is defined on a reset drive. A drive is reset when:

- Shipped from factory
- After 10 unsuccessful attempts to unlock (all crypto-parameters are zeroized)

A LOK-IT drive will require formatting any time a new encryption key is created. Table 2 shows when this happens. The same encryption key is shared by both user and CO. In addition, changing a PIN will not affect the current encryption key. There are 2 conditions (the first two listed in Table 2) when an encryption key is created:

User PIN Defined	CO PIN Defined	Action	Drive Behavior
No	No	CO Defines CO PIN	New encryption key created, drive accessible.
No	No	User Defines User PIN	New encryption key created, drive accessible.
No	Yes	User Defines User PIN	No change to key, drive content created by CO accessible.
Yes	No	CO Defines CO PIN	No change to key, drive content created by User accessible. User PIN intact
Yes	Yes	CO Changes CO PIN	No change to key, drive content still accessible
Yes	Yes	User Changes User PIN	No change to key, drive content still accessible
Yes	Yes	CO Opens Drive	User PIN erased, drive content accessible.

Table 2

PIN Transition State

PORTS AND INTERFACES

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

Physical Port	Logical Interface Definition	Description
USB Port	Data input Data output Control input Status output	Send and receive control / data packets that support the standard mass storage class. Control and status parameters are only those required to support the USB protocol. There is no connection between a locked LOK-IT and a host computer.
Numeric Button Interface*	Data input	Connects to PIN input buttons used for PIN entry to security controller.
Key Button Interface	Control input	Connects to Key button used to wake module from sleep mode, identify role, and terminate PIN entry.
LED (RGB)	Status output	See table 3 for status states
Power	Battery input USB	+5 volts from USB port charges attached battery
Crystal	Control input	Oscillator used to generate a clock for the 1861 controller.

Table 3

Physical Ports and Logical Interfaces

*Meets level 3 requirements by allowing a plain-text CSP (PIN) to be entered directly into the security controller on a physically separate port than that used for data I/O, see Figure #2.

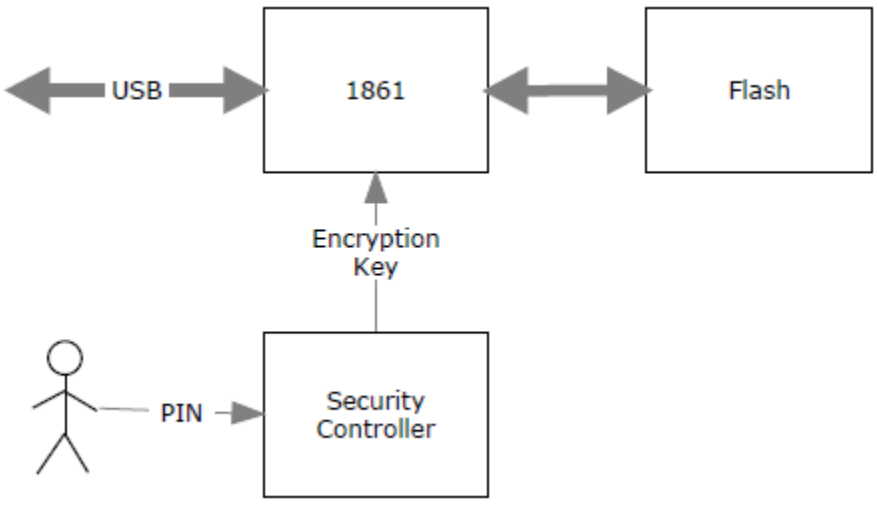

Figure 2

LOK-IT® Architecture

Figure 3 depicts two (2) blinking modes used to convey status as referenced in Table 3.

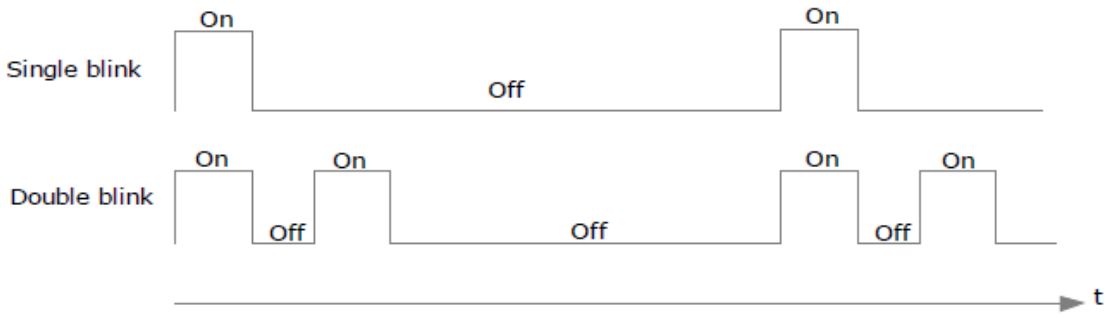

Figure 3

Single vs. Double Blink

LED State	Description
Red single blink	Module is locked, inaccessible
Green single blink	Module unlocked in User role
Green double blink	Module unlocked in CO (Cryptographic Officer) role
Red constant state	No user PIN defined
All indicators off	Module is in sleep mode
Red & Green in constant state	Change of PIN initiated
Red & Green concurrent single blink	Accepting User PIN input
Red & green concurrent double blink	Accepting CO PIN
Blue constant state	USB controller has logical connection with host
Blue blinking	Data packets being read / written

Table 4

Status Output

INDENTIFICATION AND AUTHENTICATION POLICY

LOK-IT® supports level 3 identity based authentication.

Role	Authentication Type	Authentication Data	Description
User	Identity-based operator authentication	User PIN – persistently stored in EEPROM of the security controller.	User has full access to all services.
Crypto-Officer	Identity-based operator authentication	CO PIN – persistently stored in EEPROM of the security controller.	CO has full access to all services; can zeroize user PIN.

Table 5

Roles and Required Identification and Authentication

User Authentication

a) Press KEY - Single blinking red and green indicators

b) Enter PIN - Red and green indicators blinking concurrently

c) Press KEY - Single blinking green means user authenticated, red blink means user denied

CO Authentication

a) Double Press KEY – Double blinking red and green indicators

b) Enter PIN - Red and green indicators blinking concurrently

c) Press KEY - Double blinking green means CO authenticated, red blink means user denied

Customer Delivery

On customer delivery, user and CO PIN's can be set in either order: user before CO or CO before user. In addition, it is possible to use the drive with a user PIN defined and no CO PIN defined. To account for these features, the following rules apply to when setting / changing a PIN is allowed.

User PIN Set	CO PIN Set	Setting / Changing User PIN Allowed	Setting / Changing CO PIN Allowed
No	No	Yes	Yes
No	Yes	Yes	Yes – If drive has been unlocked by CO
Yes	No	Yes – If drive is unlocked by user	No – CO may set PIN if user unlocks 1st to prevent somebody from taking a locked drive and setting CO PIN to unlock
Yes	Yes	Yes – If drive is unlocked by user	Yes – If the drive has been unlocked by CO. It is possible for the CO to set the User PIN.

Table 6

PIN Set/Change Conditions

Authentication Strength

LOK-IT Derivative	PIN Strength
10 Key	Minimum length = 7 digits. Probability of a random guess is 10^7 or 1/10,000,000. The user is locked out after 10 login failures. The probability of 10 consecutive tries is 1/1,000,000.

Table 7

Authentication Strengths

ACCESS CONTROL POLICY

Roles and Services

The LOK-IT® supports 2 distinct and separate roles: user and cryptographic officer. The role is explicitly selected during authentication:

- User – press KEY button, enter valid PIN, press KEY
- CO – double press KEY to identify CO, enter valid PIN, press KEY

Operator	Services
User Role	Open private partition to allow read/write access Lock private partition to disallow read/write access Set user PIN Change user PIN Read/write to private partition
CO Role	Open private partition to allow read/write access Lock private partition to disallow read/write access Set CO PIN Change CO PIN Read/write to private partition Zeroize/set user PIN
Un-Authenticated (no role required)	Show Status Self-Test Zeroize crypto-parameters

Table 8

Services Authorized for Each Role

Initialization

The module is shipped with no authentication CSPs to access the private partition. In this state, the user or CO must first establish a valid PIN in order to open LOK-IT®.

Definition of Critical Security Parameters (CSPs)

The following CSPs are contained within the module:

CSP	Description
AES Encryption Key	256 bit key used to encrypt private partition
User PIN	PIN used to authenticate user
Crypto-Officer PIN	PIN used to authenticate CO
DRBG Seed	Seed for random number generator
DRBG State Variables	Variables for intermediate DRBG states

Table 9

Internal CSPs

Encryption keys are created by a random number generator (RNG) that generates 256 bit keys. When zeroization occurs, the AES encryption key is set to all 0s. The unit is now in the reset state. When either operator then creates a new PIN, a new 256 bit encryption key is generated. The drive will now require formatting.

CSP Access Mode Definitions

A CSP used for authentication

E CSP used executing encryption / decryption

I CSP input using keypad

K CSP created internally when defining new PIN. The AES key is generated by the DRBG only when both user and CO PINs are undefined.

B CSP zeroized when CO opens private partition

Z CSP zeroized after 10 failed attempts to enter a valid PIN

CSP	Service							
	User Opens Private Partition	CO Opens Private Partition	Lock Private Partition	Read/Write Data	Set User PIN	Change User PIN	Set CO PIN	Change CO PIN
AES Key	Z	Z		E	K		K	
User PIN	I, A, Z	B				I		
CO PIN	Z	I, A, Z						I
DRBG Seed	Z	Z			K		K	
DRBG States	Z	Z			K		K	

Table 10

Services to CSP mapping

(1) When CO opens private partition, the user PIN is zeroized. This provides a means of recovering use of the drive in the event the user forgot their PIN.

(2) If 10 consecutive attempts to open the private partition fail, all CSPs are zeroized and drive reverts back to the factory default state. Drive content is no longer accessible.

OPERATIONAL ENVIRONMENT

The FIPS 140-2 area 6 operational environment requirements are not applicable because the module has a limited operational environment.

SECURITY RULES

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

1. The cryptographic module shall provide two distinct operator roles: user and cryptographic officer.
2. The cryptographic module shall provide identity-based authentication.
3. When the module has not been placed in a valid role, the operator shall not have access to any cryptographic service.
4. The cryptographic module performs the following tests when unit wakes from sleep:
   a) AES known answer test
   b) Firmware integrity test (16 bit cyclic redundancy check)
   c) SHA-256 known answer test
   d) Hash_DRBG known answer test
5. During operation the following conditional self-tests occur:
   a) NDRNG continuous test
   b) DRBG continuous test
6. The operator shall be capable of commanding the module to perform the power-up self-test at any time by waking the module from sleep mode.
7. Data output is inhibited during self-tests, zeroization, and authentication.
8. No CSPs are ever output in any form from the module.

PHYSICAL SECURITY POLICY

The multi-chip standalone cryptographic module includes the following physical security mechanisms:

- Production grade components
- Hard, opaque epoxy covering the cryptographic boundary
- EEPROM and Flash memory protect fuses are set in the security controller

The operator should, on a periodic basis, visually inspect the module to determine if it has been compromised. To do this, remove the module enclosure and visually inspect the epoxy and PCB for any evidence of tampering.

Note: The module epoxy hardness testing was only performed at ambient temperature 71° F; no assurance is provided for level 3 hardness conformance at any other temperature.

MITIGATION OF OTHER ATTACKS

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

REFERENCES

Reference Number	Reference Title
[1]	FIPS PUB 140-2 Security Requirements for Cryptographic Modules / NIST May 2001
[2]	Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program / NIST May 22, 2008

Table 11

List of References

DEFINITIONS AND ACRONYMS

AES – Advanced Encryption Standard

CRC – Cyclic Redundancy Check

CSP – Critical Security Parameter

CBC – Cipher Block Chaining

DRBG - Deterministic Random Bit Generator

DRNG - Deterministic Random Number Generator

FIPS – Federal Information Processing Protocol

NDRBG - Non-Deterministic Random Bit Generator

NDRNG - Non-Deterministic Random Number Generator

RNG – Random Number Generator

SHA - Secure Hashing Algorithm