LOK-IT
SECURE FLASH DRIVE™

FIPS 140-2 SECURITY POLICY V.12
For
LOK-IT™ 10 KEY (Series SDG003FM)
&
LOK-IT™ 5 KEY (Series SDG004FP)

© Prepared by ClevX, LLC on behalf of Systematic Development Group, LLC.
May be reproduced only in its original entirety [without revision].

© Prepared by ClevX, LLC on behalf of Systematic Development Group, LLC.
May be reproduced only in its original entirety [without revision].

TABLE OF CONTENTS

© Prepared by ClevX, LLC on behalf of Systematic Development Group, LLC.
May be reproduced only in its original entirety [without revision].

© Prepared by ClevX, LLC on behalf of Systematic Development Group, LLC.
May be reproduced only in its original entirety [without revision].

MODULE OVERVIEW

LOK-IT™ 10 Key (Series SDG003FM)

Hardware revision:	100-SDG003-33LF REV:1
USB controller firmware revision:	V01.12A09-F01
Security controller firmware revision:	SDG003FM-008

LOK-IT™ 5 Key (Series SDG004FP)

Hardware revision:	100-SDG004-00LF REV:1
USB controller firmware revision:	V01.12A09-F01
Security controller firmware revision:	SDG004FP-008

SDG provides FIPS 140-2 approved security functionality to the LOK-IT™USB flash drive[1]. The LOK-IT™ module employs validated Federal Information Processing Standard (FIPS 140-2) 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 PIC16F688 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

© Prepared by ClevX, LLC on behalf of Systematic Development Group, LLC.
May be reproduced only in its original entirety [without revision].

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
Module Ports and Interfaces	3
Roles, Services, and Authentication	3
Finite State Model	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
Physical Security	3

Table 1

Module Security Level Specification

© Prepared by ClevX, LLC on behalf of Systematic Development Group, LLC.
May be reproduced only in its original entirety [without revision].

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 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

Non-Approved Algorithms

There are no non-approved algorithms.

Encryption Keys

LOK-IT™ is pre-programmed with a unique set of encryption keys created during the manufacturing process. A list of 6 AES keys is supplied by a random number generator (RNG) executing on the manufacturer's computer. The RNG complies with ANSI X9.31 Appendix 2.4 specification for the generation of random numbers.

© Prepared by ClevX, LLC on behalf of Systematic Development Group, LLC.
May be reproduced only in its original entirety [without revision].

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 2

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.

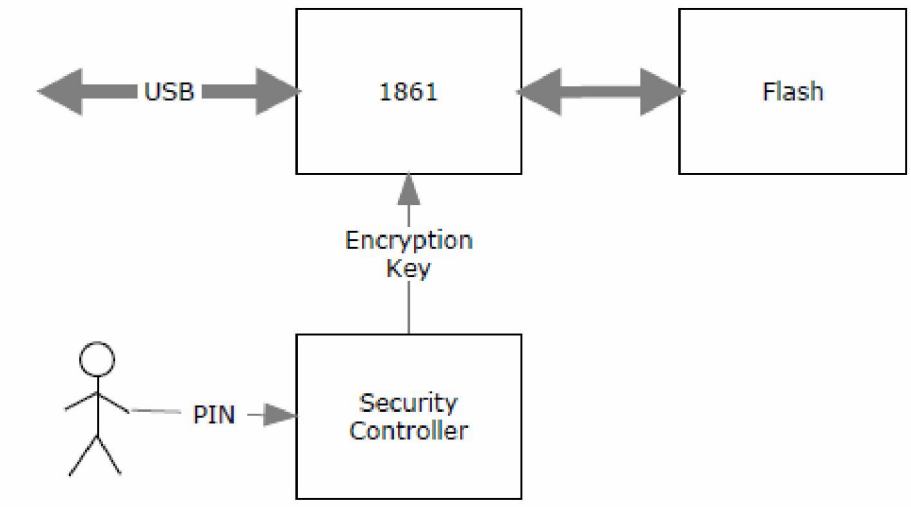

Figure 2

LOK-IT™ Architecture

© Prepared by ClevX, LLC on behalf of Systematic Development Group, LLC.
May be reproduced only in its original entirety [without revision].

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

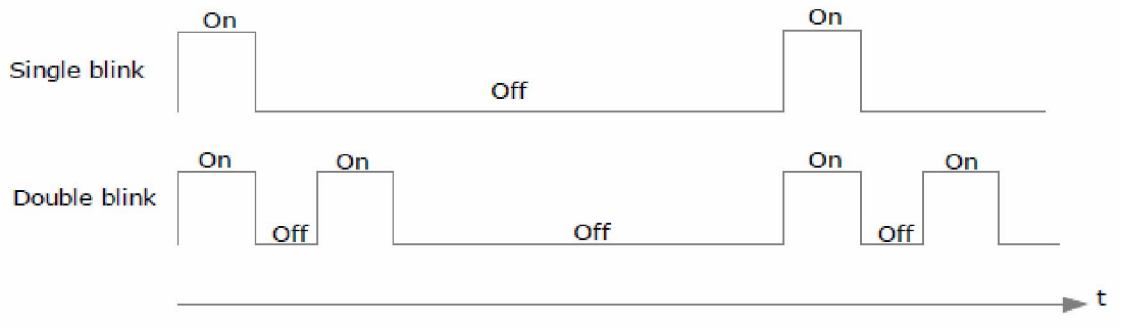

Figure 3

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
Red & Green fade on and off	All encryption keys have been used up. Or, unit failed power-on self test. Module can no longer be used.

Table 3

Status Output

© Prepared by ClevX, LLC on behalf of Systematic Development Group, LLC.
May be reproduced only in its original entirety [without revision].

© Prepared by ClevX, LLC on behalf of Systematic Development Group, LLC.
May be reproduced only in its original entirety [without revision].

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 4

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 - Single 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 5

PIN Set/Change Conditions

© Prepared by ClevX, LLC on behalf of Systematic Development Group, LLC.
May be reproduced only in its original entirety [without revision].

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.
5 Key	Minimum length = 9 digits. Probability of a random guess is 5^9 or 1/1,953,125. The user is locked out after 10 login failures. The probability of 10 consecutive tries is 1/195,312.

Table 6

Authentication Strengths

The probability that a random authentication attempt will succeed within a one-minute period is 10/1,000,000 and 10/1,193,125 respectively.

As can be seen by the pictures on page 3, the 10 key LOK-IT™ drive has 10 numeric buttons whereas the 5 key LOK-IT™ has 5 numeric buttons. The buttons are labeled 0/1, 2/3, 4/5, 6/7, 8/9. This is why the minimum PIN length is set to 9 digits instead of 7.

Since 2 numerals share the same button, the PIN 1-1-1-1-1-5-5-5-5 is electrically equivalent to 0-0-0-0-0-4-4-4-4. Hence, the need for a longer PIN.

© Prepared by ClevX, LLC on behalf of Systematic Development Group, LLC.
May be reproduced only in its original entirety [without revision].

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

Table 7

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 encrypt the private partition. Only 1 key is used to encrypt/decrypt the private partition.
User PIN	PIN used to authenticate the user
Crypto-Officer PIN	PIN used to authenticate the CO

Table 8

Internal CSPs

Each LOK-IT™ module is manufactured with 6 AES encryption keys. Only 1 of these keys is used to encrypt / decrypt data. The remaining 5 keys have no relationship to stored data.

When zeroization occurs, the AES encryption key at the top of the list is erased; the next key becomes the key used to encrypt the private partition. Given enough zeroizations, all keys will be consumed and the drive becomes inoperable.

© Prepared by ClevX, LLC on behalf of Systematic Development Group, LLC.
May be reproduced only in its original entirety [without revision].

CSP Access Mode Definitions

- A CSP is used for authentication
- D CSP is used for decrypting data
- E CSP is used for encrypting data
- I CSP is input using the keypad
- Z CSP is zeroized

CSP	User Role					CO Role				
	Open Private Partition	Close Private Partition	Read / Write Data	Change User PIN	Failed Login	Open Private Partition	Close Private Partition	Read / Write Data	Change CO PIN	Failed Login
AES Key			E, D		Z (2)			E, D		Z (2)
User PIN		I, A		I, A	Z (2)	Z (1)				Z (2)
CO PIN					Z (2)	I, A			I, A	Z (2)

Table 9

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.

© Prepared by ClevX, LLC on behalf of Systematic Development Group, LLC.
May be reproduced only in its original entirety [without revision].

OPERATIONAL ENVIRONMENT

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

© Prepared by ClevX, LLC on behalf of Systematic Development Group, LLC.
May be reproduced only in its original entirety [without revision].

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:
   a) AES known answer test
   b) Firmware integrity test (16 bit cyclic redundancy check)
5. 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.
6. Data output is inhibited during self-tests, zeroization, and authentication.
7. No CSPs are ever output in any form from the module.

© Prepared by ClevX, LLC on behalf of Systematic Development Group, LLC.
May be reproduced only in its original entirety [without revision].

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 memory protect fuse is 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; no assurance is provided for level 3 hardness conformance at any other temperature.

© Prepared by ClevX, LLC on behalf of Systematic Development Group, LLC.
May be reproduced only in its original entirety [without revision].

MITIGATION OF OTHER ATTACKS

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

© Prepared by ClevX, LLC on behalf of Systematic Development Group, LLC.
May be reproduced only in its original entirety [without revision].

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 10

List of References

© Prepared by ClevX, LLC on behalf of Systematic Development Group, LLC.
May be reproduced only in its original entirety [without revision].

DEFINITIONS AND ACRONYMS

AES – Advanced Encryption Standard

CRC – Cyclic Redundancy Check

CSP – Critical Security Parameter

CBC – Cipher Block Chaining

FIPS – Federal Information Processing Protocol

RNG – Random Number Generator

© Prepared by ClevX, LLC on behalf of Systematic Development Group, LLC.
May be reproduced only in its original entirety [without revision].