Kanguru Solutions Kanguru Biolock 1.0.1.8
Security Policy

Document Version 1.2

FIPS 140-2 Level 1 Validation

1 Introduction

This document is the Security Policy for Kanguru Solutions Kanguru Biolock cryptographic module. This Security Policy specifies the security rules under which the module shall operate to meet the requirements of FIPS 140-2 Level 1. It describes how the module functions to meet the FIPS requirements, and the actions that operators must take to maintain the security of the module.

This Security Policy describes the features and design of the module using the terminology contained in the FIPS 140-2 specification. *FIPS 140-2, Security Requirements for Cryptographic Modules* specifies the security requirements that must be satisfied by a cryptographic module utilized within a security system protecting sensitive but unclassified information. The NIST Cryptographic Module Validation Program (CMVP) validates cryptographic modules to FIPS 140-2 and other cryptography-based standards. Validated products are accepted by the Federal agencies of both the USA and Canada for the protection of sensitive or protected information.

The FIPS 140-2 standard, and information on the CMVP program, can be found at http://csrc.nist.gov/cryptval. More information describing the Kanguru Biolock application can be found at http://www.kanguru.com.

In this document, the Kanguru Biolock application is also referred to as “the module”.

This Security Policy contains only non-proprietary information. All other documentation submitted for FIPS 140-2 conformance testing and validation is “Kanguru Solutions’ – Proprietary” and is releasable only under appropriate non-disclosure agreements.

The cryptographic module meets the overall requirements applicable to Level 1 security for FIPS140-2. The operating environment used in testing was Windows XP Service Pack 2.

Table 1. Cryptographic Module Security Requirements

Security Requirements Section	*Level*
Cryptographic Module Specification	1
Cryptographic Module Ports and Interfaces	1
Roles and Services and Authentication	1
Finite State Machine Model	1
Physical Security	N/A
Operational Environment	1
Cryptographic Key Management	1
EMI/EMC	1
Self-Tests	1
Design Assurance	1
Mitigation of Other Attacks	N/A

1.1 Acronyms and Abbreviations

AES	Advanced Encryption Standard
CBC	Cipher Block Chaining
CFB	Cipher Feedback
CMVP	Cryptographic Module Validation Program
CSE	Communications Security Establishment
CSP	Critical Security Parameter
DES	Data Encryption Standard
EDC	Error Detection Code
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FCC	Federal Communication Commission
FIPS	Federal Information Processing Standard
HMAC	Keyed-Hash Message Authentication Code
KAT	Known Answer Test
LAN	Local Area Network
NIST	National Institute of Standards and Technology
PUB	Publication
RAM	Random Access Memory
RFC	Request for Comment
ROM	Read Only Memory
RNG	Random Number Generator
RSA	Rivest Shamir and Adleman Public Key Algorithm
SHA	Secure Hash Algorithm

2 Cryptographic Module

2.1 Functional Overview

The module enables users to store data in encrypted format on a Kanguru Solutions' USB 2.0 flash drive device which includes an optical fingerprint reader. Users can copy or drag and drop plaintext data files into the Kanguru Biolock application that appears as a virtual drive in Windows. The Kanguru Biolock application stores AES encrypted data on the virtual drive. It also decrypts data retrieved from the virtual drive. Users authenticate to the application by entering a password and swiping the fingerprint over the fingerprint reader.

Features of the software include:

- Operator authentication
- AES (256-bit key) data encryption

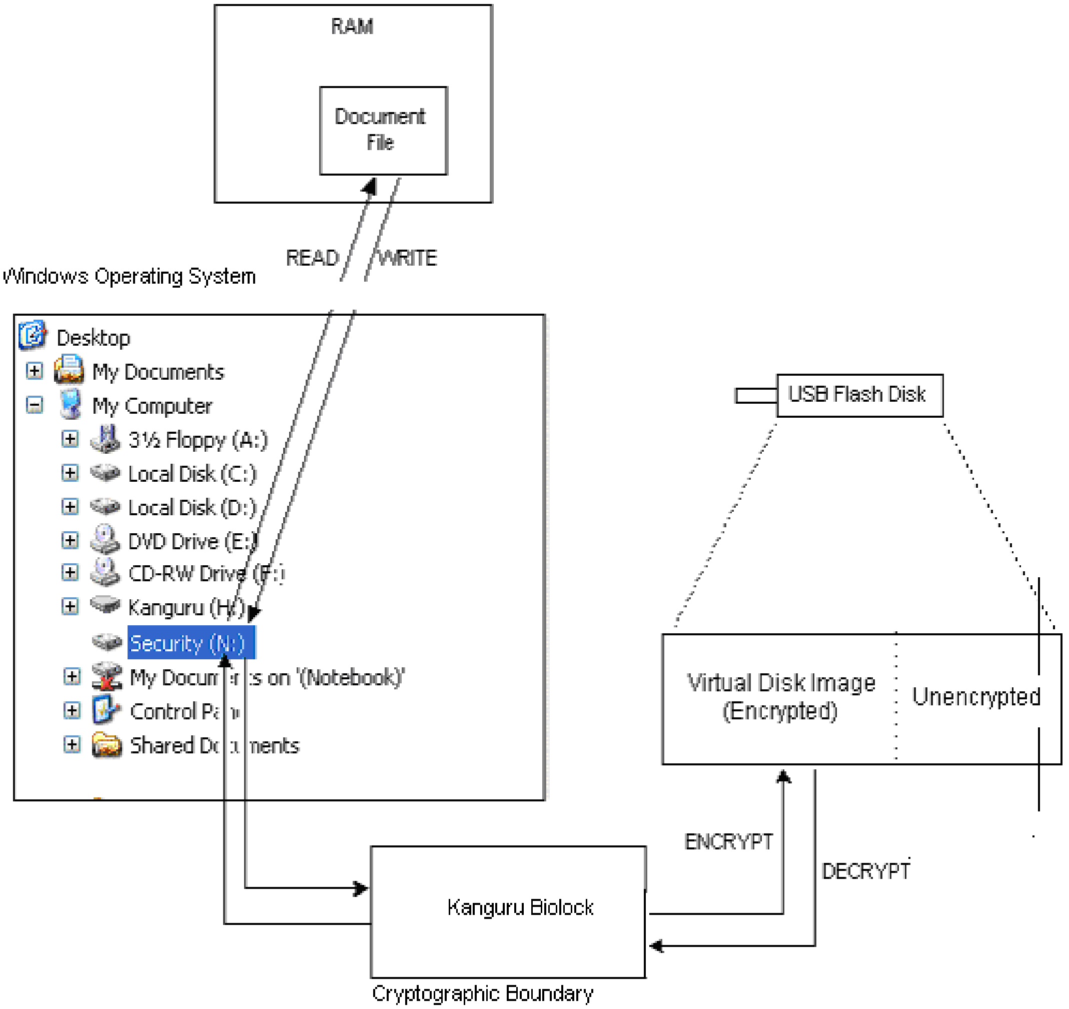
Figure 1 illustrates module operation. Once the Kanguru Biolock application is installed, a user inserts the flash drive into a USB connector. The plaintext virtual drive (drive H: in this example) opens and is available. The ciphertext virtual drive (drive N: in this example) is unavailable until the user authenticates by entering the correct password in the module's password dialog box and swiping a finger over the fingerprint reader. On successful authentication, the module mounts the ciphertext virtual drive and provides data encryption and decryption services to the user. Users can also change the authentication password and regenerate the data encryption key as needed.

The USB drive includes two partitions. The encrypted partition stores the encrypted data (files). The unencrypted partition stores the module binaries.

When the user plugs in the USB drive into the PC, the module binaries are installed from the USB drive to the PC. Then the module automatically executed on the PC. After the user enters the correct password, the data on the encrypted drive become available.

Figure 1. High Level Functional View of the Cryptographic Module.

.



2.2 Module Description

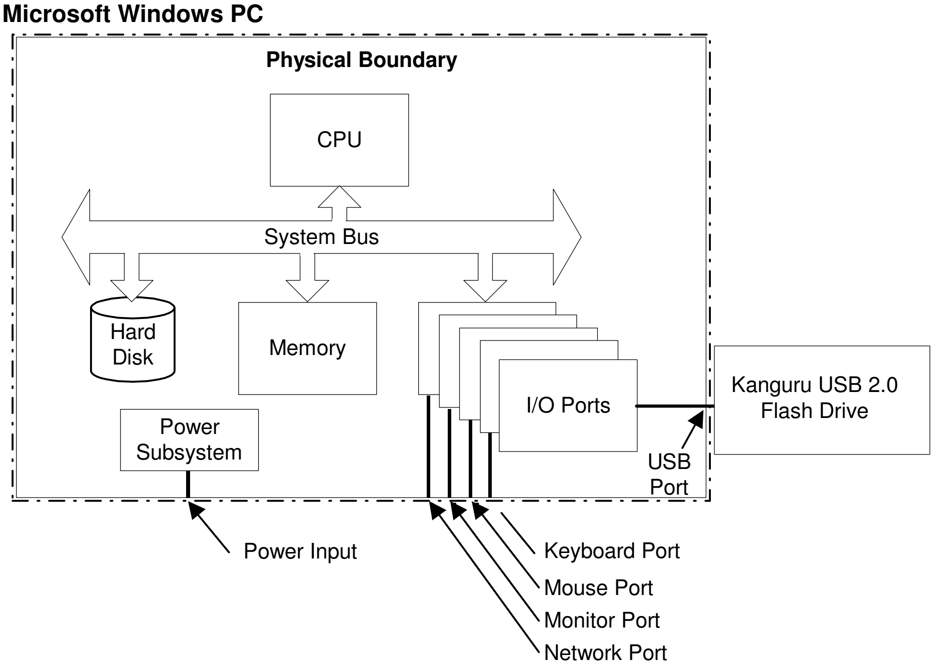
The module is a multi-chip standalone cryptographic module consisting of application software that executes on a general-purpose computing platform that is a Microsoft® Windows®-based PC, configured in single-user mode. The module stores AES-encrypted files off the module in a USB 2.0 flash drive system. The module uses a general purpose operating environment: Microsoft Windows XP. The module meets FIPS 140-2 level 1 security requirements.

The module provides authentication, cryptographic key management, and software integrity services assuring operators of a valid software state within the module and privacy services for the secure storage of data, cryptographic keys, and CSPs. The module does not have a bypass or maintenance mode.

2.3 High Level Block Diagram

Figure 2 shows a block diagram of the cryptographic module that illustrates the physical boundary of the module and shows the module physical interfaces. The physical cryptographic boundary is the physical boundary of the PC case.

Figure 2. High Level Block Diagram Showing Physical Boundaries.



Figures 1 shows a logical block diagram of the cryptographic module illustrating Kanguru Biolock application, operating system and the cryptographic boundary of the module.

The cryptographic boundary includes all application files, as listed below:

- BioLockLauncher.exe
- KanguruBioLock.exe
- cryptopp.dll
- HWCtrlAGX.dll
- brftSWP.dll
- GetMinuSWP.dll
- Kyqual.dll
- brmatchSWP.dll
- MatchSWP.dll
- LangDEU.dll

- LangENG.dll
- LangFRA.dll
- HDS4KG.dll

The following files are excluded from requirements of FIPS 140-2 as not security relevant: LangDEU.dll LangENG.dll, LangFRA.dll

Note: the cryptographic boundary includes software Crypto++ module cryptopp.dll, which was previously validated at Security Level 1 (Cert. #819).

BioLockLauncher.exe is used to copy the module binaries from the flash drive to the temporary directory on the GPC when the flash drive is inserted into the USB port of the GPC. The KanguruBioLock.exe application then runs from temp directory on the GPC.

2.4 Module Ports and Interfaces

The cryptographic module has 10 physical interfaces and four logical interfaces. The physical ports have the functions described in Table 2. Where distinct logical interfaces share the same physical port, the system timing, software and hardware protocols, software APIs, and other controls logically separate and isolate these distinct categories of data from one another. The internal system bus acts as the physical path for clocking data into and out of the module. System synchronization and timing controls ensure that logically distinct categories of data do not occupy the data path at the same time.

Table 2. Physical Interfaces and Logical Interfaces.

Physical Interface	*FIPS 140-2 Logical Interface*
PC USB port, PC network port, keyboard interface, mouse port, hard drive, floppy drive, CDROM drive	Data input interface
PC USB port, PC network port, keyboard interface, mouse port, hard drive, floppy drive, CDROM drive	Data output interface
PC keyboard port, mouse port, PC power button	Control input interface
PC monitor	Status output interface
PC power interface	Power interface

- -

The physical interfaces map to logical interfaces as described in Table 3.

Table 3. FIPS 140-2 Logical Interfaces.

Logical Interface	*Description*
Data input	The data input is: • All plaintext data entering the Kanguru Biolock application for the purpose of being encrypted and stored on an external USB flash drive. • All ciphertext data entering the Kanguru Biolock application from the external USB flash drive for the purpose of being decrypted.
Data output	The data output is: • All plaintext data exiting the Kanguru Biolock application. • All ciphertext data exiting the Kanguru Biolock application for storage on an external USB flash drive.
Control input	The Kanguru Biolock application accepts control input from the operator.

Logical Interface	*Description*
	Control input consists of all commands and command parameters.
Status output	The status output consists of all messages either logged by the module or returned by the module, and all status data obtained as a result of user commands.

3 FIPS Approved Mode of Operation

The module's Approved mode of operation is restricted to performing only FIPS-approved cryptographic algorithms and security functions.

The following steps must be performed to configure the module in the Approved mode of operation.

1. Configure Windows XP in single user mode.

2. Plug in the USB drive. Initial setup window will be displayed.

3 Set the password in the initial setup window.

4. Enroll a fingerprint by swiping a finger over the drive's optical scanner.

After this the module is configured in the approved mode of operation.

Note: the module does not implement non-approved algorithms and does not define a separate non-Approved mode of operation.

Note: disconnecting the USB drive without properly closing the Biolock application can lead to unpredictable crashes and may leave traces of plaintext data on the USB drive. As a precaution, to stay in the Approved mode, the operator shall always properly close the application before removing the USB drive.

Note: editing files from within the Biolock window and then disconnecting the USB drive without properly closing the Biolock application may leave traces of plaintext data on the USB drive. As a precaution, the operator shall copy files to the Biolock window only after the edits have been completed.

Module users must protect the password from discovery by others. Users must not write the password and leave it where others can find it. They should ensure no one is watching when entering the password.

Note: the USB drive includes the module binaries. When the USB drive is inserted into the PC, the module is automatically installed from the USB drive to the PC by copying binaries to the PC.

4 Identification and Authentication

The module supports a crypto officer role and a user role. The crypto officer and user may be different people or they may be the same person performing role-specific module operations.

The crypto officer role is implicitly assumed by the operator configuring the module. Crypto officer operations consist of configuring the PC in single user mode and running the setup program.

The user role becomes available once the user takes possession of the module by setting the password and enrolling the fingerprint. Approved mode operations available to the user include changing the password, using the module data encryption and decryption services, and reset to factory defaults.

Multiple concurrent operators are not allowed as the module is restricted to single user mode. Operators cannot change roles while authenticated to the module. The module does not display the password entered into the module. Users must disable the hint feature for FIPS Approved mode operation. Access to the authorized roles is restricted as explained in Table 4.

Table 4. Roles and Required Identification and Authentication.

Role	Type of Authentication	Authentication Data
Crypto Officer	Role-based	The crypto officer authenticates to the Microsoft Windows XP operating system before installing and configuring the module for use. Once a user has taken possession of the module by setting the password and enrolling the fingerprint , the crypto officer role becomes unavailable.
User	Role-based	An operator must enter the correct password and swipe the finger over the fingerprint reader to assume the user role.

The module does not require any physical maintenance.

5 Cryptographic Keys and CSPs

The following table identifies the Cryptographic Keys and Critical Security Parameters (CSPs) employed within the module. All keys inside the logical boundary are stored in RAM and can be zeroized by powering off the PC.

Table 5. Cryptographic Keys and CSPs.

Data Item	*Description*
Storage Key (SK)	256-bit AES key used to encrypt files. Generated by the module.
Security Key	256-bit AES key used to encrypt the fingerprint. Generated by the module.
Key Encryption Keys	These keys are used to obfuscate the Storage Key and the Security Key. The keys are not compliant since they are derived from the user password. Since Key Encryption Keys do not provide FIPS 140-2 compliant encryption, For the purposes of FIPS 140-2 the Storage Key and the Security Key are considered to be non-encrypted (plaintext) keys.
Password	The password is a 8 to 31 character password that is used to authenticate the user. The password derives an AES key that obfuscates the SK. If the password-derived key successfully decrypts the SK, authentication is successful. The password is not stored on the USB drive and needs to be entered by the user during the authentication. Note: The password is never stored in any permanent storage. When it is entered during the user authentication it is temporary stored in the RAM on the GPC where the module is executed, but is never saved to any permanent storage. SHA-256 hash of the password is stored on the USB drive. When the password is entered, it is hashed and compared to the stored hash value.
ANSI X9.31 RNG seed	Used to seed the ANSI X9.31 RNG. Generated by the module.
ANSI X9.31 RNG seed key	The ANSI X9.31 RNG seed key. Generated by the module.
HMAC Key	Used for the strong integrity check. Hardcoded into the embedded Crypto++ module.
DSA Public Key	Used for the strong integrity check. Hardcoded into the module.

6 Roles and Services

The module supports services that are available to crypto officers and users. All of the services are described in detail in the module's user documentation.

The crypto officer role (unauthenticated) accesses the module initialization service, available only when the Kanguru Biolock application is installed on a PC platform but not yet initialized. The crypto officer role becomes unavailable after the module is initialized.

The user role becomes available after the operator sets the password and enrolls the fingerprint. The operator must enter the correct password and swipe the finger over the image scanner to assume the User role. An authenticated user accesses all module services (except initialization).

Table 6 shows the services available to the various roles.

Table 6. Roles and Services

Service	*Crypto Officer / Owner*	*User*
Install the module	X	
Reset to factory defaults		X
Change Password		X
Change Fingerprint		X
Read/Write encrypted files and directories		X
View version information		X
Run Self-Tests		X
Show Status		X
Zeroize Keys		X
Authenticate		X

The services are described below:

Install the module - perform initial installation steps for the module.

Reset to factory defaults – reset the module to the factory default state. This will reformat the USB drive and erase all secret keys stored on the drive. The user can execute "Reset to Factory defaults" service by clicking the "Reset to factory defaults" button in the Kanguru BioLock login window.

Read/Write encrypted files and directories – reads or writes information from or to the USB drive encrypting file contents on write and decrypting file contents on read.

View version information – outputs application version information

Run Self-Tests – runs self-tests on demand by restarting the module. To restart the module one needs to exit and restart KanguruBioLock.exe application.

Change Password - changes the password.

Show Status - shows status of the module. In an error state, the module displays a message box specifying the error that occurred, and then exits. If self-tests pass successfully, the module shows a secure drive image in Windows.

Zeroize Keys – all keys inside the logical boundary are stored in RAM and are zeroized by powering off the PC.

Authenticate – authenticate to the module using the password and the fingerprint

7 Access Control

Table 7 shows services that use or affect cryptographic keys or CSPs. For each service, the key or CSP is indicated along with the type of access.

R - The item is **read** or referenced by the service.
W - The item is **written** or updated by the service.
E - The item is **executed** by the service. (The item is used as part of a cryptographic service.)
D - The item is **deleted** by the service.

Table 7. Access Control.

Key or CSP	*Service*	*Access Control*
Key Encryption Keys	Reset to Factory Defaults	R,E,D, W
	Change Password	R,E,D, W
	Change Fingerprint	R, E
	Authenticate	R,E
	Zeroize	D
	Read/Write files	R,E
Storage Key	Reset to Factory Defaults	R,E, D, W
	Change Password	R,E,D,W
	Authenticate	R,E
	Read/write files	R,E
	Zeroize	D
Security Key	Reset to Factory Defaults	R,E, D, W
	Change Password	R,E,D,W
	Change Fingerprint	R, E
	Authenticate	R,E
	Read/write files	R,E
	Zeroize	D
Fingerprint	Reset to Factory Defaults	R,E,D, W
	Change Fingerprint	R,E,D, W
	Read/write files	R, E
	Zeroize	D
	Authenticate	R,E
Password	Reset to Factory Defaults	R,E,D, W
	Change Password	R,E,D, W
	Authenticate	R,E
	Read/write files	R, E
	Zeroize	D

8 Approved Security Functions.

Approved Security Functions implemented by the module are specified in the table below.

Table 9. Approved Security Functions.

Algorithm	Certificate Number
AES	499
SHS	569
HMAC	253
ANSI X9.31 RNG	279
DSA	206
Triple-DES	512

9 Self Tests

The module performs both power-on self test (POST) and conditional self tests to verify the integrity and correct operational functioning of the cryptographic module. If the system fails a self test, it reports status indicating which failure occurred and transitions to an error state. The C++ functions that run the self-test do not include any calls to output data and this blocks all traffic on the data ports, preventing use of any cryptographic keys, CSPs, cryptographic algorithms, and security functions except as needed by the self tests. If self-tests fail, the module displays a message box specifying the error that occurred, and then exits. If self-tests pass successfully, the module shows a secure drive image in Windows.

To indicate failure of self-tests, the module issues a Windows API command to display an error message box containing a description of the error. To indicate success of self-tests, the module issues a Windows API command to display a secure drive in Windows.

The user can run self-tests on demand by using the Run Self Tests service, which amounts to restarting the module. Table 8 summarizes the system self tests.

Table 10. Self Tests.

Self Test	*Description*
Mandatory power-up tests performed at power-up and on demand:	
Cryptographic Algorithm Known Answer Tests	Each cryptographic algorithm (AES, SHA, HMAC, SHS, and RNG) performed by the module, is tested using a "known answer" test to verify the operation of the function. The AES known answer performs both encryption and decryption. Note: the Crypto++ module implement the algorithms (AES, SHA, HMAC, SHS, and RNG) and perform the KAT.
Software Integrity Test	The module verifies the integrity of the software using DSA signatures. In addition, the embedded Crypto++ module uses HMAC to check its integrity.
Conditional tests performed, as needed, during operation:	
Continuous RNG	This test checks the RNG output data for failure to a constant value.

Known answer tests for encryption/decryption or hashing, function by encrypting (or hashing) a string for which the calculated output is known and stored within the cryptographic module. An encryption or hashing test passes when the freshly calculated output matches the expected (stored) value. A test fails when the calculated outmatch does not match the expected value. The test then decrypts the ciphertext string. A decryption test passes when the freshly calculated output matches the plaintext value. A test fails when the calculated output does not match the plaintext value.

Known answer tests for Random Number Generators function by seeding the RNG with known values and checking that the output matches the pre-calculated value stored within the cryptographic module. The test passes when the freshly generated output matches the pre-calculated value. A test fails when the generated outmatch does not match the pre-calculated value.

10 References

National Institute of Standards and Technology, *FIPS PUB 140-2: Security Requirements for Cryptographic Modules*, available at URL: http://www.nist.gov/cmvp.

National Institute of Standards and Technology, *FIPS 140-2 Annex A: Approved Security Functions*, available at URL: http://www.nist.gov/cmvp.

National Institute of Standards and Technology, *FIPS 140-2 Annex B: Approved Protection Profiles*, available at URL: http://www.nist.gov/cmvp.

National Institute of Standards and Technology, *FIPS 140-2 Annex C: Approved Random Number Generators*, available at URL: http://www.nist.gov/cmvp.

National Institute of Standards and Technology, *FIPS 140-2 Annex D: Approved Key Establishment Techniques*, available at URL: http://www.nist.gov/cmvp.

National Institute of Standards and Technology and Communications Security Establishment, *Derived Test Requirements (DTR) for FIPS PUB 140-2, Security Requirements for Cryptographic Modules*, available at URL: http://www.nist.gov/cmvp.

National Institute of Standards and Technology, *Data Encryption Standard (DES)*, Federal Information Processing Standards Publication 46-3, available at URL: http://www.nist.gov/cmvp.

National Institute of Standards and Technology, *DES Modes of Operation*, Federal Information Processing Standards Publication 81, available at URL: http://www.nist.gov/cmvp.

National Institute of Standards and Technology, *Digital Signature Standard (DSS)*, Federal Information Processing Standards Publication 186-2, available at URL: http://www.nist.gov/cmvp.

National Institute of Standards and Technology, *Secure Hash Standard (SHS)*, Federal Information Processing Standards Publication 180-1, available at URL: http://www.nist.gov/cmvp.