IronKey Secure Flash Drive Cryptographic Module

IronKey, Inc.

Security Policy

(Document Version 1.2)

April 3, 2008

Copyright IronKey, Inc. 2008. May be reproduced only in its original entirety [without revision].

TABLE OF CONTENTS

1. MODULE OVERVIEW 3

2. SECURITY LEVEL 4

3. MODES OF OPERATION 5

4. PORTS AND INTERFACES 5

5. IDENTIFICATION AND AUTHENTICATION POLICY 5

6. ACCESS CONTROL POLICY 7

ROLES AND SERVICES 7
UNAUTHENTICATED SERVICES 7
DEFINITION OF CRITICAL SECURITY PARAMETERS (CSPS) 8
DEFINITION OF CSPS MODES OF ACCESS 9

7. OPERATIONAL ENVIRONMENT 11

8. SECURITY RULES 11

9. PHYSICAL SECURITY POLICY 12

PHYSICAL SECURITY MECHANISMS 12
OPERATOR REQUIRED ACTIONS 12

10. MITIGATION OF OTHER ATTACKS POLICY 12

11. DEFINITIONS AND ACRONYMS 13

1. Module Overview

The IronKey Secure Flash Drive Cryptographic Module (HW P/Ns 46.012.001.01 Version 1.0, 46.012.001.02 Version 1.0, 46.012.001.04 Version 1.0, and 46.012.001.08 Version 1.0; FW Version 1.3) is a multi-chip standalone cryptographic module designed to provide secure data storage and operator authentication. The module under validation includes four configurations, which differ only in flash size and are physically identical:

- HW P/N 46.012.001.01 Version 1.0 includes 1GB flash
- HW P/N 46.012.001.02 Version 1.0 includes 2GB flash
- HW P/N 46.012.001.04 Version 1.0 includes 4GB flash
- HW P/N 46.012.001.08 Version 1.0 includes 8GB flash

The cryptographic boundary is defined as being the outer perimeter of the epoxy potting.

Figure 1 – Image of Cryptographic Module in Typical External Metallic Packaging

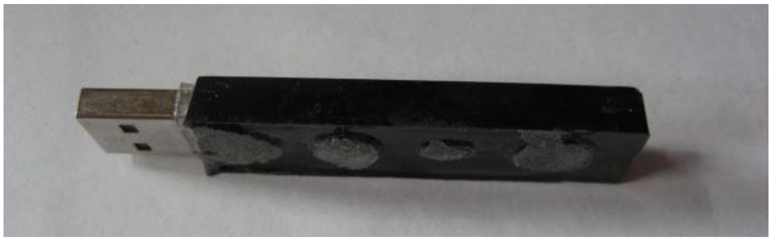

Figure 2 – Image of Cryptographic Module at Cryptographic Boundary

When the module is connected to a PC, it mounts two drives: a secure volume and a CD drive. All files mounted within the CD drive are excluded from the cryptographic boundary as they cannot execute within the cryptographic boundary and only exist for storage. The applications included in the CD drive are as follows:

- Firefox
- Password Manager
- Control Panel
- The Onion Router (TOR)
- BackUp

The cryptographic boundary does not include the metallic case and USB cap of the IronKey Secure Flash Drive. The potting (cryptographic boundary) provides sufficient physical security; compromising the exterior metallic casing does not compromise the security of the device.

No excluded components process CSPs, plaintext data, or other information that if misused could lead to a compromise.

2. Security Level

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

Table 1 - Module Security Level Specification

Security Requirements Section	Level
Cryptographic Module Specification	3
Module Ports and Interfaces	3
Roles, Services and Authentication	3
Finite State Model	2
Physical Security	2
Operational Environment	N/A
Cryptographic Key Management	3
EMI/EMC	3
Self-Tests	2
Design Assurance	3
Mitigation of Other Attacks	N/A

3. Modes of Operation

Approved mode of operation

The module only supports an Approved mode of operation. The operator can verify that the firmware version matches the Approved version by clicking on the Control Panel application that interfaces with the IronKey Secure Flash Drive with CAPSLOCK on. The module supports the following FIPS Approved algorithms:

- AES
- SHA-256
- SHA-1, SHA-256
- RSA Sign/Verify
- ANSI X9.31 DRNG, Appendix A.2.4.

The module supports the following non-Approved algorithms:

- NDRNG
- RSA Encrypt/Decrypt (key wrapping; key establishment methodology provides 112 bits of encryption strength)
- TDES (used for authentication only; non-compliant)

4. Ports and Interfaces

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

-	USB:	Data In/Out, Control In, Status Out, Power In
-	Two-color LED:	Status Output

5. Identification and Authentication Policy

Assumption of roles

The cryptographic module supports three distinct roles, the User, Cryptographic Officer, and the Server. Only one User and one Cryptographic Officer are supported by the module. All previous authentications are cleared upon power cycling the module.

Table 2 - Roles and Required Identification and Authentication

Role	Type of Authentication	Authentication Data
User	Identity-based operator authentication	Password Digest Verification
Cryptographic Officer	Identity-based operator authentication	Digital Signature Verification or Knowledge of Shared Secret
Server	Identity-based operator authentication	Digital Signature Verification

Table 3 – Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
Password Digest, 256-bits	The probability that a random attempt will succeed or a false acceptance will occur is 1/2^256, which is less than 1/1,000,000. The module can be configured to restrict the number of consecutive authentication failures to a value between one and 239 before it destroys the contents. The probability of successfully authenticating to the module within one minute through random attempts is less than 1/100,000.
Digital Signature Verification, 2048-bit keys.	The probability that a random attempt will succeed or a false acceptance will occur is 1/2^112, which is less than 1/1,000,000. The probability of successfully authenticating to the module within one minute through random attempts is less than 1/100,000 due to performance limitations of the USB interface and of the processor.
Knowledge of Shared Secret, 112-bits	The probability that a random attempt will succeed or a false acceptance will occur is 1/2^112, which is less than 1/1,000,000. The module can perform a maximum of three consecutive authentication failures before the module is zeroized. The probability of successfully authenticating to the module within one minute through random attempts is 3/2^112, which is less than 1/100,000.

6. Access Control Policy

Roles and Services

Table 4 – Services Authorized for Roles

Role	Authorized Services
User:	- Secure Data Storage: Safely store your data within the flash. - Change Password: Modify the User password. - Get Public Key: Retrieve a public key from the module. - Import Public/Private Key - Format Drive: Re-initialize the secure volume. - Lock Device: Logout and prohibit access to the flash. - Login: Authenticate to the module. - Device Recovery: Assist the module to recover from a lost password. - Admin Management: Configure the module to assist in Device Recovery. - Authenticate to External Server: Instruct the module to generate a digital signature for the purpose of authenticating to an external server.
Cryptographic Officer:	- Firmware Upgrade: Update the firmware. - Zeroize: Destroy all plaintext CSPs within the device.
Server	- Policy Import: Configure the module's policy.

Unauthenticated Services

The cryptographic module supports the following unauthenticated services:

- Show Status: Provides the current status of the cryptographic module through the LED.
- Self-Tests: Executes the power-on self-tests and is invoked by a power cycle.

Definition of Critical Security Parameters (CSPs)

Table 5 – Module CSPs

K-Device Private Key:	Facilitates key transport.
Admin Authentication Key:	Facilitates CO authentication.
C-Browser Private Key:	Authenticates the module to external entities.
K-Subscription Private Key:	Authenticates the module to external entities.
Shared Admin Private Key:	RSA unwraps the Password Recovery Key.
Secure Volume Key:	Provides data protection for the flash drive contents.
Box AES Key:	Provides data protection for application data.
Password Recovery Key:	Facilitates password recovery.
Password:	Authenticates the User.
DRNG State:	Used to generate random numbers.
Secure Channel Key:	Provides data protection for communications between the module and applications.

Definition of Public Keys

Table 6 - Module Public Keys

K-Device Public Key:	Facilitates key transport.
Peer Public Key:	Facilitates key transport for a peer device.
C-Browser Public Key:	Authenticates the module to external entities.
K-Subscription Public Key:	Authenticates the module to external entities.
Shared Admin Public Key:	RSA wraps the Password Recovery Key.
Server Public Key:	Digital signature verification.
Enterprise Public Key:	RSA wraps the Password Recovery Key.
FW Upgrade Public Key:	Authenticates firmware images.

Definition of CSPs Modes of Access

Table 7 defines the relationship between access to CSPs and the different module services. The modes of access shown in the table are defined as follows:

- Read
- Use
- Write

Table 7 - CSP Access Rights within Roles & Services

Role			**Service**	**Cryptographic Keys and CSPs Access Operation**
C.O.	**User**	**Server**		
	X		Secure Data Storage	Use Secure Volume Key Use Box AES Key, Use Secure Channel Key
	X		Change Password	Read/Write Password Use Secure Channel Key
	X		Get Public Key	Use Secure Channel Key
	X		Import Public/Private Key	Use K-Device Private Key Use Secure Channel Key
	X		Format Drive	Use Secure Channel Key Use Secure Volume Key
	X		Login	Read, Use Secure Channel Key Read, Use Password Read Box AES Key
	X		Lock Device	Use Secure Channel Key
	X		Device Recovery	Use Secure Channel Key Use Shared Admin Private Key, C-Browser Private Key Use Password Recovery Key
	X		Admin Management	Use Secure Channel Key Use C-Browser Private Key
	X		Authenticate to External Server	Use Secure Channel Key Use K-Subscription Private Key Use C-Browser Private Key

X			Firmware Upgrade	Use Secure Channel Key
X			Zeroize	Write All CSPs Use Admin Authentication Key
		X	Policy Import	Use Secure Channel Key

7. Operational Environment

The FIPS 140-2 Area 6 Operational Environment requirements are not applicable because the device does not contain a modifiable operational environment. The module only allows the loading of trusted, validated code that is signed by IronKey.

8. Security Rules

The cryptographic module's design corresponds to the cryptographic module's security rules. This section documents the security rules enforced by the cryptographic module to implement the security requirements of this FIPS 140-2 Level 2 module.

1. The cryptographic module shall provide three distinct roles. These are the User role, the Server role and the Cryptographic-Officer role.
2. The cryptographic module shall provide identity-based authentication.
3. When an operator has not been authenticated to a valid role, the operator shall not have access to any cryptographic services.
4. The cryptographic module shall clear previous authentications upon power off.
5. The cryptographic module shall perform the following tests:

   <u>Power up Self-Tests:</u>

   1. Cryptographic algorithm tests:
      a. AES Known Answer Test
      b. SHA-1, SHA-256 Known Answer Test
      c. SHA-256 Known Answer Test
      d. RSA Sign/Verify Pairwise Consistency Test
      e. RSA Encrypt/Decrypt Pairwise Consistency Test
      f. DRNG Known Answer Test

   2. Firmware Integrity Test (RSA Signature Verification)
   3. Critical Functions Tests: N/A.

   <u>Conditional Self-Tests:</u>

   1. Continuous RNG test – performed on NDRNG and DRNG

   2. Firmware Load Test

6. At any time, the operator shall be capable of commanding the module to perform the

power-up self-test.

7. Data output shall be inhibited during key generation, self-tests, zeroization, and error states.
8. Status information shall not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
9. The module shall not support concurrent operators or a maintenance role.
10. The module shall not support a bypass capability.
11. The module does not support the plaintext entry or output of CSPs.
12. All secret and private keys shall be entered in an encrypted format.
13. No secret or private keys shall be output by the module in plaintext.
14. The module shall provide the means to zeroize all CSPs.
15. The module shall not support manual key entry.
16. The module shall not allow an operator to change roles.
17. The module shall not support the output of intermediate key generation values.
18. The module shall not support the entry of seed keys.
19. The module shall not support split-knowledge key entry procedures.
20. The module shall not generate asymmetric key pairs.

9. Physical Security Policy

Physical Security Mechanisms

The cryptographic module includes the following physical security mechanisms:

- Production-grade components
- Hard potting material encapsulation of multiple chip circuitry enclosure with removal/penetration attempts causing serious damage.

Operator Required Actions

The operator is required to periodically inspect the external potting for tamper evidence.

10. Mitigation of Other Attacks Policy

The module has not been designed to mitigate attacks beyond the scope of FIPS 140-2 requirements.

11. Definitions and Acronyms

AES - Advanced Encryption Standard
CM - Configuration Management
CO - Cryptographic Officer
DRNG - Deterministic Random Number Generator
GPC - General Purpose Computer
LED - Light Emitting Diode
NDRNG - Non-Deterministic Random Number Generator
PC - Personal Computer
RAM - Random Access Memory
ROM - Read Only Memory
RSA - Rivest Shamir Adelman
SHA - Secure Hash Algorithm
TDES - Triple-Data Encryption Standard
TOR- The Onion Router