IronKey S250/D250

Kingston Technology Company, Inc.

Security Policy

(Document Version 1.1)

May 19, 2016

TABLE OF CONTENTS

1. Module Overview

The IronKey S250/D250, hereafter referred to as the IronKey Secure Flash Drive or the cryptographic module, is a multi-chip standalone cryptographic module designed to provide secure data storage and operator authentication. The module under validation includes the following configurations, which differ only in flash size and are physically identical:

IronKey S250 (FW Version: 4.0.0)	
Hardware P/N	*SLC* Flash Size*
D2-S250-S01	1 GB
D2-S250-S02	2 GB
D2-S250-S04	4 GB
D2-S250-S08	8 GB
D2-S250-S16	16 GB
D2-S250-S32	32 GB
IKS250 Series [1GB, 2GB, 4GB, 8GB, 16GB, 32GB],	1 GB, 2 GB, 4 GB, 8 GB, 16 GB, 32 GB

* SLC Flash = Single-Level Cell Flash

IronKey D250 (FW Version: 4.0.0)	
Hardware P/N	*MLC* Flash Size*
D2-D250-B01	1 GB
D2-D250-B02	2 GB
D2-D250-B04	4 GB
D2-D250-B08	8 GB
D2-D250-B16	16 GB
D2-D250-B32	32 GB
D2-D250-B64	64 GB
IKD250 Series [1GB, 2GB, 4GB, 8GB, 16GB, 32GB, 64GB]	1 GB, 2 GB, 4 GB, 8 GB, 16 GB, 32 GB, 64 GB

* MLC Flash = Multi-Level Cell Flash

The cryptographic boundary is defined as being the outer perimeter of the metallic enclosure and is depicted below.

Figure 1 – Image of the Cryptographic Module (S250)

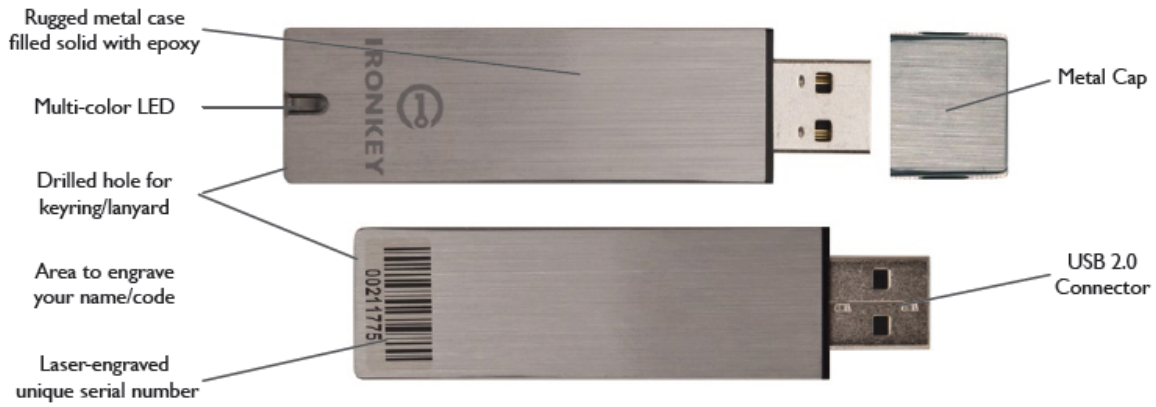
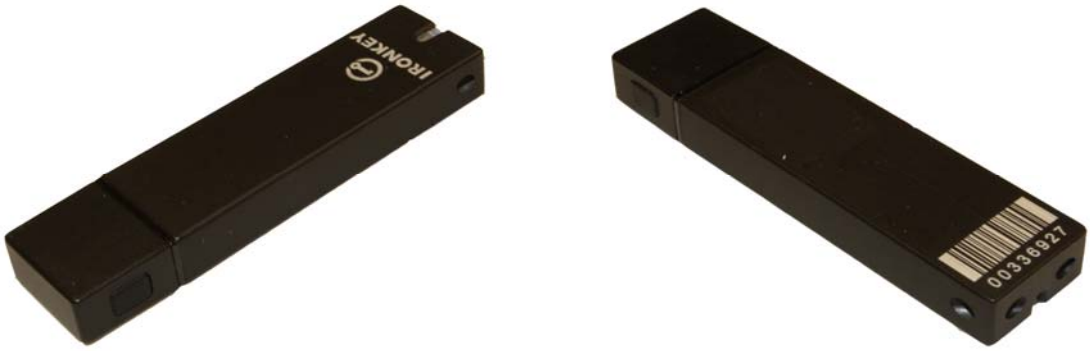


Figure 2 – Images of the Cryptographic Module (D250)



When the IronKey Secure Flash Drive is connected to a PC, it mounts two drives: a secure volume and a CD drive. All files mounted within the CD drive are outside the logical boundary of the cryptographic module, as they cannot execute within the cryptographic boundary, cannot lead to a compromise of the module's security, and exist for storage only; however, the CD drive contents are read-only and protected by digital signature to prevent unauthorized modification and substitution. Files distributed with the module mounted within the internal CD Drive are excluded from the validation.

2. Security Level

The cryptographic module meets the overall requirements applicable to Level 3 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	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

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 128, 192, 256-bit (Cert. #1412)
- AES 256-bit (Cert. #1874)
- SHA-1, SHA-256 (Cert. #1282)
- SHA-256 (Cert. #1647)
- HMAC SHA-256 (Certs. #1118, #1119)
- FIPS 186-2 RSA Sign/Verify (Cert. #688)
- FIPS 186-2 RSA Sign/Verify (Cert. #954)
- FIPS 186-3 RSA Verify (Cert. #955)
- SP800-90 DRBG (Cert. #152)
- Triple-DES (Cert. #965)
- ANSI X9.31 RNG (Cert. #774)
- PBKDF2 (Per SP800-132, vendor affirmed)

The module supports the following non-Approved algorithms which are allowed for use in the FIPS Approved mode of operation:

- NDRNGs
- RSA Key Transport (key wrapping; key establishment methodology provides 112 bits of encryption strength)

4. Ports and Interfaces

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

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

5. Identification and Authentication Policy

Assumption of roles

The cryptographic module supports three distinct roles, the User, the Cryptographic Officer, and the Server. 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 Hash
Cryptographic Officer	Identity-based operator authentication	Digital Signature Verification
Server	Identity-based operator authentication	Digital Signature Verification

Table 3 – Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
Password Hash Verification	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, through policy, to a value between one and 239 before it zeroizes all data and CSP contents of the module (Default is 10). The probability of successfully authenticating to the module within one minute through random attempts is less than 1/100,000.
Digital Signature Verification, 1024 or 2048-bit keys.	The probability that a random attempt will succeed or a false acceptance will occur is 1/2^80, 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.

* Note: The original authentication data for the User is assumed to meet the 1/1,000,000 strength requirements defined in Section 4.3.3 in FIPS 140-2.

6. Access Control Policy

Roles and Services

Table 4 – Services Authorized for Roles

Role	Authorized Services
User	- Login: Initialize the device and allow the operator to authenticate. - Secure Data Storage: Safely store your data within the flash. - Change Password: Modify the User password. - Format Drive: Re-initialize the secure volume. - Get Version: Retrieve current version information. - Lock Device: Logout the User and prohibit access to the flash. - Get Public Key: Retrieve a public key from the module. - RSA Sign/Verify: Create or verify a digital signature with a specified key. - RSA Wrap/Unwrap: RSA encrypt/decrypt a key value with a specified key. - Get Random: Request a random number from the module. - Generate Key Pair: RSA key pair is created using the internal RNG. - Read Application Key: Retrieve an application's stored AES key. - Application Data Access: Support data read/write privileges to secure portions of flash allocated to an application. - Import Key Pair: Enter a public or private RSA key into the module's secure storage.
Cryptographic Officer	- Firmware Upgrade: Update the firmware or CD Update Public Key.
Server	- Policy Import: Configure the module's policy. - Access Restrictions: Authorize or prohibit User authentication. This service may also be used to force a User to specify a new password. - Device Recovery: Assist the recovery of a module with a lost password. - Device Reset: Recommissions a device for a new employee. - Self-Destruct: Zeroize the device.

Unauthenticated Services

The cryptographic module supports the following unauthenticated services:

- Show Status: Provides the current status of the cryptographic module through error codes and the LED.
- Self-Tests: Executes the power-on self-tests and is invoked by a power cycle.
- Basic Reset: Re-initializes the device for a new User.

For additional information, please see the IronKey User Guide.

Definition of Critical Security Parameters (CSPs)

Table 5 –CSPs

Device Private Key:	2048-bit RSA key. Facilitates key transport.
Login Private Key:	2048-bit RSA key. Facilitates key transport.
Browser Private Key:	2048-bit RSA key. Authenticates the device to the IronKey Server.
User Private Keys:	2048-bit RSA key. Used at the discretion of the User.
Subscription Private Key:	2048-bit RSA key. Authenticates the device to the TOR.
Master Key:	256-bit AES key used to encrypt the Secure Volume Key.
Secure Volume Key:	256-bit AES key. Provides data protection for the flash drive contents.
Password Hash:	SHA-256 hash of the User's password. Authenticates the User.
Device Recovery Key:	256-bit HMAC SHA-256 Key. Facilitates device recovery.
DRBG Seed Key and Seed:	Used to generate random numbers.
DRNG Seed Key and Seed:	Used to generate random numbers.
Box AES Keys:	256-bit AES key. Provides data protection for application data.
Identity Manager Key:	256-bit AES key. Provides data protection for the identity application data.
Secure Session Encryption Key:	256-bit AES key. Provides data protection for communications between the module and the host device.
Secure Session Integrity Key:	HMAC-SHA-256 key. Provides data integrity for the channel between the module and the host device.
Secure Channel Encryption Keys:	128-bit Triple-DES keys. Provides data protection for communications between the module and a Server.
Secure Channel Integrity Keys:	128-bit Triple-DES keys. Provides data integrity for communications between the module and a Server.
Subscriber Security Domain (SSD) Keys	128-bit Triple-DES keys. Provides data protection and integrity for firmware updates.

Definition of Public Keys

Table 6 - Public Keys

Device Public Key:	2048-bit RSA key. Facilitates key transport and signature verification.
P-Controller Session Public Key:	2048-bit RSA key. Facilitates key transport.
Server Public Key:	2048-bit RSA key. Digital signature verification and key transport.
Host Public Key:	2048-bit RSA key. Digital signature verification and key transport.
Browser Public Key	2048-bit RSA key. Used by the Server to authenticate the device.
User Public Keys	2048-bit RSA key. Used at the discretion of the User.
Subscription Public Key	2048-bit RSA key. Used by the TOR to authenticate the device.
Data Authentication Pattern Public Key:	1024-bit RSA key. Digital signature verification.
CD Update Public Key:	2048-bit RSA key. Digital signature verification.
Login Public Key	2048-bit RSA key. Facilitates authentication between device and Host.
Token Public Key	1024-bit RSA Key. Digital signature verification.

Definition of CSPs Modes of Access

Table 7 defines the relationship between access to CSPs and the different module services. Note that all User services are issued through an AES 256-bit encrypted secure channel and potentially additionally encrypted by a 128-bit Triple-DES encrypted secure session. The modes of access shown in the table are defined as follows:

- Read
- Write
- Destroy

Table 7 - CSP Access Rights within Roles & Services

Role			**Service**	**Cryptographic Keys and CSPs Access Operation**
C.O.	**User**	**Server**		
	X		Login	Read, Write Secure Session Encryption Key, Secure Session Integrity Key, Secure Channel Encryption Key, Secure Channel Integrity Key, Login Private Key, DRBG Seed Key and Seed, DRNG Seed Key and Seed, Master Key, Device Recovery Key Read Password Hash Destroy All Plaintext CSPs (if authentication retry limit is exceeded)

Role			Service	Cryptographic Keys and CSPs Access Operation
C.O.	User	Server		
	X		Secure Data Storage	Read Secure Session Encryption Key, Secure Session Integrity Key, Secure Channel Encryption Key, Secure Channel Integrity Key, Device Private Key, Secure Volume Key, Box AES Keys
	X		Change Password	Read/Write Password Hash, Master Key Read Secure Session Encryption Key, Secure Session Integrity Key, Secure Channel Encryption Key, Secure Channel Integrity Key, Device Private Key
	X		Format Drive	Read Secure Session Encryption Key, Secure Session Integrity Key, Secure Channel Encryption Key, Secure Channel Integrity Key, Device Private Key
	X		Get Version	Read Secure Session Encryption Key, Secure Session Integrity Key, Secure Channel Encryption Key, Secure Channel Integrity Key, Device Private Key
	X		Lock Device	Read Secure Session Encryption Key, Secure Session Integrity Key, Secure Channel Encryption Key, Secure Channel Integrity Key, Device Private Key
	X		Get Public Key	Read Secure Session Encryption Key, Secure Session Integrity Key, Secure Channel Encryption Key, Secure Channel Integrity Key, Device Private Key
	X		RSA Sign/Verify	Read Secure Session Encryption Key, Secure Session Integrity Key, Secure Channel Encryption Key, Secure Channel Integrity Key, Device Private Key, RSA Private Keys
	X		RSA Wrap/Unwrap	Read Secure Session Encryption Key, Secure Session Integrity Key, Secure Channel Encryption Key, Secure Channel Integrity Key, Device Private Key, RSA Private Keys
	X		Get Random	Read Secure Session Encryption Key, Secure Session Integrity Key, Secure Channel Encryption Key, Secure Channel Integrity Key, Device Private Key Read/Write RNG Seed and Seed Key
	X		Generate Key Pair	Read Secure Session Encryption Key, Secure Session Integrity Key, Secure Channel Encryption Key, Secure Channel Integrity Key, Device Private Key, DRNG Seed and Seed Key Write User Private Keys
	X		Read Application Key	Read Secure Session Encryption Key, Secure Session Integrity Key, Secure Channel Encryption Key, Secure Channel Integrity Key, Device Private Key, Identity Manager Key
	X		Application Data Access	Read Secure Session Encryption Key, Secure Session Integrity Key, Secure Channel Encryption Key, Secure Channel Integrity Key, Device Private Key, Box AES Keys, RSA Private Keys

Role			Service	Cryptographic Keys and CSPs Access Operation
C.O.	User	Server		
	X		Import Key Pair	Read Secure Session Encryption Key, Secure Session Integrity Key, Secure Channel Encryption Key, Secure Channel Integrity Key, Device Private Key Write User Private Keys
X			Firmware Upgrade	Read Secure Session Encryption Key, Secure Session Integrity Key, SSD Keys
		X	Policy Import	Read Secure Session Encryption Key, Secure Session Integrity Key, Secure Channel Encryption Key, Secure Channel Integrity Key, Box AES Key, Device Private Key
		X	Access Restrictions	Read Secure Session Encryption Key, Secure Session Integrity Key, Secure Channel Encryption Key, Secure Channel Integrity Key, Device Private Key
		X	Device Recovery	Read Secure Session Encryption Key, Secure Session Integrity Key, Secure Channel Encryption Key, Secure Channel Integrity Key, Device Recovery Key, Password Hash, Login Private Key, Device Private Key
		X	Device Reset	Read Secure Session Encryption Key, Secure Session Integrity Key, Secure Channel Encryption Key, Secure Channel Integrity Key, Device Private Key Destroy User Private Keys, Box AES Key
		X	Self-Destruct	Read Secure Session Encryption Key, Secure Session Integrity Key, Secure Channel Encryption Key, Secure Channel Integrity Key, Device Private Key Destroy all CSPs
X	X	X	Show Status	N/A
X	X	X	Self-Tests	N/A
X	X	X	Basic Reset	Read Secure Session Encryption Key, Secure Session Integrity Key, Secure Channel Encryption Key, Secure Channel Integrity Key, Device Private Key Destroy User Keys, Box AES 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 Kingston Technology Company, Inc.

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 3 module.

1. The cryptographic module shall provide three distinct roles. These are the User role, the Cryptographic-Officer role, and the Server 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:

   Power up Self-Tests:

   1. Cryptographic algorithm tests:
      a. AES 256-bit Known Answer Tests
      b. SHA-1, SHA-256 Known Answer Tests
      c. HMAC SHA-256 Known Answer Tests
      d. RSA Sign/Verify Known Answer Tests
      e. RSA Decrypt Known Answer Test
      f. SP800-90 DRBG Known Answer Test
      g. Triple-DES Known Answer Test
      h. ANSI X9.31 RNG Known Answer Test
      i. PBKDF2 Known Answer Test
   2. Firmware Integrity Test (16-bit EDCs)
   3. Critical Functions Tests: N/A.

   Conditional Self-Tests:

   1. Continuous RNG Tests: Performed on NDRNGs, ANSI X9.31 RNG, and SP800-90 DRBG
   2. Firmware Load Test (RSA Signature Verification)
   3. Pairwise Consistency Tests (RSA Sign/Verify and Encrypt/Decrypt)
6. Successful completion of self-tests is indicated by the loading of the control panel and login screen.
7. At any time, the operator shall be able to command the module to perform the power-up self-tests by power cycling the module.
8. Data output shall be inhibited during key generation, self-tests, zeroization, and error states.
9. Status information shall not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
10. The module shall not support concurrent operators or a maintenance role.
11. The module shall not support a bypass capability.
12. The module does not support the plaintext entry or output of CSPs. All secret and private keys shall be entered and output in encrypted format.
13. The module shall not support manual key entry or split-knowledge key entry procedures.
14. The module shall not allow an operator to change roles without reauthenticating first.

15. The module shall not support the output of intermediate key generation values.
16. The module shall not support the entry of seed keys.
17. Keys derived from passwords as shown in SP800-132 shall only be used for storage applications.

9. Physical Security Policy

Physical Security Mechanisms

The cryptographic module includes the following physical security mechanisms:

- Production-grade components
- Hard metallic composite enclosure

Operator Required Actions

The operator is required to periodically inspect the enclosure 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
ANSI	American National Standards Institute
CD	Compact Disc
CM	Configuration Management
CO	Cryptographic Officer
CSP	Critical Security Parameter
DES	Data Encryption Standard
DRBG	Deterministic Random Bit Generator
DRNG	Deterministic Random Number Generator
EDC	Error Detection Code
FIPS	Federal Information Processing Standard
GPC	General Purpose Computer
HMAC	Keyed-Hash Message Authentication Code
NDRNG	Non-Deterministic Random Number Generator
PBKDF	Password-based Key Derivation Function
PC	Personal Computer
RAM	Random Access Memory
RNG	Random Number Generator
ROM	Read Only Memory
RSA	Rivest Shamir Adelman
SHA	Secure Hash Algorithm
TDES	Triple Data Encryption Standard
TOR	The Onion Router