IronKey S300/D300

IronKey, Inc.

Security Policy

(Document Version 1.0)

December 10, 2010

TABLE OF CONTENTS

1. Module Overview

The IronKey S300/D300, hereafter referred to as the IronKey Secure Flash Drive, 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 S300 (FW Version 2.1.0)	
Hardware P/N	*SLC* Flash Size*
D2-S300-S01	1 GB
D2-S300-S02	2 GB
D2-S300-S04	4 GB
D2-S300-S08	8 GB
D2-S300-S16	16 GB

* SLC Flash = Single-Level Cell Flash

IronKey D300 (FW Version 2.1.0)	
Hardware P/N	*MLC* Flash Size*
D2-D300-B01	1 GB
D2-D300-B02	2 GB
D2-D300-B04	4 GB
D2-D300-B08	8 GB
D2-D300-B16	16 GB
D2-D300-B32	32 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 (S300)

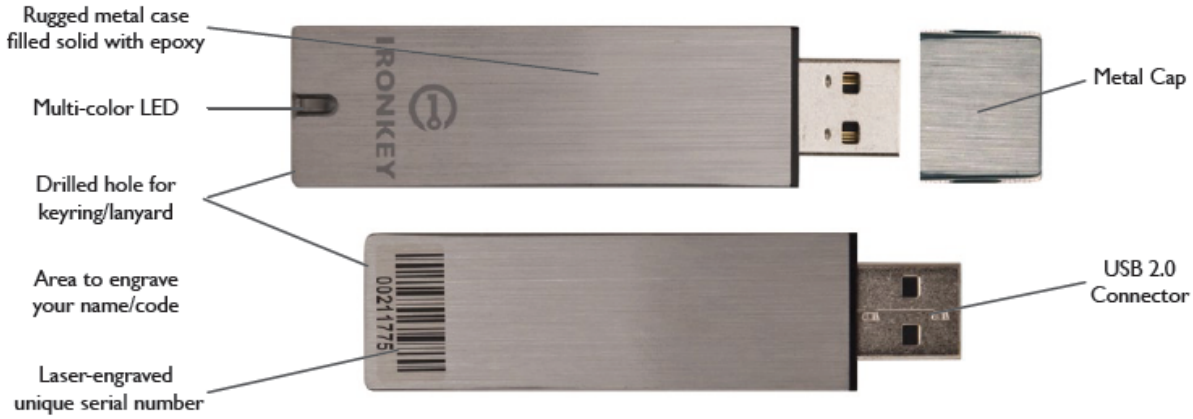
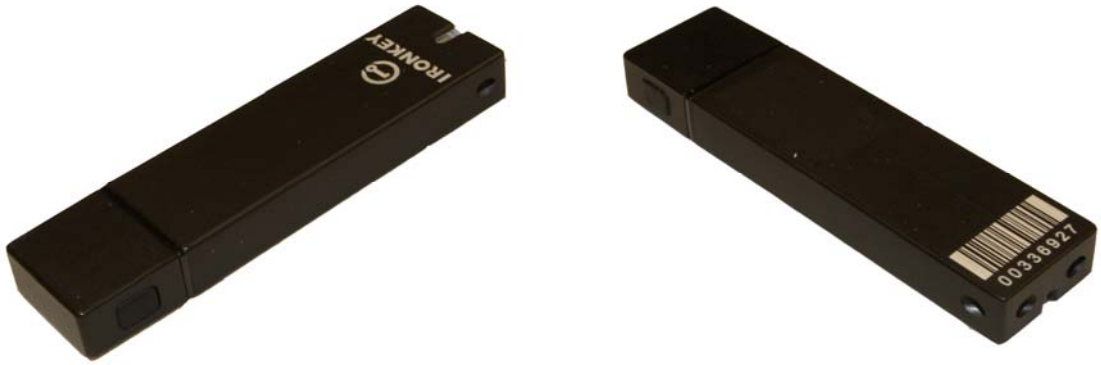


Figure 2 – Image of the Cryptographic Module (D300)



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 256-bit (Cert. #1034)
- SHA-256 (Cert. #987)
- HMAC SHA-256 (Cert. #579)
- SHA-1, SHA-256 (Cert. #1154)
- RSA Sign/Verify (Cert. #605)
- NIST-Recommended ANSI X9.31 RNG with AES (Cert. #587)
- ANSI X9.31 RNG (Cert. #702)

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

- NDRNG
- 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 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. All services are passed through a Secure Channel, encrypted with 256-bit AES.

Table 2 - Roles and Required Identification and Authentication

Role	Type of Authentication	Authentication Data
User	Identity-based operator authentication	256-bit Password Digest*
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 Digest 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, 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.

* 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. - Regenerate Secure Volume Key: Generates a new AES key for securing user data. - 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 AES Key: Retrieve an application's stored AES key (the Back Up & Identity Manager Key). - Application Data Access: Support data read/write privileges to secure portions of flash allocated to an application. - Import Public/Private Key: Enter a public or private RSA key into the module's secure storage. - Export Shared Admin Private Key: Output the RSA wrapped Shared Admin Key - Format Drive: Re-initialize the secure volume. - User Reset: Returns the device to factory defaults. - Refurbish: Returns the device to factory defaults, but maintains user certificates. - Lock Device: Logout the User and prohibit access to the flash. - Device Recovery: Assist the recovery of a module with a lost password. - OTP Support: The module can be used to facilitate OTP authentication to an external server. - Get Version: Retrieve current version information. - Get Status: Retrieve non-security relevant device status.
Cryptographic Officer	- Firmware Upgrade: Update the firmware.
Server	- Policy Import: Configure the module's policy. - Silver Bullet: Authorize or prohibit User authentication. This service may also be used to zeroize the IronKey drive.

Unauthenticated Services

The cryptographic module supports the following unauthenticated services:

- Show Status: Provides the current status of the cryptographic module through the LED. The module indicates successful completion of initialization and power-on self-tests by blinking the LED a solid green once. If there is a failure during initialization or power-on self-tests, the module will cease operation and will indicate failure by blinking the LED red.
- Self-Tests: Executes the power-on self-tests and is invoked by a power cycle.
- Blind Reset: Returns the device to factory defaults, if enabled by policy.
- Zeroize: Destroys all data and plaintext CSPs stored within the module.

For additional information, please see the IronKey User Guide.

Definition of Critical Security Parameters (CSPs)

Table 5 – Module 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 module to external entities.
User Private Key:	2048-bit RSA key. User keys imported or generated for general use.
Subscription Private Key:	2048-bit RSA key. Authenticates the module to external entities.
Shared Admin Private Key:	2048-bit RSA key. RSA unwraps the Password Recovery Key.
Secure Volume Key:	256-bit AES key. Provides data protection for the flash drive contents.
Box AES Key:	256-bit AES key. Provides data protection for application data.
Certificate Manager Key	256-bit AES key. Provides data protection for PKCS#11 certificates.
Back Up & Identity Manager Key:	256-bit AES key. Facilitates back-up and identity management.
Password Hash:	SHA-256 hash of the User's password. Authenticates the User.
RNG Seed Key and Seed:	Used to generate random numbers.
Secure Channel Key:	256-bit AES key. Provides data protection for communications between the module and a Server.
Secure Channel MAC Key:	HMAC-SHA-256 key. Provides data integrity for the channel between the module and a Server.
Secure Login Key:	256-bit AES key. Provides data protection for communication between the module and the Host PC.
Password Recovery Key:	256-bit AES key. Facilitates password recovery.
Firmware Integrity Key	HMAC-SHA-256 key. Performs the firmware integrity test at power-up.
Firmware Encryption Key	256-bit AES key. Provides AES-256 bit protection of the firmware.

Definition of Public Keys

Table 6 - Module Public Keys

Device Public Key:	Facilitates key transport.
Login Public Key:	Facilitates key transport.
Peer Device Public Key:	Facilitates key transport for a peer device.
C-Browser Public Key:	Authenticates the module to external entities.
C-User Public Key:	User imported or generated public key for general purpose.
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.
Service Public Key:	Digital signature verification.
Enterprise Public Key:	RSA wraps the Password Recovery Key.
Firmware Upgrade Public Key:	Authenticates firmware images.

Note: All public keys are 2048-bit RSA keys.

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. 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 Channel Key, Secure MAC Key, Secure Login Key, RNG Seed Key and Seed Read Password Hash
	X		Secure Data Storage	Read Secure Volume Key Read Box AES Keys
	X		Change Password	Read/Write Password Hash, Password Recovery Key
	X		Regenerate Secure Volume Key	Write RNG Seed Key and Seed, Secure Volume Key
	X		Get Public Key	N/A
	X		RSA Sign/Verify	Read RSA Private Key

Role			Service	Cryptographic Keys and CSPs Access Operation
C.O.	**User**	**Server**		
	X		RSA Wrap/Unwrap	Read Device Private Key, Login Private Key, Shared Admin Private Key
	X		Get Random	Read, Write RNG Seed Key and Seed
	X		Generate Key Pair	Write User Private Key Read RNG Seed Key and Seed
	X		Read AES Key	Read Back-Up and Identity Manager Key
	X		Application Data Access	Read Box AES Keys, Subscription Private Key
	X		Import Public/Private Key	Read Device Private Key
	X		Export Shared Admin Private Key	Read Shared Admin Private Key
	X		Format Drive	N/A
	X		User Reset	Destroy All CSPs, except Device Private Key, Login Private Key, Firmware Integrity Key, and Firmware Encryption Key
	X		Refurbish	Destroy All CSPs, except Device Private Key, Login Private Key, Firmware Integrity Key, Firmware Encryption Key, and Certificate Manager Key
	X		Lock Device	N/A
	X		Device Recovery	Read Shared Admin Private Key, Browser Private Key Read Password Recovery Key
	X		OTP Support	Read RNG Seed Key and Seed, Box AES Key
	X		Get Version	N/A
	X		Get Status	N/A
X			Firmware Upgrade	Read Firmware Encryption Key
		X	Policy Import	Read Box AES Key
		X	Silver Bullet	Read/Write Secure Channel Key, Secure Channel MAC Key or Destroy All CSPs
X	X	X	Show Status	N/A
X	X	X	Self-Tests	N/A
X	X	X	Blind Reset	Destroy All CSPs, except Device Private Key, Login Private Key, Firmware Integrity Key, and Firmware Encryption 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 3 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:

   Power up Self-Tests:

   1. Cryptographic algorithm tests:
      a. AES 256-bit Known Answer Test
      b. SHA-1, SHA-256 Known Answer Test
      c. SHA-256 Known Answer Test
      d. HMAC SHA-256 KAT (Tested as a part of the Firmware Integrity Test)
      e. RSA Sign/Verify Pairwise Consistency Test
      f. RSA Encrypt/Decrypt Pairwise Consistency Test
      g. NIST-Recommended ANSI X9.31 RNG based on AES Known Answer Test
      h. ANSI X9.31 RNG Known Answer Test
   2. Firmware Integrity Test (RSA 2048-bit Signature Verification and HMAC SHA-256)
   3. Critical Functions Tests: N/A.

   Conditional Self-Tests:

   1. Continuous RNG Tests: Performed on NDRNG, ANSI X9.31 RNG, and NIST Recommended ANSI X9.31 RNG
   2. Firmware Load Test (RSA 2048-bit Signature Verification)
   3. Pairwise Consistency Test
6. At any time, the operator shall be able to command 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. All secret and private keys shall be entered and output in encrypted format.

12. The module shall provide the means to zeroize all CSPs.
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. The only User-invoked method by which to zeroize all CSPs contained within the module is to exceed the authentication retry count described in Table 3 above. The retry count is adjustable and once exceeded, the module will zeroize all data and CSP contents of the module, rendering the device inoperable and unrecoverable.

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. **Note: No operating and storage temperature ranges were provided to the lab, so the module hardness testing was only performed at ambient temperature; no assurance is provided for Level 3 hardness conformance at any other temperature.**
- 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
CM	Configuration Management
CO	Cryptographic Officer
GPC	General Purpose Computer
HMAC	Keyed-Hash Message Authentication Code
LED	Light Emitting Diode
NDRNG	Non-Deterministic Random Number Generator
OTP	One-Time Password
PC	Personal Computer
RAM	Random Access Memory
RNG	Random Number Generator
ROM	Read Only Memory
RSA	Rivest Shamir Adelman
SHA	Secure Hash Algorithm