IronKey H350

Imation Corp.

FIPS 140-2 Non-Proprietary Security Policy

(Document Version 1.0)

April 1, 2015

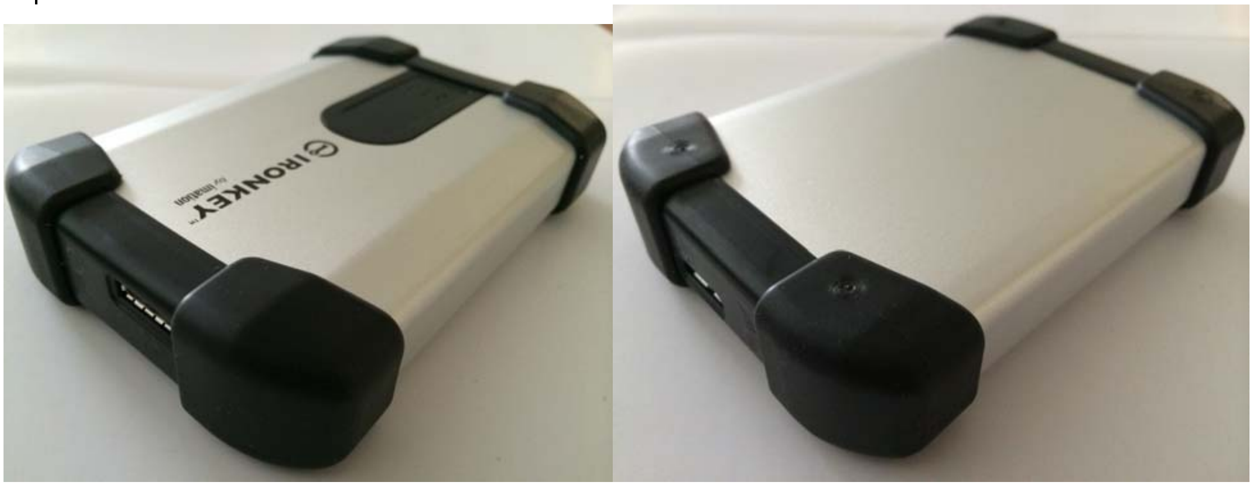
TABLE OF CONTENTS

1. Module Overview

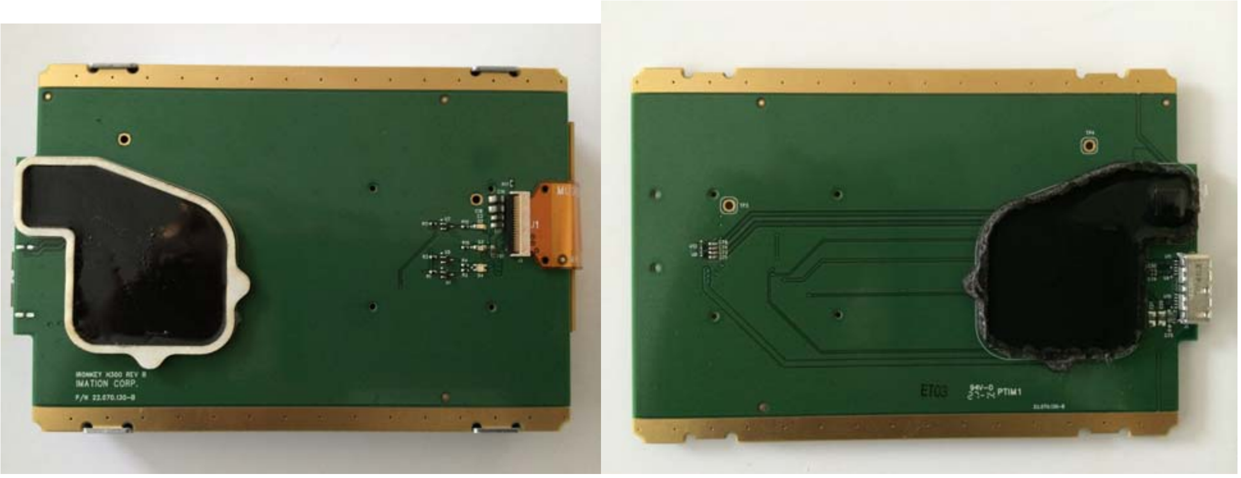
The IronKey H350, hereafter referred to as the cryptographic module, is a multi-chip standalone cryptographic module designed to provide secure data storage and operator authentication. The module under validation includes the following configurations, which differ only in storage size and are physically identical:

IronKey H350 (FW Version: 1.0.0)	
HW P/N (SKU)	*Description*
MXKB1B500G5001FIPS	DRIVE EA IRONKEY BASIC H350 2.5 EHDD USB 3.0 500GB
MXKB1B001T5001FIPS	DRIVE EA IRONKEY BASIC H350 2.5 EHDD USB 3.0 1TB

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



Figures 1 & 2 – Images of the Cryptographic Module w/ Excluded Case



Figures 3 & 4 – Images of the Cryptographic Module w/o Excluded Case

When the IronKey H350 is connected to a PC, it mounts two drives: a secure volume and a Read-Only hard disk drive (HDD). All files mounted within the Read-Only HDD 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. Files distributed with the module mounted within the internal Read-Only HDD are excluded from the validation. The metallic enclosure is excluded from the cryptographic boundary, as it is removable. The module relies on the features described in Section 9, Physical Security Policy, of this document for physical protection. Lastly, the physical HDD is also excluded from the cryptographic boundary, as it is also removable and does not contain any plaintext secrets or information that could be used to compromise the module's security.

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 through the 'Get Version' service, which can be accessed by checking the Device Info provided in the Control Panel application that interfaces with the H350. The module supports the following FIPS Approved algorithms:

- AES 128, 192, 256-bit (Cert. #1412)
- AES-XTS 256-bit (Cert. #2559)
- SHA-1, SHA-256 (Cert. #1282)
- SHA-256 (Cert. #2158)
- HMAC SHA-256 (Certs. #1577, #1579)
- FIPS 186-2 RSA Sign/Verify (Cert. #688)
  - SIG(gen): 2048;, SHS: SHA-256
  - SIG(ver): 1024, 2048;, SHS: SHA-1 and SHA-256
- FIPS 186-2 RSA Verify (Cert. #1311)
- Triple-DES (Cert. #965)

  Note: From January 1, 2011 through December 31, 2015, the use of two-key Triple DES for encryption is **restricted**: the total number of blocks of data encrypted with the same cryptographic key **shall not** be greater than 2^{20}
- Triple-DES MAC (Triple-DES Cert. #965, vendor affirmed)
- ANSI X9.31 RNG (Cert. #774)
- PBKDF (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:

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

Other: The following algorithm is present in the module, but is not used nor is it accessible to an operator:

- FIPS 186-2 RSA (Cert. #688): PKCS #1 1.5 signature generation: 1024 and 2048 using SHA-1

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
- LEDs (Qty. 3):	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 performance limitations of the USB port and the performance of the processor allow for 1111 RSA signature verifications to be performed in one minute (1 every 54ms). Therefore, the probability of successfully authenticating to the module within one minute through random attempts is less than 1/100,000.

* 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	- Secure Data Storage: Safely store your data within the storage. - 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 HDD. - 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 storage 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 Application Volume.
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: Re-commissions 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.
- Login:	Initialize the device and allow the operator to authenticate.
- Secure Channel:	Establish a secure channel to facilitate authentication. No authentication or secure services are supported outside of a secure channel.

For additional information, please see the Imation 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 Imation 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 HDD 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.
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 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.
HMAC Integrity Key	HMAC SHA-256 key. Provides firmware integrity.

Definition of Public Keys

Table 6 - Public Keys

Device Public Key:	2048-bit RSA key. Facilitates key transport and signature verification.
Host Public Key:	2048-bit RSA key. Digital signature verification and key transport.
Server 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.
Firmware and Application Volume 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. The modes of access shown in the table are defined as follows:

- Read
- Write
- Execute

Table 7 - CSP Access Rights within Roles & Services

Role			**Service**	**Cryptographic Keys and CSPs Access Operation**
C.O.	**User**	**Server**		
	X		Secure Data Storage	Read Device Private Key, Secure Volume Key, Box AES Keys
	X		Change Password	Read/Write Password Hash, Master Key Read Device Private Key
	X		Format Drive	Read Device Private Key
	X		Get Version	Read Device Private Key
	X		Lock Device	Read Device Private Key
	X		Get Public Key	Read Device Private Key
	X		RSA Sign/Verify	Read/Execute Device Private Key, RSA Private Keys

Role			Service	Cryptographic Keys and CSPs Access Operation
C.O.	User	Server		
	X		RSA Wrap/Unwrap	Read/Execute Device Private Key, RSA Private Keys
	X		Get Random	Read/Execute Device Private Key Read/Write/Execute RNG Seed and Seed Key
	X		Generate Key Pair	Read/Execute Device Private Key, DRNG Seed and Seed Key Write User Private Keys
	X		Read Application Key	Read/Execute Device Private Key, Identity Manager Key
	X		Application Data Access	Read/Execute Device Private Key, Box AES Keys, RSA Private Keys
	X		Import Key Pair	Read/Execute Device Private Key Write User Private Keys
X			Firmware Upgrade	Read/Execute SSD Keys, Firmware and Application Volume Public Key
		X	Policy Import	Read/Execute Box AES Key, Device Private Key
		X	Access Restrictions	Read/Execute Device Private Key
		X	Device Recovery	Read/Execute Device Recovery Key, Password Hash, Login Private Key, Device Private Key
		X	Device Reset	Read/Execute Device Private Key Write User Private Keys, Box AES Key (Zeroize)
		X	Self-Destruct	Read/Execute Device Private Key Write all CSPs (Zeroize)
X	X	X	Show Status	N/A
X	X	X	Self-Tests	N/A
X	X	X	Basic Reset	Read/Execute Device Private Key Write User Keys, Box AES Key (Zeroize)
X	X	X	Login	Read/Write/Execute Login Private Key, DRNG Seed Key and Seed, Master Key, Device Recovery Key Read/Execute Password Hash Write All Plaintext CSPs (if authentication retry limit is exceeded, Zeroize)
X	X	X	Secure Channel	Read/Write/Execute Secure Channel Encryption Key, Secure Channel Integrity Key

7. Operational Environment

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

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 Encrypt Known Answer Tests
      b. AES Decrypt Known Answer Tests
      c. SHA-1, SHA-256 Known Answer Tests
      d. HMAC SHA-256 Known Answer Tests
      e. RSA Sign Known Answer Test (Cert. #688)
      f. RSA Sign Known Answer Test (Cert. #1311)
      g. RSA Verify Known Answer Test (Cert. #688)
      h. RSA Verify Known Answer Test (Cert. #1311)
      i. Triple-DES Encrypt Known Answer Test
      j. Triple-DES Decrypt Known Answer Test
      k. ANSI X9.31 RNG Known Answer Test
      l. PBKDF Known Answer Test
   2. Firmware Integrity Tests
   3. Critical Functions Tests: N/A.

   Conditional Self-Tests:

   1. Continuous RNG Tests: Performed on NDRNG and ANSI X9.31 RNG
   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 IronKey Unlocker.
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, opaque epoxy

Note: The module hardness testing was only performed at ambient temperature and no assurance is provided for Level 3 hardness conformance at any other temperature.

Operator Required Actions

The operator is required to periodically inspect the epoxy encapsulate 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
HDD	Disk Drive
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
HDD	Hard Disk Drive
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