Kingston Technology Company, Inc.

IronKey D500S Series USB Flash Drive

FIPS 140-3 Non-Proprietary Security Policy

Document Version 1.0

TABLE OF CONTENTS

TABLE OF TABLES

1. GENERAL

1.1 OVERVIEW

The Kingston Technology Company, Inc. (Kingston) *IronKey D500S Series USB Flash Drive* is a hardware cryptographic module designed to meet the overall requirements of FIPS 140-3 Security Level 3.

1.2 SECURITY LEVELS

Table 1 – Security Levels

ISO/IEC 24759	FIPS 140-3 Section Title	Security Level
1	General	3
2	Cryptographic Module Specification	3
3	Cryptographic Module Interfaces	3
4	Roles, Services, and Authentication	3
5	Software/Firmware Security	3
6	Operational Environment	N/A
7	Physical Security	3
8	Non-Invasive Security	N/A
9	Sensitive Security Parameter Management	3
10	Self-Tests	3
11	Life-Cycle Assurance	3
12	Mitigation of Other Attacks	N/A
	Overall Level:	3

2. CRYPTOGRAPHIC MODULE SPECIFICATION

2.1 DESCRIPTION

The Kingston *IronKey D500S Series USB Flash Drive* (*refer to Figure 1*) is a hardware cryptographic module designed for organizations that require a secure way to store and transfer portable data. The stored data is secured by hardware-based 256-bit AES on-the-fly encryption to guard sensitive information in case the drive is lost or stolen. Its strong, durable, metal casing provides robust physical protection. Its strong password rules and lock-down control protect against brute force attacks. Such advanced security features make the *IronKey D500S Series USB Flash Drive* ideal for corporations and service organizations that require employees to transport large digital files consisting of confidential documents.

2.1.1 TOEPP AND CRYPTOGRAPHIC BOUNDARY

The module is a multi-chip standalone cryptographic module whose outer enclosure defines the cryptographic boundary and Tested Operational Environment's Physical Perimeter (TOEPP) (refer to Figure 1).

Figure 1 – Cryptographic Boundary

2.2 TESTED AND VENDOR AFFIRMED MODULE VERSION AND IDENTIFICATION

The *IronKey D500S Series USB Flash Drive* is a FIPS 140-3 Security Level 3 (*refer to Table 1*) multi-chip standalone cryptographic module (module) available in the following configurations:

- IKD500S/xGB
- IKD500SM/xGB

x = 8, 16, 32, 64, 128, 256 and 512 (denotes module's memory capacity)

2.2.1 TESTED OPERATING ENVIRONMENTS

The module's operating environment is defined as the non-modifiable, Kingston PS2251-15 USB AES Micro-Controller. The FIPS 140-3 Security Level 3 validated versioning information is shown in Table 2. The hardware versions differ by memory capacity e.g., 16GB, 32GB, etc. The Kingston *IronKey D500S Series USB Flash Drive* is marketed as IronKey D500S or IronKey D500SM. There is no physical or logical difference between these two branded products.

Table 2 – Tested Module Identification - Hardware

Model/Part Number(s)	Hardware Version(s)	Firmware Version(s)	Processor(s)	Non-Security Relevant Distinguishing Features
IronKey D500S Series USB Flash Drive	IronKey D500S/8GB	3.06	Kingston PS2251-15 USB AES Micro-Controller	8GB of user data storage
	IronKey D500S/16GB			16GB of user data storage
	IronKey D500S/32GB			32GB of user data storage
	IronKey D500S/64GB			64GB of user data storage
	IronKey D500S/128GB			128GB of user data storage
	IronKey D500S/256GB			256GB of user data storage
	IronKey D500S/512GB			512GB of user data storage
	IronKey D500SM/8GB			8GB of user data storage
	IronKey D500SM/16GB			16GB of user data storage
	IronKey D500SM/32GB			32GB of user data storage
	IronKey D500SM/64GB			64GB of user data storage
	IronKey D500SM/128GB			128GB of user data storage
	IronKey D500SM/256GB			256GB of user data storage
	IronKey D500SM/512GB			512GB of user data storage

2.3 Excluded Components

The module does not exclude any components from the requirements of FIPS 140-3.

2.4 Modes of Operation

The module supports a single approved mode of operation that is entered by powering-on the module. There are no non-approved modes, degraded modes or non-approved services available to the module. The module's firmware provides an indicator (i.e., "FIPS ACTIVE") showing the approved configuration which can be queried. This global indicator will be used along with the successful return codes of each service to indicate the module has provided an approved security service. If the module reports "FIPS DEFAULT", the module is awaiting a new password (CO Password) to be set. The module is always running in an approved mode when module reports either "FIPS DEFAULT" or "FIPS ACTIVE". The approved mode cannot be exited.

The module does not support a non-approved or degraded mode of operation. In case of critical error, the module will remain in an error state, until reset. While in its error state, the LED will blink rapidly until it is reset.

2.5 ALGORITHMS

2.5.1 APPROVED ALGORITHMS

The module supports the following approved cryptographic algorithms.

Table 3 – Approved Algorithms

CAVP Cert(s)	Algorithm	Standards	Modes/ Methods	Description / Key Sizes, Curves, or Moduli / Key Strengths	Use/Function
A3268	AES-CBC	FIPS 197 NIST SP 800-38A	CBC	Key Length: 256-bit Strength: 256 bits	Prerequisite for KW Data Encryption/Decryption
A3268	AES-ECB	FIPS 197 NIST SP 800-38A	ECB	Key Length: 256-bit Strength: 256 bits	Prerequisite for KW Data Encryption/Decryption
A3268	AES-KW	FIPS 197 NIST SP 800-38F	KW	Key Length: 256-bit Strength: 256 bits	DEK_CO and DEK_U Encryption/Decryption
A3268	AES-XTS[1]	FIPS 197 NIST SP 800-38E	XTS	Key Length: 256-bit Strength: 256 bits	Mass-Storage Data Encryption/Decryption
A3268	ECDSA KeyGen	FIPS 186-5	Key Generation	Curve: P-256 Strength: 128 bits	Key Generation of KAS keys
A3268	ECDSA KeyVer	FIPS 186-4	Key Verification	Curve: P-256 Strength: 128 bits	Key Verification of KAS keys
A3268	HMAC-SHA2-256	FIPS 198-1	SHA2-256	Key Length: 256-bit Strength: 256 bits	Prerequisite for KDA Message Authentication
A3268	HMAC DRBG	NIST SP 800-90A	HMAC-SHA2-256	Security strength: 256 bits	Deterministic Random Bit Generation
A3268	KAS-ECC-SSC	NIST SP 800-56Ar3	ECC CDH C(2e, 0s)	Curve: P-256 Strength: 128 bits	Key Agreement Shared Secret calculation
A3268	KDA	NIST SP 800-56Cr2	Two-Step KDF (HMAC-SHA2-256)	Derived Key Length: 256 bits Shared Secret Length: 256 bits	Key derivation as part of KAS
A3268	PBKDF[2]	NIST SP 800-132 (option 2A)	HMAC-SHA2-256	Password length: 8 to 136 bytes (refer to Section 4.1) Salt Length: 256-bit	Deriving KEK_CO, KEK_U, KEK_R
A3268	RSA SigVer (PKCS1 v1.5)	FIPS 186-4	Digital Signature Verification	Modulo: 2048 Strength: 128 bits	Digital Signature Verification

[1] AES XTS was designed for the cryptographic protection of data on storage devices per NIST SP 800-38E. It was not designed for other purposes, such as the encryption of data in transit.

[2] The module implements PBKDF in conformance with NIST SP 800132 and FIPS IG D.N. Specifically, the module implements Option 2a from Section 5.4 to generate the Key Encryption Key (KEK) responsible for protecting the Data Encryption Key using AES KW (Cert. #3268). The module implements an iteration counter equal to 1024 bits which is greater than the minimum recommendation documented within NIST SP 800-132 - Section 5.2. This is also justified by the maximum limit enforced on password retry attempts (Max = 10).

CAVP Cert(s)	Algorithm	Standards	Modes/ Methods	Description / Key Sizes, Curves, or Moduli / Key Strengths	Use/Function
A3268	SHA2-256	FIPS 180-4	SHA2-256	Strength: 128 bits	Prerequisite for HMAC Message Digest

2.5.2 Vendor Affirmed Algorithms

The module supports the following vendor affirmed algorithms.

Table 4 - Vendor Affirmed Algorithms

Algorithm Name	Algorithm Properties	Implementation	Reference
CKG	Key Type: Symmetric	Crypto Library FW v2.00	NIST SP 800-133r2 Sections 4 5.1 and 6.1

2.5.3 Non-Approved, Allowed Algorithms

The module does not support non-approved algorithms.

Table 5 – Non-Approved, Allowed Algorithms

Algorithm Name	Algorithm Properties	Implementation	Reference
N/A	N/A	N/A	N/A

2.5.4 Non-Approved, Allowed Algorithms with No Security Claimed

The module does not support non-approved algorithms.

Table 6 – Non-Approved, Allowed Algorithms with No Security Claimed

Algorithm	Caveat	Use/Function
N/A	N/A	N/A

2.5.5 Non-Approved, Not Allowed Algorithms

The module does not support non-approved algorithms.

Table 7 – Non-Approved, Not Allowed Algorithms

Algorithm	Use/Function
N/A	N/A

2.6 Security Function Implementations (SFI)

Table 8 - Security Function Implementations (SFI)

Name	Type	Description	SF Properties	Algorithms / CAVP Cert
KAS	KAS-Full	NIST SP 800-56Arev3 per IG D.F Scenario 2 path (2)	Standards: NIST SP 800-56Arev3, NIST SP 800-56Crev2, FIPS 186-4	KAS-ECC-SSC: (A3268)
				KDA: (A3268)
				ECDSA KeyVer: (A3268)
KTS	KTS-Unwrap	Key unwrapping per NIST SP 800-38F Per IG D.G. Used for the entry of the operator's password.	Standards: FIPS 197, FIPS 198-1, NIST SP 800-38A	AES-CBC: (A3268)
				HMAC-SHA2-256: (A3268)

2.7 Algorithm Specific Information

The module utilizes only approved algorithms (*refer to Table 3*) that are tested and validated under the Cryptographic Module Validation Program (CAVP).

2.8 RBG and Entropy

The module includes an internal entropy source for the generation of the DRBG seed. Please refer to the Entropy Source Validation (ESV) certificate #E55.

Table 9 - Non-Deterministic Random Number Generation Specification

Entropy Sources	Minimum Number of Bits of Entropy	Details
Kingston Technology Company, Inc. Crypto Library FW v2.00 ESV Validation #E55	The ESV source outputs 1024 bits with a minimum of 256 bits of entropy	Based on the heuristic lower bound entropy estimate, the entropy source has a rate of 1-bit per nibble or 25%. This means the entropy input required for the DRBG is 1024*0.25 = 256 bits.

2.9 Key Generation

The module generates cryptographic keys using a NIST SP 800-90A conforming DRBG (Cert. #A3268) for the encryption and protection of user data.

2.10 Key Establishment

The module supports a NIST SP 800-56Ar3 conforming key agreement scheme for the establishment of AES 256 and HMAC-SHA2-256 keys to secure communication to / from the module. In addition, the module supports KTS using AES CBC with HMAC-SHA2-256 in conformance with NIST SP 800-38F and IG D.G.

2.11 INDUSTRY PROTOCOLS

The module relies upon the standard USB protocol for communication with general purpose computer (GPC) systems.

3. CRYPTOGRAPHIC MODULE INTERFACES

3.1 PORTS AND INTERFACES

The module incorporates both physical and logical interfaces as described within Table 10.

Table 10 - Ports and Interfaces

Physical Port	Logical Interface	Data that Passes over Port/Interface
USB Port (Rx / Tx)	Data Input	The USB 3.0 port connects the module to the host computer. It is used to receive user data as well as API calls issued by the host via the USB protocol. The input is received by the module on the Rx line.
	Data Output	The USB 3.0 port connects the module to the host computer. It is used to send user data as well as return codes upon completion of API calls issued by the host via the USB protocol. The input is received by the module on the Tx line.
	Control Input	The USB 3.0 port connects the module to the host computer. It is used to receive commands as well as API calls issued by the host via the USB protocol. The input is received by the module on the Rx line.
	Status Output	Error codes and other statuses are transmitted from the module to the host computer.
LED	Status Output	Error codes and other statuses are transmitted by the LED: – Active data transfer with host computer: LED blinks at 3Hz – Error state: LED blinks rapidly at 16Hz – Pre-operational Self-test status output: LED blinks at 3Hz if all self-tests completed, LED blinks at 16Hz if failed – Continuous Self-test status output: LED blinks at 16Hz if failed – Periodic Self-test status output: LED blinks at 16Hz if failed
USB Port (VCC)	Power	The USB VBUS (+5VDC) powers the module.

3.2 TRUSTED CHANNEL

The module does not support a Trusted Channel.

4. ROLES, SERVICES, AND AUTHENTICATION

4.1 AUTHENTICATION METHODS

The module supports identity-based authentication in the form of a User ID and Password (Memorized Secret) in conformance with NIST SP 800-140E and SP 800-63B (*refer to Section 5.1.1*).

4.1.1 PASSWORDS

Per NIST SP 800-63B – Section 5.1.1, passwords must be a minimum of 8 bytes (enforced by the module). The password must contain three of the following four-character types: lowercase letters, uppercase letters, numeric characters and/or special characters. This greatly increases the passwords entropy. Assuming a mix of lowercase letters, uppercase letters, numeric characters, the

password can consist of the following set: uppercase letters, lowercase letters, numbers, and special characters, yielding 95 choices per character. The probability of a successful random attempt is 1/(10 * 26 * 26 * 95^5) ~= $1/2^{45}$, which is less than 1/1,000,000. The module only allows for ten (10) unsuccessful authentication attempts. Therefore, the probability of success with multiple attempts in a one-minute period is $10/2^{45}$, which is less than 1/100,000.

Table 11 – Authentication Methods

Name	Description	Mechanism	Strength Each Attempt	Strength Per Minute
ID/Password	CO and User role authentication method. The password is at least 8 bytes in length and includes the numbers, the uppercase letters, the lowercase letters, and the special characters.	ID & Password combination used within a challenge/response mechanism	The upper bound for the probability of having the password guessed at random is: 1 / (10 * 26 * 26 * 95^5) ~= $1/2^{45}$ < 1/1,000,000	The probability of the consecutive failed authentication attempts in one minute period is approximately 10/ 2^{45} < 1/100,000

4.2 ROLES

Table 12 lists the roles supported by the module with the respective services supported by that role.

Table 12 – Roles, Service Commands, Input and Output

Role	Service	Input	Output
Crypto Officer (CO)	Change CO Password	Current CO Password and new CO Password	Status Out (success, session invalid, wrong password) LED blinks at 16Hz if fatal error
	Close Partition (Logout)	N/A	Status Out (success, session invalid, partition has been closed) LED blinks at 16Hz if fatal error
	Decrypt	Disk accessing	Read partition data
	Encrypt	Disk accessing	Write partition data
	Initialize	CO Password and the drive's partition configuration	Status Out (success, configuration invalid) LED blinks at 16Hz if fatal error
	Open Partition (Login)	CO ID & Password, and the selected partition	Status Out (success, session invalid, partition has been opened, wrong password) LED blinks at 16Hz if fatal error, the partition is opened if success
	Setup User Password	Current CO Password and new User Password	Status Out (success, session invalid, wrong password) LED blinks at 16Hz if fatal error

Role	Service	Input	Output
	Setup Recovery Password	Current CO Password and new Recovery Password	Status Out (success, session invalid, wrong password) LED blinks at 16Hz if fatal error
User	Change User Password	Current User Password and new User Password	Status Out (success, session invalid, wrong password) LED blinks at 16Hz if fatal error
	Close Partition (Logout)	N/A	Status Out (success, session invalid, partition has been closed) LED blinks at 16Hz if fatal error
	Decrypt	Disk accessing	Read partition data
	Encrypt	Disk accessing	Write partition data
	Open Partition (Login)	User ID & Password, and the selected partition	Status Out (success, session invalid, partition has been opened, wrong password) LED blinks at 16Hz if fatal error, the partition is opened if success
	Setup User Password (Using Recovery Password)	Recovery Password and new User Password	Status Out (success, session invalid, wrong password, recovery password not created) LED blinks at 16Hz if fatal error
Unauthenticated	CD Update	API call with CD Image, Signature	Status Out (success, session invalid, signature verification failed)
	Perform Self-Tests	Power-on the module	LED blinks at 3Hz if all tests complete LED blinks at 16Hz if failed
	Reset Drive	N/A	Status Out (success, session invalid) Internally zeroize all CSPs except the session keys and generate DEK_CO and configure to the single partition. LED blinks at 16Hz if fatal error
	Show Module Version	N/A	Returns module ID and version information, in addition to the approved mode indicator to API call.
	Show Error Status	N/A	Returns the error log to API call
	Show Status	N/A	Reply the service status, the disk status, or the session establishment status to API call
	Zeroization	N/A	Status Out (success) Internally zeroize all CSPs. LED blinks at 16Hz if fatal error

The operator must perform that following initialization procedures to access the module for the first time.

1. Connect the *IronKey D500S Series USB Flash Drive* to a GPC. The module will enumerate onto the GPC and register its CD ROM partition. Locate and run the application located on the CD-ROM partition.
2. Follow the instructions presented by the application to 'Initialize' the module. Initialize the CO authentication by establishing a password and continue to login to the device. Per NIST SP 800-63B – Section 5.1.1 the password must be at least 8 characters.

Table 13 – Roles and Authentication

Role	Authentication Method	Authentication Strength	
		Strength Each Attempt	**Strength Per Minute**
Crypto Officer (CO)	ID & Password combination used within a challenge/response mechanism. The password must be at least 8 characters long and must contain at least one integer, one lower-case letter, and one upper-case letter.	The upper bound for the probability of having the password guessed at random is: $1 / (10 * 26 * 26 * 95^5) \sim= 1/2^{45} < 1/1,000,000$	The probability of the consecutive failed authentication attempts in one minute period is approximately $10/ 2^{45} < 1/100,000$
User	ID & Password combination used within a challenge/response mechanism. The password must be at least 8 characters long and must contain at least one integer, one lower-case letter, and one upper-case letter.	The upper bound for the probability of having the password guessed at random is: $1 / (10 * 26 * 26 * 95^5) \sim= 1/2^{45} < 1/1,000,000$	The probability of the consecutive failed authentication attempts in one minute period is approximately $10/ 2^{45} < 1/100,000$

4.3 Approved Services

SSP access rights are defined as follows:

- G = Generate: The module generates or derives the SSP.
- R = Read: The SSP is read from the module (e.g., the SSP is output).
- W = Write: The SSP is updated, imported, or written to the module.
- E = Execute: The module uses the SSP in performing a cryptographic operation.
- Z = Zeroize: The module zeroizes the SSP.

Table 14 – Approved Services

Service	Description	Approved Security Functions	Keys & SSPs	Roles	Access Rights to Keys and / or SSPs	Indicator
(All CO/User Services)	Secure Communication Session	KAS-ECC-SSC & KDA	AES Session Key, MAC Session Key	CO and User	Shared Secret (Z): **G, E, Z** AES Session Key: **G, E** MAC Session Key: **G, E** Device ECDH Private Key: **G, Z** Device ECDH Public Key: **G, R, Z** Host ECDH Public Key: **W, Z** DRBG Internal State: **G, E**	Return status via the API: 0x0000: success 0x4002: session invalid
CD Update	Load/Update CD Image to the CD-ROM partition	RSA (PKCS1 v1.5) Signature Verification	CD Update Public Key	Unauthenticated	CD Update Public Key: **E**	Return status via the API: 0x0000: success 0x4002: session invalid 0x4006: signature verification failed
Change CO Password	Create new CO password	DRBG, PBKDF, SHA2-256	KEK_CO, CO Password, CO Password Hash DRBG Internal State	CO	KEK_CO: **G, E, Z** CO Password: **E, Z** CO Password Hash: **Z, G** DRBG Internal State: **G, E**	Return status via the API: 0x0000: success 0x8102: configuration invalid

Service	Description	Approved Security Functions	Keys & SSPs	Roles	Access Rights to Keys and / or SSPs	Indicator
Change User Password	Create new User Password	DRBG, PBKDF, SHA2-256	KEK_U User Password, User Password Hash, DRBG Internal State	User	KEK_U: **G, E, Z** User Password: **E, Z** User Password Hash: **Z**, **G** DRBG Internal State: **G, E**	Return status via the API: 0x0000: success 0x8102: configuration invalid
Close Partition (Logout)	Logout. Locks drive	N/A	DEK_CO or DEK_U	CO	DEK_CO: **Z** AES Session Key: **Z** MAC Session Key: **Z**	Return status via the API: 0x0000: success 0x1602: session invalid 0x1604: partition has been closed
				User	DEK_U: **Z** AES Session Key: **Z** MAC Session Key: **Z**	
Decrypt	Read partition data	AES-XTS	DEK_CO or DEK_U	CO	DEK_CO: **E**	Return status via the API: 0x0000: success
				User	DEK_U: **E**	
Encrypt	Write partition data	AES-XTS	DEK_CO or DEK_U	CO	DEK_CO: **E**	Return status via the API: 0x0000: success
				User	DEK_U: **E**	
Initialize	Create CO password and generate DEK	DRBG, PBKDF, SHA2-256, AES-KW	DEK_CO, KEK_CO, CO Password, CO Password Hash, Entropy Input, DRBG Nonce, DRBG Internal State	CO	DEK_CO: **Z, G** KEK_CO: **G, E, Z** CO Password: **W, E, Z** CO Password Hash: **G** Entropy Input: **G, E** DRBG Nonce: **G, E** DRBG Internal State: **G, E**	Return status via the API: 0x0000: success 0x8102: configuration invalid
Open Partition (Login)	Authenticates either the CO or User to the module	PBKDF, SHA2-256, AES-KW	CO Password KEK_CO & DEK_CO or User Password, KEK_U & DEK_U	CO	CO Password: **W, E, Z** KEK_CO: **G, E, Z** DEK_CO: **E**	Return status via the API: 0x0000: success 0x1402: session invalid 0x1404: partition has been opened 0x1406: wrong password
				User	User Password: **W, E, Z** KEK_U: **G, E, Z** DEK_U: **E**	
Perform Self-Tests	Perform Pre-Operational and Conditional Self-Tests	N/A	N/A	Unauthenticated	DRBG Internal State: **G, E**	LED Flashing

Service	Description	Approved Security Functions	Keys & SSPs	Roles	Access Rights to Keys and / or SSPs	Indicator
Reset Drive	Erase all files stored on the module and zeroizes all CSPs	N/A	DEK_CO, DEK_U, CO Password Hash, User Password Hash, Recovery Password Hash, DRBG Internal State	Unauthenticated	DEK_CO: **Z** DEK_U: **Z** CO Password Hash: **Z** User Password Hash: **Z** Recovery Password Hash: **Z** DRBG Internal State: **Z**	Return status via the API: 0x0000: success 0x8101: session invalid
Setup User Password	Create new User password	DRBG, PBKDF, SHA2-256	DEK_U, KEK_U, User Password, User Password Hash, DRBG Internal State	CO	DEK_U: **G, Z** KEK_U: **G, E, Z** User Password: **W, E, Z** User Password Hash: **G** DRBG Internal State: **G, E**	Return status via the API: 0x0000: success 0x8102: configuration invalid
Setup User Password (Using Recovery Password)	Create new User Password	DRBG, PBKDF, SHA2-256	KEK_R, KEK_U Recovery Password, Recovery Password Hash, User Password, User Password Hash, DRBG Internal State	User	KEK_U: **G, E, Z** KEK_R: **G, E, Z** Recovery Password: **E, Z** Recovery Password Hash: **Z** User Password: **W, E, Z** User Password Hash: **G** DRBG Internal State: **G, E**	Return status via the API: 0x0000: success 0x8102: configuration invalid
Setup Recovery Password	Create Recovery password	DRBG, PBKDF, SHA2-256	KEK_R, Recovery Password, Recovery Password Hash, DRBG Internal State	CO	KEK_R: **G, E, Z** Recovery Password: **W, E, Z** Recovery Password Hash: **G** DRBG Internal State: **G, E**	Return status via the API: 0x0000: success 0x8102: configuration invalid
Show Module Version	Get module ID and version	N/A	N/A	Unauthenticated	N/A	Return status via the API: 0x0000: success
Show Error Status	Returns the most recent error details	N/A	N/A	Unauthenticated	N/A	Return status via the API: 0x0000: success
Show Status	Get the module's status	N/A	N/A	Unauthenticated	N/A	Return status via the API: 0x0000: success

Service	Description	Approved Security Functions	Keys & SSPs	Roles	Access Rights to Keys and / or SSPs	Indicator
Zeroization	Zeroize all keys and CSPs	N/A	N/A	Unauthenticated	DEK_CO: **Z** DEK_U: **Z** CO Password Hash: **Z** User Password Hash: **Z** Recovery Password Hash: **Z** DRBG Internal State: **Z** AES Session Key: **Z** MAC Session Key: **Z**	Return status via the API: 0x0000: success

4.4 Non-Approved Services

The module does not support any non-approved services.

4.5 External Software/Firmware Loaded

The module's firmware is non-modifiable. It does not have the ability to support the external software / firmware loading.

4.6 Identification and Authentication

The module supports the following authenticated roles:

- Crypto Officer (CO)
- User

It enforces the separation of roles using identity-based authentication. The operator must perform that following initialization procedures to access the module for the first time.

1. Connect the IronKey D500S Series USB Flash Drive to a GPC. The module will enumerate onto the GPC and register its CD ROM partition. Locate and run the application located on the CD-ROM partition.
2. Follow the instructions presented by the application to 'Initialize' the module. Initialize the CO authentication by establishing a password and continue to login to the device. Per NIST SP 800-63B – Section 5.1.1 the password must be at least 8 characters.

Table 13 lists all operator roles supported by module. The module also supports an Unauthenticated role.

5. SOFTWARE/FIRMWARE SECURITY

5.1 INTEGRITY TECHNIQUES

The module incorporates an RSA 2048 PKCS1 v1.5 (Cert. #A3268) digital signature mechanism over its firmware. The digital signature provides integrity as well as authentication.

All commands sent to and from the cryptographic module are protected with HMAC-SHA2-256.

5.2 INITIATE ON DEMAND

The module loads the firmware image from non-volatile memory to on-chip RAM when powering on the module where it then performs the firmware integrity test using the module's RSA-2048 'Firmware Integrity Public Key'. If the test fails, the module enters an error state, the data output interface is inhibited, and the module's LED (status output) blinks at 16Hz.

The firmware integrity test is a part of Pre-Operational Self-Tests. It is automatically executed at power-on or during the Periodic Self-Tests. It can also be invoked by power-cycling the module.

6. OPERATIONAL ENVIRONMENT

6.1 OPERATIONAL ENVIRONMENT TYPE AND REQUIREMENTS

The operational environment is classified as non-modifiable.

7. PHYSICAL SECURITY

The module is a multiple-chip standalone module and conforms to FIPS 140-3 Security Level 3 physical security requirements. The module is housed within a strong, non-removable, tamper-evident enclosure. The enclosure is opaque within the visible spectrum. In addition, all components are protected with a hard epoxy coating that protects each component from being viewed or probed. Attempts at removing the epoxy will render the module inoperable.

7.1 MECHANISMS AND ACTIONS REQUIRED

7.1.1 PHYSICAL SECURITY INSPECTION GUIDELINES

The operator of the module should inspect the outer casing of the module each time prior to connecting the module to a computer. If tamper evidence is observed on the outer casing, the module should not be used.

Table 15 - Physical Security Inspection Guidelines

Physical Security Mechanism	Recommended Frequency of Inspection / Test	Inspection/Test Guidance Details
Tamper Evidence	Each time the module is used	Upon each use of the module the operator should examine the module for evidence of tamper.

The module supports the operation, storage and distribution temperatures listed in Table 16.

Table 16 – Normal Operation, Storage and Distribution Temperature Ranges

	Low Temperature	High Temperature
Normal Operation	0˚C	60˚C
Storage	-20˚C	85˚C
Distribution	-20˚C	85˚C

7.2 EFP/EFT

The module does not incorporate any environmental protection mechanisms (EFP). The module satisfies environmental failure testing (EFT) requirements.

Table 17 – EFP/EFT

Environment	Temperature / Voltage Measurement	EFP / EFT	Shutdown, Zeroization, Undefined Failure, Known Error Sate or Continues to Operate Normally[3]
Low Temperature	-100°C	EFT	Continues to Operate Normally
High Temperature	+122°C	EFT	Undefined Failure
Low Voltage	3.2V	EFT	Shutdown
High Voltage	10.1V	EFT	Undefined Failure

7.3 HARDNESS TESTING

The module supports and has been tested at the operation, storage and distribution temperatures listed in Table 16. The module's epoxy and outer enclosure hardness are assured within these ranges.

Table 18 – Hardness Testing Temperature Ranges

	Hardness Tested Temperature Measurement
Low Temperature	-20˚C
High Temperature	85˚C

[3] For EFP, states can be *Shutdown* or *Zeroise*; for EFT, states can be Shutdown, Zeroization, Undefined Failure, Known Error Sate or Continues to Operate Normally.

8. NON-INVASIVE SECURITY

The module does not provide protections against non-invasive security methods.

9. SENSITIVE SECURITY PARAMETERS (SSP) MANAGEMENT

The module incorporates both Critical Security Parameters (CSPs) and Public Security Parameters (PSPs).

9.1 STORAGE AREAS

The module is designed to encrypt and store arbitrary data with XTS-AES within eMMC memory components. The module physically and logically protects static keys and CSPs. Please refer to Table 19 for additional information.

9.2 SSP INPUT/OUTPUT METHODS

The module inputs CSPs encrypted with AES CBC and authenticated with HMAC-SHA2-256. The module does not output CSPs. PSPs are output in order to authenticate the module to the connected GPC. Please refer to Table 19 for additional information.

9.3 SSP ZEROIZATION METHODS

During normal operation, the module explicitly erases copies of CSPs in volatile memory (e.g., RAM) by overwriting with zeros after their use. For CSPs stored in non-volatile memory the module initiates its erase operation to zeroize.

The following methods are used to zeroize the module's CSPs during normal operation.

- 'Zeroization' and 'Reset Drive' service: This service overwrites all CSPs with zeroes and returns the module to its factory default state.
- After ten failed CO authentication attempts the respective CO and User DEKs are erased.
- After ten failed User authentication attempts the respective User DEK is erased.

9.4 Sensitive Security Parameters (SSPs)

The module incorporates SSPs as defined with Table 19.

Table 19 – SSPs

Key/CSP Name	Strength	Security Function & Cert. Number	Generation	Import / Export	Establishment	Storage	Zeroization	Use & related SSPs
DEK_CO (Data Encryption Key - CO)	256 bits	AES-XTS (Cert. #A3268)	Generated (via SP 800-90A DRBG)	Entry: N/A Output: N/A	N/A	eMMC - Encrypted with KEK_CO	Zeroization of the KEK_CO during 'Close Partition' service or disconnecting the drive. 'Zeroization' or 'Reset Drive' services.	Data Encryption / Decryption
DEK_U (Data Encryption Key - User)	256 bits	AES-XTS (Cert. #A3268)	Generated (via SP 800-90A DRBG)	Entry: N/A Output: N/A	N/A	eMMC - Encrypted with KEK_U	Zeroization of the KEK_U during 'Close Partition' service or disconnecting the drive. 'Zeroization' or 'Reset Drive' services.	Data Encryption / Decryption
KEK_CO (Key Encryption Key - CO)	256 bits	AES-KW (Cert. #A3268)	N/A	Entry: N/A Output: N/A	Derived from Crypto Officer Password	RAM (Plaintext)	Overwritten with zeros immediately after use	Encrypt / Decrypt DEK_CO
KEK_U (Key Encryption Key - User)	256 bits	AES-KW (Cert. #A3268)	N/A	Entry: N/A Output: N/A	Derived from User Password	RAM (Plaintext)	Overwritten with zeros immediately after use	Encrypt / Decrypt DEK_U
KEK_R (Recovery KEK)	256 bits	AES-KW (Cert. #A3268)	N/A	Entry: N/A Output: N/A	Derived from Recovery Password	RAM (Plaintext)	Overwritten with zeros immediately after use	Encrypt / Decrypt DEK_U

Key/CSP Name	Strength	Security Function & Cert. Number	Generation	Import / Export	Establishment	Storage	Zeroization	Use & related SSPs
Crypto Officer Password	8 ~ 136 bytes (refer to Section 4.1)	PBKDF (Cert. #A3268)	Created by Crypto Officer	Entry: AES Encrypted entry via host application Output: N/A	N/A	RAM (Plaintext)	Overwritten with zeros immediately after use	Used to generate the KEK_CO
User Password	8 ~ 136 bytes (refer to Section 4.1)	PBKDF (Cert. #A3268)	Created by User	Entry: AES Encrypted entry via host application Output: N/A	N/A	RAM (Plaintext)	Overwritten with zeros immediately after use	Used to generate the KEK_U
Recovery Password	8 ~ 136 bytes (refer to Section 4.1)	PBKDF (Cert. #A3268)	Created by Crypto Officer	Entry: AES Encrypted entry via host application Output: N/A	N/A	RAM (Plaintext)	Overwritten with zeros immediately after use	User to generate the KEK_R
Crypto Officer Password Hash	128-bits	SHA2-256 (Cert. #A3268)	Generated from CO Password	Entry: N/A Output: N/A	N/A	eMMC Hashed with SHA2-256	'Zeroization' or 'Reset Device' service	Used for Authentication
User Password Hash	128-bits	SHA2-256 (Cert. #A3268)	Generated from User Password	Entry: N/A Output: N/A	N/A	eMMC Hashed with SHA2-256	'Zeroization' or 'Reset Device' service	Used for Authentication
Recovery Password Hash	128-bits	SHA2-256 (Cert. #A3268)	Generated from Recovery Password	Entry: N/A Output: N/A	N/A	eMMC Hashed with SHA2-256	'Zeroization' or 'Reset Device' service	Used for Authentication
Entropy Input	1024 bits (Security strength is 256 bits)	Entropy Source (Cert. #E55)	Internally from SP 800-90B Entropy Source	Entry: N/A Output: N/A	N/A	RAM (Plaintext)	Overwritten with zeros immediately after use	Used as entropy input to the SP 800-90A DRBG
DRBG Nonce	512 bits (Security strength is 128 bits)	HMAC DRBG (Cert. #A3268)	Internally from SP 800-90B Entropy Source	Entry: N/A Output: N/A	N/A	RAM (plaintext)	Overwritten with zeros immediately after use	Used as nonce input to the SP 800-90A DRBG
DRBG Internal State (V and Key)	N/A	HMAC DRBG (Cert. #A3268)	Internally from SP 800-90A DRBG	Entry: N/A Output: N/A	N/A	RAM (plaintext)	'Zeroization' or 'Reset Device' service	The internal state of the SP 800-90A DRBG

Key/CSP Name	Strength	Security Function & Cert. Number	Generation	Import / Export	Establishment	Storage	Zeroization	Use & related SSPs
Device ECDH Private Key	256 bits (Security strength is 256 bits)	ECDSA Key Gen (Cert. #A3268)	Internally from SP 800-90A DRBG	Entry: N/A Output: N/A	N/A	RAM (plaintext)	Overwritten with zeros immediately after use	Used by the module for key agreement (KAS-ECC-SSC per SP 800-56Ar3)
Shared Secret (Z)	256 bits (Security strength is 128 bits)	KDA (Cert. #A3268)	N/A	Entry: N/A Output: N/A	Shared Secret from KAS-ECC-SSC C(2e, 0s) ECC CDH	RAM (plaintext)	Overwritten with zeros immediately after use	Used to derive the Session Key Material
AES Session Key	256 bits (Security strength is 128 bits)	AES-CBC (Cert. #A3268)	N/A	Entry: N/A Output: N/A	Derived by the KDA Two-Step Key Derivation Function	RAM (plaintext)	Overwritten with zeros immediately after secure session is terminated 'Zeroization' service	AES Session Key serves to encrypt data during the Secure Session.
MAC Session Key	256 bits (Security strength is 128 bits)	HMAC-SHA2-256 (Cert. #A3268)	N/A	Entry: N/A Output: N/A	Derived by the KDK via KDA Two-Step Key Derivation Function	RAM (plaintext)	Overwritten with zeros immediately after secure session is terminated 'Zeroization' service	MAC Session Key serves to authenticate data during the Secure Session.
CD Update Public Key	RSA 2048 (112 bits)	RSA 2048 (Cert. #A3268)	N/A	Entry: Manufacturing Output: N/A	N/A	eMMC	N/A – protected with SHA2-256[4]	Validates the CD ROM partition.
Device ECDH Public Key	P-256 (256 bits)	KAS-ECC-SSC (Cert. #A3268)	Generated internally from DRBG	Entry: N/A Output: Plaintext	N/A	RAM (plaintext)	Overwritten with zeros immediately after used	Used by the module for key agreement (KAS-ECC-SSC per SP 800-56Ar3)
Host ECDH Public Key	P-256 (256 bits)	KAS-ECC-SSC (Cert. #A3268)	N/A	Entry: Plaintext Output: N/A	N/A	RAM (plaintext)	Overwritten with zeros immediately after used	Used by the module for key agreement (KAS-ECC-SSC per SP 800-56Ar3)

[4] *Per IG 9.6.A – Additional Comment #6 – "a PSP is considered protected if it cannot be modified or if its modification can be determined by the module."*

10. SELF-TESTS

10.1 PRE-OPERATIONAL SELF-TESTS

The module performs pre-operational self-tests and conditional self-tests (*refer to Section 10.2*). Both self-tests ensure that the module is not corrupted, and the cryptographic algorithms work as expected. During self-tests, data output (via the data output interface) is inhibited. The module services are not available until the self-tests have completed successfully.

Table 20 – Pre-Operational Self-Tests

Algorithm or Test	Test Properties	Test Method	Type	Indicator	Details
Firmware Integrity Test	RSA 2048 PKCS1 v1.5 Digital Signature Verification	RSA 2048 Digital Signature Verification	SW / FW Integrity	Success: LED blinks at 3Hz Error: LED blinks at 16Hz	Performed during module power-on, on-demand, and on a periodic basis

For the above error case, the device can be powered cycle to reinitiate the power-up self-tests.

Please note: An RSA signature verification known-answer test (KAT) is performed prior to the firmware integrity test being performed.

10.2 CONDITIONAL SELF-TESTS

Table 21 – Conditional Self-Tests

Algorithm or Test	Test Properties	Test Method	Type	Indicator	Details	Conditions for Performing Test
AES CBC	256-bit	KAT	CAST	Success: LED blinks at 3Hz Error: LED blinks at 16Hz	Encrypt KAT Decrypt KAT	Power-on & Periodically (11 mins)
AES ECB	256-bit	KAT	CAST	Success: LED blinks at 3Hz Error: LED blinks at 16Hz	Encrypt KAT Decrypt KAT	Power-on & Periodically (11 mins)
AES KW	256-bit	KAT	CAST	Success: LED blinks at 3Hz Error: LED blinks at 16Hz	Key Wrap KAT Key Unwrap KAT	Power-on & Periodically (11 mins)
AES XTS	256-bit	KAT	CAST	Success: LED blinks at 3Hz Error: LED blinks at 16Hz	Encrypt KAT Decrypt KAT	Power-on & Periodically (11 mins)
AES-XTS Key Gen (Ref: IG C.I)	XTS Key Validity	--	--	Success: LED blinks at 3Hz Error: LED blinks at 16Hz	Key1≠ Key2	Generation of DEK_CO or DEK_U

Algorithm or Test	Test Properties	Test Method	Type	Indicator	Details	Conditions for Performing Test
DRBG	Instantiate, Generate and Reseed[5]	KAT	CAST	Success: LED blinks at 3Hz Error: LED blinks at 16Hz	Instantiate KAT Generate KAT	Power-on & Periodically (11 mins)
ECC CDH P-256	ECC CDH P-256 keypair pairwise consistency test.	PCT	PCT	Success: LED blinks at 3Hz Error: LED blinks at 16Hz	Performed immediately after key generation during key agreement	ECC CDH keypair generation during key agreement when 'Open Partition' service is called.
ECC CDH P-256	ECC CDH P-256 Public Key Validation	PKV	PKV	Success: LED blinks at 3Hz Error: LED blinks at 16Hz	Full Public Key Validation of host public key	Part of key agreement when 'Open Partition' service is called.
Entropy Source	N/A	APT/RCT	APT	Success: LED blinks at 3Hz Error: LED blinks at 16Hz	Adaptive Proportion Test	Continuous
HMAC-SHA2-256	256-bit	KAT	CAST	Success: LED blinks at 3Hz Error: LED blinks at 16Hz	HMAC KAT	Power-on & Periodically (11 mins)
KAS-ECC-SSC	Private Key:256-bit Public Key: 256-bit	KAT	CAST	Success: LED blinks at 3Hz Error: LED blinks at 16Hz	Compares output with expected result	Power-on & Periodically (11 mins)
KDA	Shared Secret: 256-bit	KAT	CAST	Success: LED blinks at 3Hz Error: LED blinks at 16Hz	Compares output with expected result	Power-on & Periodically (11 mins)
PBKDF	Salt 256-bit, Password: 8-bytes	KAT	CAST	Success: LED blinks at 3Hz Error: LED blinks at 16Hz	Compares output with expected result	Power-on & Periodically (11 mins)
SHA2-256	N/A	KAT	CAST	Success: LED blinks at 3Hz Error: LED blinks at 16Hz	SHA2-256 KAT	Power-on & Periodically (11 mins)
RSA-2048	RSA 2048 & SHA2-256	KAT	CAST	Success: LED blinks at 3Hz Error: LED blinks at 16Hz	Signature Verification KAT	Power-on & Periodically (11 mins)

10.3 Periodic Self-Tests

The module performs all self-tests automatically (with no operator intervention) every 11 minutes after being powered-on.

[5] The module is reseeded after every 10,000 DRBG operations.

10.4 Error States

The module supports the following error states:

Table 22 – Error States

State Name	Description	Conditions	Recovery Mode	Indicator
Hard Error	Hard Error State	Transitions to this state for all self-test errors	Power-Cycle	LED Blink Pattern, Error Code.
Soft Error	Soft Error State	Transitions to this state for all non-critical errors	Automatic	LED Blink Pattern, Error Code.

The module transitions into an error state when an error condition is encountered and provides an unambiguous error status indicator (i.e., blinking LED and error code). All data output is inhibited while the module is in the error state.

10.5 Operator Initiation of Self-Tests

The operator can initiate the self-tests at any time by power-cycling the module or via the 'Perform Self-Tests' command.

11. LIFE-CYCLE ASSURANCE

11.1 Installation, Initialization, and Startup Procedures

The User must configure and enforce the following initialization procedures:

1. Connect the *IronKey D500S Series USB Flash Drive* to a GPC. The module will enumerate onto the GPC and register its CD ROM partition. Locate and run the application located on the CD-ROM partition.
2. Follow the instructions presented by the application to 'Initialize' the module. Setup the new CO password and continue to login to the device.
3. Click on the Kingston icon in the system tray to bring up a pull-up menu and select "About - D500S" option (*refer to Figure 2*). The application will display the firmware and application versions. Verify that the firmware version is 3.06. This is the FIPS validated version of the module.

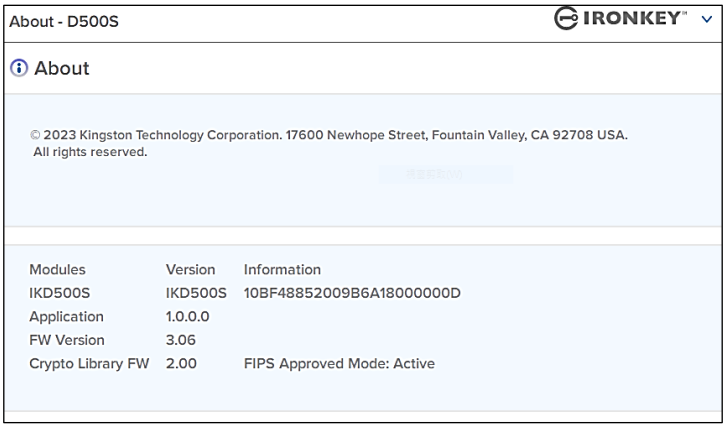

Figure 2 - PC Application

11.2 Administrator Guidance

Upon receipt of the module an operator must follow the initialization procedure outlined in Section 11.1. This establishes the operator as the Cryptographic Officer (CO) with a valid ID and password.

The module is designed to securely store authorized user's data files using physical and logical security methods. A user may transfer files to the device via a compatible PC or similar device. Over the life of the device an operator may:

- Initialize the device as a single operator (CO only).
- Initialize the device for multiple operators (CO and User).
- Transfer files to the device for secure storage.
- Reset the device effectively erasing all data and security parameters.

Services available to the CO role are listed in Table 12.

11.3 Non-Administrator Guidance

The cryptographic officer must establish access for additional operators. Additional operators will be assigned to the User role. An operator under the User role shall authenticate and transfer files to the device via a compatible PC or similar device. Services available to the User role are listed in Table 12.

11.4 Design and Rules of Operation

In the approved mode of operation, the module shall adhere to the following rules:

- The module prohibits operator passwords less than 8 characters.
- The module generates at a minimum 256 bits of entropy for use in key generation (*refer to ESV validation #E55).*
- The cryptographic module satisfies the requirements of FIPS 140-3 IG C.I for AES-XTS key generation (i.e., key_1 ≠ key_2).

- The cryptographic module does not output CSPs in any form.
- The cryptographic module enters its defined error state upon failure of self-tests, ceasing cryptographic services.
- The approved DRBG is used for generating cryptographic keys.
- The cryptographic module enforces identity-based authentication for security relevant services.
- The operator can invoke the module to perform the Pre-Operational and Conditional self-tests on-demand by power-cycling the module.
- The module performs firmware integrity test as part of the Pre-Operational self-tests at power-on, prior to each operator authentication, on demand and automatically after a set period of time.
- The module does not support concurrent operators.
- The module inhibits data output via the data output interface during self-tests, SSP generation, error states and zeroization.
- Modification of PSPs by unauthorized operators is prohibited.
- The module does not support bypass mechanisms.
- The module does not support maintenance role.
- The operator cannot change roles without first exiting from the currently assumed role.
- Cryptographic keys derived from passwords conformant with NIST standard Special Publication (SP) 800-132 - 'Recommendation for Password-Based Key Derivation' (PBKDF) may only be used in storage applications.

11.5 End of Life

Upon the need to decommission the module, the CO should perform a 'Reset Drive' operation to securely overwrite all security parameters which makes all stored data unrecoverable. The module can then be repurposed or physically scrapped.

12. MITIGATION OF OTHER ATTACKS

This module is not designed to mitigate other attacks beyond the scope of FIPS 140-3 requirements.

13. APPENDIX A: REFERENCES

Table 23 – References

Reference Number	Reference Title	Publishing Entity	Publication Date
1	ISO/IEC 19790 – Security requirements for cryptographic modules	ISO/IEC	2015
2	ISO/IEC 24759 – Test requirements for cryptographic modules	ISO	2015
3	FIPS 140-3 – Security requirements for cryptographic equipment	NIST	2019
4	SP 800-140 – FIPS 140-3 Derived Test Requirements (DTR)	NIST	2020
5	SP 800-140A – CMVP Documentation Requirements	NIST	2020
6	SP 800-140B – CMVP Security Policy Requirements	NIST	2022
7	SP 800-140C – CMVP Approved Security Functions	NIST	2023
8	SP 800-140D – CMVP Approved Sensitive Security Parameter Generation and Establishment Methods	NIST	2023
9	SP 800-140E – CMVP Approved Authentication Mechanisms	NIST	2020
10	SP 800-140F – CMVP Approved Non-Invasive Attack Mitigation Test Metrics	NIST	2020

14. APPENDIX B: ABBREVIATIONS AND DEFINITIONS

Table 24 – Abbreviations and Definitions

Term	Definition
ANSI	American National Standards Institute
CMVP	Cryptographic Module Validation Program
CSEC	Communications Security Establishment of Canada
CSP	Critical Security Parameter
DRBG	Deterministic Random Bit Generator
DTR	Derived Test Requirements
ECB	Electronic Codebook
FIPS	Federal Information Processing Standards
GPC	General Purpose Computer
GUI	Graphical User Interface
HMAC	Hashed Message Authentication Code
KAT	Known Answer Test
NIST	National Institute of Standards and Technology
NVRAM	Non-Volatile Random Access Memory
PBKDF	Password-Based Key Derivation Function
RNG	Random Number Generator
RSA	Rivest Shamir Adelman
SHA	Secure Hash Algorithm
USB	Universal Serial Bus