DataLocker Inc.
DL4FE

FIPS 140-2 Non-Proprietary Security Policy

TABLE OF CONTENTS

TABLE OF TABLES

1. CRYPTOGRAPHIC MODULE SPECIFICATION

1.1 SECURITY LEVEL

The module meets the overall requirements of FIPS 140-2 Level 3.

Table 1 – Module Security Level

FIPS Area	FIPS Security Requirement	Level
1	Cryptographic Module Specification	*3*
2	Module Ports and Interfaces	*3*
3	Roles, Services, and Authentication	*3*
4	Finite State Model	*3*
5	Physical Security	*3*
6	Operational Environment	*N/A*
7	Cryptographic Key Management	*3*
8	EMI/EMC	*3*
9	Self-Tests	*3*
10	Design Assurance	*3*
11	Mitigation of Other Attacks	*N/A*

1.2 OVERVIEW

This document defines the Security Policy for the DataLocker Inc. (DataLocker) DL4FE module, hereafter "the module". The module is an encrypted portable storage device, featuring three crypto processors, which provide layers of cryptographic protection. It requires no additional software or drivers to be installed on the host PC. The module is intended for use by US Federal agencies or other markets that require FIPS 140-2 validated encrypted storage.

The physical form of the module is depicted in Figure 1 and the module versions are given in Table 2. The module is a multi-chip standalone embodiment as defined by FIPS 140-2 and conforms to Security Level 3. The cryptographic boundary is the outer perimeter of the module's enclosure[1].

[1]Several non-sensitive components within the cryptographic boundary are excluded from the requirements of FIPS 140-2 under AS.01.09. These components are primarily passive in nature (e.g. resistors, capacitors, LED) or provide additional support to the general functionality of the module (e.g. enclosure, HDD/SSD, LCD touch panel). Failure or malfunction of these components would not compromise the security of the module.

Table 2 – Module Versions

Model	Hardware Versions	Firmware Versions	Difference in Models
DL4FE – 500GB HDD	DL4-500GB-FE	Firmware Versions 1.49 and 2.11 Bootloader Version 1.12	500GB HDD
DL4FE – 1TB HDD	DL4-1TB-FE		1TB HDD
DL4FE – 2TB HDD	DL4-2TB-FE		2TB HDD
DL4FE – 500GB SSD	DL4-SSD-500GB-FE		500GB SSD
DL4FE – 1TB SSD	DL4-SSD-1TB-FE		1TB SSD
DL4FE – 2TB SSD	DL4-SSD-2TB-FE		2TB SSD
DL4FE – 4TB SSD	DL4-SSD-4TB-FE		4TB SSD
DL4FE – 7.6TB SSD	DL4-SSD-7.6TB-FE		7.6TB SSD
DL4FE – 16TB SSD	DL4-SSD-16TB-FE		16TB SSD

Figure 1 – DL4FE

1.3 MODES OF OPERATION

The module only supports an Approved mode of operation and cannot be configured to operate in a non-Approved mode. Once the operator has authenticated, the unlocked screen will display "FIPS AES-256-XTS" along with the evaluated firmware version, "DL4FE Ver 1.49" or "DL4FE Ver 2.11". The Bootloader Version (1.12) can be verified via the SDK.

2. MODULE PORTS AND INTERFACES

The module supports the following ports and interfaces:

Table 3 - Physical Ports and Logical Interfaces

Physical Port	Logical Interface	Description
LCD Touch Panel	Control in | Data in | Status out	Used to enter configuration options, as well as to support authentication.
USB Port	Power | Control in | Data in | Data out | Status out	Transfers data in/out, as well as supporting the SDK API.
Buzzer	Status out	Audible feedback
LED	Status out	Indicates power and drive status

3. ROLES, SERVICES, AND AUTHENTICATION

Table 4 lists all operator roles supported by the module. The module does not support a maintenance role or bypass capability. The module does not support concurrent operators. Stored authentication data is protected by the physical security mechanisms employed by the module and all previous authenticated states are cleared upon power cycle.

3.1 ROLES

The module supports a single User and a single Cryptographic Officer (CO) role; the role is explicitly selected during the authentication process via the LCD touchscreen.

3.2 IDENTIFICATION AND AUTHENTICATION

The module supports identity-based authentication by requiring a unique username and password for each operator. The module is configured to self-destruct after a pre-configured amount of consecutive failed authentication attempts (10) across all roles, which is configurable up to 50. The module does not include a default passphrase and the module enforces the CO to configure their own during initialization. If the optional User is created, the User must also configure a passphrase.

Table 4 – Roles and Authentication

Role	Role Selection	Auth. Type	Authentication Method	Authentication Strength
Cryptographic Officer	Explicitly selected	Identity-based	Username and minimum 8-character password.	The password is between 8 and 64 characters in length and is obscured during entry. The password is selected from 46 possible symbols. As a result, the probability that a random authentication attempt will succeed is one in 46^8 (which is less than one in 1,000,000). The module will self-destruct and zeroize all CSPs if enough consecutive failed authentication attempts are made. The number of failed authentication attempts allowed is between 10 and 50, depending on the selected configuration. Therefore, the highest probability that a brute force attack will succeed in one minute is 50 in 46^8, which is less than the required probability of one in 100,000.
User	Explicitly selected	Identity-based	Username and minimum 8-character password.	Same as CO.
Unauthenticated Role	N/A	N/A	N/A	N/A

3.2.1 INITIALIZATION

The module does not include a default passphrase. Upon first use, the module enforces the CO to configure their own during initialization. If the optional User role is created, the User must also configure a passphrase. There are no other instructions for initializing the module for use in the Approved mode of operation.

3.3 SERVICES

Table 5 specifies all services available within the module and the modes of access each service has to the CSPs and PSPs (as specified in Section 6.2). The module does not support input or output of secret or private keys. Passphrases are either entered directly into module through a dedicated physical port or input encrypted by the Session Encryption Key. The modes of access shown in the table are defined as:

- G = Generate: The module generates or derives the CSP or PSP.
- O = Output: The CSP or PSP is output from the module.
- I = Input: The CSP or PSP is input into the module.
- E = Execute: The module uses the CSP or PSP in performing a cryptographic operation.
- Z = Zeroise: The module zeroises the CSP or PSP.

Table 5 – Services Available

Role(s) with Service Access	Service	Description	Access Rights to CSPs/PSPs
CO	Change Settings	Configure operational settings	E: Passphrase, KEK, SBK
	Show System	Show the current system configuration	E: SBK
	Create User Account	Create User account	None
	Zeroize Drive	Destroys all copies of the DEK, invalidates passphrases, and generates a new DEK. Holding down the "Zeroize Drive" service option via the Touch Panel for five seconds will cause a factory reset. If the command is received via the SDK, then the module may be configured to destroy device instead (DEK and firmware are destroyed).	Z: All CSPs G/E: DRBG EI, DRBG-State G: DEK G/E: SBK
	Reset	Soft Reset. The equivalent of power cycling.	Z: DRBG EI, DRBG-State, KEK, SS, SEK, EPrK
CO and User	Login	Authenticate to the module via the LCD Touch Panel	I/E: Passphrase G/E: KEK E: DEK, SBK
	Lock Device	Log out the operator and lock the device	Z: SS, SEK, EPr
	Secure Channel	Establish an AES-CTR encrypted secure channel with Host PC	G/E: DRBG EI, DRBG-State, SS, SEK, EPrK G/E/O: EPuK E/I: EPPuK
	Change Password	Update operator passphrase and SilentKill Code	I/E: Passphrase G/E: KEK E: SBK
	Encrypt Data	Encrypt user data in persistent storage	E: DEK
	Decrypt Data	Decrypt user data in persistent storage	E: DEK
	SilentKill	Destroys all copies of the DEK, invalidates passphrases, and generates a new DEK.	Z/G/E: DRBG EI, DRBG-State Z/I/E: Passphrase G/E: KEK Z/G: DEK

Role(s) with Service Access	Service	Description	Access Rights to CSPs/PSPs
	Self-Destruct	The module may be configured to either destroy device (DEK and firmware are destroyed) or destroy data only (DEK is destroyed and data is lost).	Z: All CSPs
	Firmware Update	Update the firmware or Virtual CD-ROM contents (VCD); the VCD is not firmware and only contains data.	G/E: SS, SEK, EPrK E/I: VCD-LOAD-PUB, FW-LOAD-PUB
	Remount	Dismount and remount the private partition	G/E: KEK E: DEK, SBK
	Get Info	Retrieve device information, such as firmware version and serial number.	None
Unauthenticated	Self-tests	Reset the module by power-cycling to invoke self-tests on demand.	None
	Show Status	Status via LCD Display, buzzer, and LEDs	None

3.4 SECURITY RULES

This section documents the security rules enforced by the cryptographic module to implement the security requirements of a FIPS 140-2 Level 3 module.

1. The module provides two distinct operator roles: User and Cryptographic Officer.
2. The module provides identity-based authentication and clears previous authentications on power cycle.
3. An operator does not have access to any cryptographic services prior to assuming an authorized role.
4. The module allows the operator to initiate power-up self-tests by power cycling power or resetting the module. Power up self-tests do not require any operator action.
5. Data output is inhibited during key generation, self-tests, zeroization, and error states.
6. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
7. There are no restrictions on which keys or CSPs are zeroized by the zeroization service.
8. The module does not support concurrent operators, a maintenance interface, or maintenance role.
9. The module does not support manual key entry.
10. The module does not have any proprietary external input/output devices used for entry/output of data.
11. The module does not output intermediate key values or plaintext CSPs; plaintext operator passwords are entered directly via the touch screen panel.

12. All CSPs are protected from unauthorized disclosure, modification, and substitution.
13. All PSPs are protected from unauthorized modification and substitution.
14. When the module is in an error state, the operator shall not have access to any cryptographic service.

4. PHYSICAL SECURITY

The DL4FE is protected by an opaque epoxy and conforms to FIPS 140-2 Level 3 physical security requirements. Epoxy hardness was tested at ambient temperature and no assurance is provided for Level 3 hardness conformance at any other temperature

The operator is required to physically inspect the module for indications of tampering attempts at intervals specified by their organization's policies. The fascia can be removed without tamper evidence and should be inspected when examining for tamper evidence.

5. OPERATIONAL ENVIRONMENT

The FIPS 140-2 Area 6 (Operational Environment) requirements for the module are not applicable because the device does not contain a modifiable operational environment. The module's operational environment is limited. The module includes a firmware load service to support necessary updates. Firmware versions validated through the FIPS 140-2 CMVP will be explicitly identified on a validation certificate. Any firmware not identified in this Security Policy does not constitute the module defined by this Security Policy or covered by this validation.

6. CRYPTOGRAPHIC KEY MANAGEMENT

6.1 ALGORITHMS

The module supports the following cryptographic algorithms. Note the referenced certificates include additional modes and options, but only what is listed in the table below are actively employed within the module.

6.1.1 FIPS APPROVED ALGORITHMS

Table 6 – FIPS Approved Algorithms

CAVP Cert(s)	Algorithm	Standard(s)	Modes/ Methods	Key Lengths, Curves, or Moduli, Strengths	Use
3971	AES	[197], [38A]	CTR, GCM[2]	256 bits	Encrypt, Decrypt

[2] The IV is randomly generated internally using the Approved DRBG (Cert. #1187) and is 96 bits in length per IG A.5.

CAVP Cert(s)	Algorithm	Standard(s)	Modes/ Methods	Key Lengths, Curves, or Moduli, Strengths	Use
5695	AES	[197], [38E], IG A.9	XTS[3]	256 bits	Encrypt, Decrypt
Vendor Affirmed	CKG	[133], IG D.12	Section 4 and 6.1: Direct symmetric key generation using unmodified DRBG output		Key Generation
1187*	DRBG	[90A]	HASH_DRBG	SHA-256	Deterministic Random Bit Generation Security Strength = 256
890*	ECDSA	[186]		P-256	ECC key generation
			SHA-256	P-256	Digital signature verification
2589	HMAC	[198]	SHA-256	(See PBKDF)	Used within PBKDF
Vendor Affirmed	KAS-SSC	[56Ar3]	Ephemeral Unified ECC CDH	P-256 Key establishment methodology provides 128 bits of encryption strength.	Shared secret computation (relying on ECDSA #890 key generation).
Vendor Affirmed	KDA	[56Cr1]	One-step KDF w/ SHA-256	N/A	Key derivation of Session Encryption Key from KAS-SSC, prerequisite SHA-256 (Cert. #3299).
Vendor Affirmed	PBKDF	[132], IG D.6	Option 1a	Based on password	Key derivation. Keys derived using PBKDF are only used for storage applications, prerequisite HMAC-SHA-256 (Cert. #2589).
3275	SHS	[180]	SHA-256		Message Digest Generation
3299*	SHS	[180]	SHA-256		Used within HASH_DRBG and ECDSA Signature Verification
4565	SHS	[180]	SHA-256		Firmware Integrity Test

*Algorithms demarked with an * are provided by the embedded FIPS 140-2 module (Cert. #3175)

[3] The XTS algorithm implementation includes a check to ensure Key_1 ≠ Key_2. XTS is only used to protect stored data.

6.1.2 FIPS ALLOWED ALGORITHMS

Table 7 – FIPS Allowed Algorithms

Algorithm	Standard(s)	Key Lengths, Curves, or Moduli	FIPS Caveat	Use
NDRNG	IG 7.14, Case 1a	Provides 384 bits of entropy input to DRBG (Cert. #1187). Minimum of 8 bits per access, buffered by the device driver, which also performs the continuous RNG test when a 32-bit value is available.	N/A	Entropy source to seed the DRBG

6.2 CSP AND PSP MANAGEMENT

6.2.1 CRITICAL SECURITY PARAMETERS (CSPS)

Table 8 – CSPs

CSP/ Key	Security Function	Strength	Description
DRBG-EI	DRBG	384 bits	DRBG entropy input (384 bits) to the Hash_DRBG.
DRBG-State	DRBG	880 bits	Hash_DRBG internal state.
Passphrase	PBKDF	8-64 characters	User or CO authentication passphrase, inclusive of numbers, letters, and special characters (!, *, -, %, ~, #, . , @, &, $).
Key Encryption Key (KEK)	AES-GCM	256 bits	Key derived from the passphrase using PBKDF2. The Key Encryption Key is used to encrypt the Data Encryption Key.
Data Encryption Key (DEK)	AES-XTS	256 bits	Key used to encrypt user data for persistent storage.
Shared Secret (SS)	KAS-SSC	P-256 (128 bits)	The shared secret calculated per SP800-56A-rev3. Used as input to the SP800-56C-rev1 KDF to establish the Session Encryption Key.
ECDH Private Key (EPrK)	KAS-SSC	P-256 (128 bits)	ECC key used to establish the Session Encryption Key.
Session Encryption Key (SEK)	AES-CTR	256 bits	Symmetric key is established by ECDH and used for encryption of the USB session with the client application.
System Base Key (SBK)	AES-CTR	256 bits	Symmetric key used to encrypt system configuration data.

6.2.2 PUBLIC SECURITY PARAMETERS (PSPS)

Table 9 – PSPs

PSP/ Key	Security Function	Strength	Description
VCD-Load-Pub	ECDSA	P-256 (128 bits)	ECDSA P-256 Public Key for update of the Virtual CD-ROM contents (operator data stored in a restricted volume).
FW-Load-Pub	ECDSA	P-256 (128 bits)	ECDSA P-256 Public Key for firmware integrity and upgrade signature verification. Also used to verify bootloader integrity.
ECDH Public Key (EPuK)	KAS-SSC	P-256 (128 bits)	ECC P-256 key used to establish the Session Encryption Key.
ECDH Peer Public Key (EPPuK)	KAS-SSC	P-256 (128 bits)	ECC P-256 key used to establish the Session Encryption Key.

6.2.3 ZEROIZATION

The Self-Destruct and Zeroize Drive services satisfy the zeroization requirements of FIPS 140-2. Other services that may partially zeroize the module are described in Table 5.

7. SELF-TESTS

All Power-On Self-Tests (POSTs) must be completed successfully prior to any other use of cryptography by the module. If one of the POSTs fails, the module enters the error state and will output an error message to the attached screen prior to shutting down; otherwise it indicates successful completion by presenting the login screen.

If an error is encountered during POSTs, operators must power-cycle the device to reinitiate the power-up self-tests. The module can be used if tests are successful.

7.1 POWER-ON SELF-TESTS

Table 10 – Power-On Self-Tests

Tested Function	Self-Test
Firmware Integrity of Microcontroller	16-bit CRC
Firmware Integrity of Bridge Controller	SHA-256 (Cert. #4565)
Firmware Integrity of Bootloader	ECDSA (Cert. #890) P-256 Signature Verification
Firmware Integrity of Firmware	ECDSA (Cert. #890) P-256 Signature Verification

Tested Function	Self-Test
AES-CTR (Cert. #3971)	Encrypt and Decrypt KATs
AES-GCM (Cert. #3971)	Encrypt and Decrypt KATs
AES-XTS (Cert. #5695)	Encrypt and Decrypt KATs
DRBG: HASH_DRBG (Cert. #1187)	Performs a fixed input KAT and all SP 800-90A health test monitoring functions
ECDSA (Cert. #890)	ECDSA Signature Verification KAT
KAS-SSC	ECDH Shared Secret Computation KAT per IG D.8
KDA	KDA KAT
PBKDF (HMAC Cert. #2589 is also tested)	PBKDF KAT, which also satisfies HMAC SHA-256 KAT
SHA-256 KATs (Cert. #3275, 4565, and 3299)	SHA-256 KATs for all implementations

7.2 CONDITIONAL SELF-TESTS

The module supports the following conditional self-tests:

Table 11 – Conditional Self-Tests

Tested Function	Self-Test
NDRNG	Continuous RNG test per IG 9.8 to assure output is different than the previous value
DRBG (Cert. #1187)	Continuous RNG test per IG 9.8 to assure output is different than the previous value
EC Pairwise Consistency Test	Pairwise Consistency Test (PWCT) for Key Generation
ECC Full Public Key Validation	As specified by [56Ar3], Section 5.6.2.3.3
Firmware Load Test	ECDSA (Cert. #890) P-256 signature verification of SHA-256 based signature

8. MITIGATION OF OTHER ATTACKS

This module is not designed to mitigate other attacks beyond the scope of FIPS 140-2 requirements.

9. APPENDIX A: REFERENCES

Table 12 – References

Reference Number	Reference Title	Publishing Entity	Publication Date
140-2	Security Requirements for Cryptographic Modules	NIST	May 25, 2001
IG	Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program	NIST	August 28, 2020
131A	Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths	NIST	March 2019
132	NIST Special Publication 800-132, Recommendation for Password-Based Key Derivation, Part 1: Storage Applications	NIST	December 2010
133	NIST Special Publication 800-133 Revision 2, Recommendation for Cryptographic Key Generation	NIST	June 2020
186	National Institute of Standards and Technology, Digital Signature Standard (DSS), Federal Information Processing Standards Publication 186-4	NIST	July 2013
197	National Institute of Standards and Technology, Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197	NIST	November 26, 2001
198	National Institute of Standards and Technology, The Keyed-Hash Message Authentication Code (HMAC), Federal Information Processing Standards Publication 198-1	NIST	July 2008
180	National Institute of Standards and Technology, Secure Hash Standard, Federal Information Processing Standards Publication 180-4	NIST	August 2015
38A	National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation, Methods and Techniques, Special Publication 800-38A	NIST	December 2001
38E	National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices, Special Publication 800-38E	NIST	January 2010
56Ar3	NIST Special Publication 800-56A Revision 3, Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography	NIST	April 2018
56Cr1	NIST Special Publication 800-56C Revision 1, Recommendation for Key-Derivation Methods in Key-Establishment Schemes	NIST	August 2018
90A	National Institute of Standards and Technology, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, Special Publication 800-90A	NIST	June 2015