DataLocker Enterprise, V2.0 (DataLocker DL2)

DataLocker, Inc.

FIPS 140-2 Security Policy

Version 1.1

Last Update: 2016-06-28

Table of Contents

Document History

Version	Date of Change	Author	Changes to Previous Version
0.1	2010-06-02	atsec	Initial draft
0.2	2010-06-11	atsec	Updated block diagram and module image
0.3	2010-08-15	atsec	Including DataLocker revisions
0.5	2010-09-08	atsec	Additional DataLocker revisions for Design Assurance
0.6	2010-11-10	atsec	Addition of pictures, minor revisions for clarity
0.7	2010-11-11	atsec	Updates based on initial internal review
0.8	2010-11-17	atsec	Set Area 3 to Level 2, Added Area 11
0.9	2011-01-19	atsec	Response to NIST comments
1.0	2011-02-11	atsec	Version for public release
1.1	2016-06-28	atsec	Added alias module name

Acronyms

AES	Advanced Encryption Standard
ASIC	Application Specific Integrated Circuit
CBC	Cipher Block Chaining
CO	Cryptographic Officer
CPU	Central Processing Unit
CSP	Critical Security Parameter
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FIPS	Federal Information Processing Standard
HDD	Hard Disk Drive
LCD	Liquid Crystal Display
NIST	National Institute of Standards and Technology
PIN	Personal Identification Number
RAM	Random Access Memory
ROM	Read Only Memory
SATA	Serial Advanced Technology Attachment
USB	Universal Serial Bus

1. Cryptographic Module Specification

Security Component	Security Level
Cryptographic Module Specification	1
Cryptographic Module Ports and Interfaces	1
Roles, Services and Authentication	2
Finite State Model	1
Physical Security	1
Operational Environment	N/A
Cryptographic Key Management	1
EMI/EMC	3
Self Tests	1
Design Assurance	1
Mitigation of Other Attacks	1

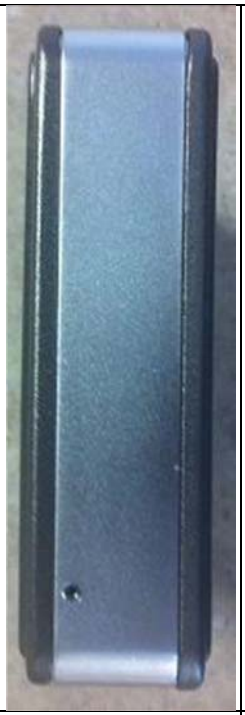
1.1. Description of Module

The DataLocker Enterprise, V2.0 (DataLocker DL2), (hereafter referred to as the cryptographic module, module, or the DataLocker) is a secure, portable multiple-chip standalone, data storage solution that is platform independent and provides hardware-based AES encryption to protect User data. All authentication, encryption and administration processes are performed by the DataLocker through its integrated touch screen display without the need to interface a host system. Two configurations of the module are available, which are identical with the exception of their internal hard disk size; the DL500E2 includes a 500 GB hard disk, where as the DL1000E2 includes a 1 TB hard disk.L

The module is comprised of the following hardware and firmware components:

- DataLocker Enclosure (Part Numbers: DL500E2, DL1000E2)
- DataLocker Firmware Version 2.30
- A 2.5 Inch SATA Hard Drive.

Image 1: Front

				
Image 2: Back	**Image 3: Top**	**Image 4: Left**	**Image 5: Bottom**	**Image 6: Right**

1.2. Description of Approved Mode

The cryptographic module supports the following Approved algorithms in the Approved mode of operation:

- AES CBC mode, 128 and 256-bit keys (Cert. #250)

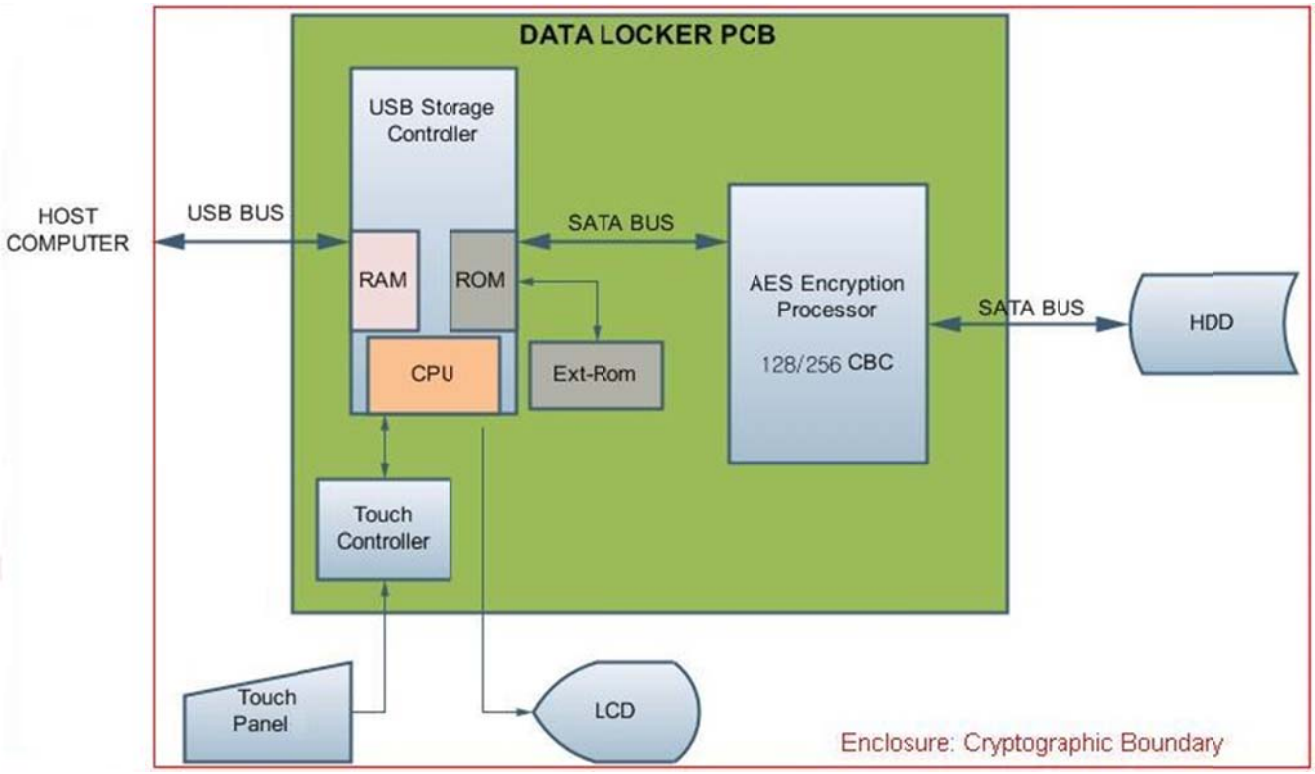
The module also supports a non-Approved mode where the operator may generate AES encryption keys using a non-Approved method for data encryption. Switching between the modes of operation will invoke zeroization and destroy all existing critical security parameters (CSPs).

The operator may determine the mode of operation by verifying a FIPS mode flag; on the home screen, “FIPS KEY ACTIVE” will be displayed to indicate the Approved mode of operation.

1.3. Cryptographic Module Boundary

The cryptographic boundary is defined as the physical perimeter of the hard, opaque enclosure. No components have been excluded from the cryptographic boundary.

1.4.Block Diagram



2. Cryptographic Module Ports and Interfaces

The DataLocker supports the following physical ports and logical interfaces:

- LCD Touch Panel: Data Input, Data Output, Control Input, Status Output
- USB Port: Power Input, Data Input, Data Output, Control Input, Status Output
- DC In: Power Input
- Power Switch: Control Input
- Buzzer: Status Output
- Power LED: Status Output
- HDD LED: Status Output

3. Roles, Services and Authentication

3.1. Roles

The module supports role-based authentication and two operator roles: the Cryptographic Officer, which is fulfilled by the Adminstrator, and the User. Each of the roles is implicitly selected based on the PIN entered during login. The module only supports a single Cryptographic Officer and a single User and no support is provided for multiple concurrent operators or a Maintenance operator.

3.2. Services

The following table describes the services available to each role and the CSP access rights for each role and service. Note that the Show Status and Self-Tests services do not require an authorized role to be assumed, as they are available to any operator.

- R: Read
- W: Write
- Z: Zeroize

Role/Service Access Rights Table

Role	Service	CSP	Algo/Mode(s)	Access
User, Administrator	Change Settings	N/A	N/A	N/A
User, Administrator	Change Main Key	Main Key	AES CBC	R, W
User	Change Password	PIN, Main Key	AES CBC	W (Pin), R (Main Key)
User, Administrator	Self-Destruct	PIN, Master PIN, Main Key	N/A	Z
User, Administrator	Encrypt Data	Main Key	AES CBC	R
User, Administrator	Decrypt Data	Main Key	AES CBC	R
Administrator	Change Master Password	Master PIN, Main Key	AES CBC	W (Master PIN), R (Main Key)
User, Administrator, Any	Self-Tests	N/A	N/A	N/A
User, Administrator, Any	Show Status	N/A	N/A	N/A

3.3. Operator Authentication

Each operator authenticates with a PIN that is between six and 18 digits in length and is obscured during entry. As a result, the probability that a random authentication attempt will succeed is at least one in 5,000,000. The DataLocker will self-destruct and zeroize all CSPs if nine consecutive failed authentication attempts are made. The probability that a brute force attack, given one minute of time, will succeed is 9 in 5,000,000, which is less than the required probability of one in 100,000.

Operators may not change roles; a new role may only be assumed after disconnecting from the currently assumed role and re-authenticating as the new role.

Authentication is required after each power cycle.

4. Physical Security

The module is a multi-chip standalone device that is designed to comply with FIPS 140-2 Level 1 physical security requirements. The module is contained within a hard plastic enclosure and is constructed of production grade components. There are no removable doors/covers and no maintenance interface.

5. Operational Environment

The operational environment requirements of FIPS 140-2 are not applicable, because the DataLocker has a non-modifiable operational environment.

6. Cryptographic Key Management

Keys and CSPs are protected by the physical enclosure. In addition, CSPs are stored in a reserved sector of the hard disk drive that is inaccessible to operators. There are no unauthorized interfaces through which an adversary can modify, substitute, or disclose a CSP. Keys are associated with the User or memory sector in the reserved sector. The module does not support manual key entry.

Key Life cycle Table

Name	Description	Auth Role	Generation/ Establishment	Entry/ Output	Storage	Zeroization
PIN	6-18 digit value used to authenticate the User	User thru "Change Password" service	N/A. Specified by User. Default is 6 zeroes.	Entered through the touch panel during device unlock, initialization, and update.	Reserved Sector	"Self Destruct" or "Change Main Key"
Master PIN	6-18 digit value used to authenticate the Administrator	Administrator thru "Change Master Password" service	N/A. Specified by User. Set as 6 zeroes.	Entered through the touch panel during device unlock, initialization, and update.	Reserved Sector	"Self Destruct" or "Change Main Key"
Main Key	128 or 256 bit value used to secure HDD data with AES	User or Administrator thru "Change Main Key"	N/A. Initially installed during manufacturing.	Imported during initialization in a secure environment.	Reserved Sector	"Self Destruct" or "Change Main Key"

7. Electromagnetic Interference/Electromagnetic Compatibility

The DataLocker Enterprise conforms to the EMI/EMC requirements specified by 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class B (i.e., for home use). As a result, the module complies with the requirements of FIPS 140-2, Level 3 for EMI/EMC only.

8.Self Tests

All data output is inhibited when the module is in the self-test state. Furthermore, no cryptographic services are available when the module is in a self-test state. The module is disabled in the error state and will not perform any cryptographic service while in the error state. Data output is also inhibited while in the error state. Self-tests do not require user intervention or actions to initiate. Successful completion of self-tests is indicated by display of the home screen. Self-tests may also be invoked on demand by power-cycling the device.

8.1. Power-Up Tests

The following power-up self-tests are performed. An error in either of the self-tests will cause the module to re-attempt all self-tests. If two buzzer beeps are emitted during the self-tests, then there was an error with the AES KAT, where as three buzzer beeps indicates an error with the firmware integrity test. If no errors were detected, the operator will be presented with the home screen.

- AES KAT
- Firmware Integrity Test (16-bit Checksum)

8.2. Conditional Tests

No conditional tests are supported by the module.

9. Design Assurance

9.1. Configuration Management

All source code changes are internally controlled by DataLocker company policy. All file revisions are recorded in the “exrom.c” and “releaseNote.txt” files.

All hardware modifications are subject to revision control. Release notes are recorded on the master schematic and the corresponding revision code is printed on the top of the PCB. Revision notes are recorded in the file “RevisionNote.txt” and are internally controlled.

9.2. Delivery and Operation

All initial setup is done at the factory level. AES keys are generated by an Approved RNG and injected into the DataLocker at the production facility in a secure area by only designated personnel. Each DataLocker unit undergoes extensive testing prior to delivery. The complete DataLocker unit is delivered to the end user pre-formatted and pre-initialized. The User and CO must simply set their PINs before using the DataLocker securely in the Approved mode.

9.3. Development

The DataLocker was developed using the software tools described in this section.

Firmware development tools:

1. Keil uVision C51 Compiler (RealView MDK Professional) - Firmware source code compiler.
2. BitFontCreator v1.6 - LCD Menu design tool
3. Microsoft Visual C++ 2008 - Firmware Update Utility, Master Password Utility, Key Injector

Hardware development tools:

1. Orcad Capture - Schematic design tool

2. PADS PCB - PCB Artwork

9.4. Guidance

The following security rules must be adhered to in order to operate the DataLocker securely:

1. Operators must set a PIN of no less than seven digits and no more than 18 digits.
2. The Administrator PIN must be configured.
3. Self-Destruct mode must always be enabled.

Please see the associated DataLocker User Manual for additional guidance.

10. Mitigation of Other Attacks

An attacker may be able to determine an operator's PIN by observing the geometric pattern created during PIN entry and then repeating it. This observation method is often referred to as "shoulder surfing".

The DataLocker Enterprise reduces the ability of an attacker to perform such an attack by re-arranging the touch screen keypad into one of several different patterns at each log in. Randomizing the keypad makes it more difficult for an observing attacker to determine the operator's PIN, because the geometric entry pattern will be different for each log in and cannot be imitated.

Keypad randomization is a common technique used for virtual PIN pads on PIV (Personal Identity Verification) devices used in the GSA PIV program.