FIPS 140-2 Non-Proprietary Security Policy

Kingston Technology DataTraveler DT4000 Series

Document Version 2.2

April 29, 2010

Prepared For:

Kingston Technology Company, Inc.

17600 Newhope Street

Fountain Valley, CA 92708

www.kingston.com

Prepared By:

Apex Assurance Group, LLC

5448 Apex Peakway Drive, Ste. 101

Apex, NC 27502

www.apexassurance.com

Abstract

This document provides a non-proprietary FIPS 140-2 Security Policy for the DataTraveler DT4000 Series.

Table of Contents

List of Tables

List of Figures

1 Introduction

1.1 About FIPS 140

Federal Information Processing Standards Publication 140-2 — Security Requirements for Cryptographic Modules specifies requirements for cryptographic products to be deployed in a Sensitive but Unclassified environment. The National Institute of Standards and Technology (NIST) and Communications Security Establishment of Canada (CSEC) Cryptographic Module Validation Program (CMVP) owns the FIPS 140 program. The CMVP accredits independent testing labs to perform FIPS 140 testing; the CMVP also validates test reports for all products pursuing FIPS 140 validation. *Validation* is the term given to a product that is documented and tested against the FIPS 140 criteria.

More information is available on the CMVP website at http://csrc.nist.gov/groups/STM/cmvp/index.html.

1.2 About this Document

This non-proprietary Cryptographic Module Security Policy for the DataTraveler DT4000 Series from Kingston Technology provides an overview of the product and a high-level description of how it meets the security requirements of FIPS 140-2. This document contains details on the module's cryptographic keys and critical security parameters. This Security Policy concludes with instructions and guidance on running the module in a FIPS 140-2 mode of operation.

The Kingston Technology DataTraveler DT4000 Series may also be referred to as the "module" in this document.

1.3 External Resources

The Kingston Technology website (http://www.kingston.com) contains information on the full line of products from Kingston Technology, including a detailed overview of the DataTraveler DT4000 Series solution. The Cryptographic Module Validation Program website (http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401val2009.htm) contains links to the FIPS 140-2 certificate and Kingston Technology contact information.

1.4 Notices

This document may be freely reproduced and distributed in its entirety without modification.

1.5 Acronyms

The following table defines acronyms found in this document:

Acronym	Term
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
CSEC	Communications Security Establishment of Canada
CSP	Critical Security Parameter
DTR	Derived Test Requirements
ECB	Electronic Codebook
FIPS	Federal Information Processing Standard
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
PRNG	Pseudo-Random Number Generator
RNG	Random Number Generator
SHA	Secure Hash Algorithm
USB	Universal Serial Bus

Table 1 – Acronyms and Terms

2 Kingston Technology DataTraveler DT4000 Series

2.1 Product Overview

Kingston's DataTraveler DT4000 Series USB Flash drive is assembled in the U.S. for organizations that require a secure way to store and transfer portable data. The stored data is secured by hardware-based 256-bit AES encryption to guard sensitive information in case the drive is lost or stolen. Its durable, aluminium casing provides added protection.

The Kingston's DataTraveler DT4000 Series offers unique protection to safeguard critical data even if the drive is lost or stolen. It is an enterprise-grade USB Flash drive with 256-bit on-the-fly encryption. Its strong password rules and lock-down control protect against brute force attacks. Such advanced security features make the Kingston's DataTraveler DT4000 Series drives ideal for corporations and service organizations that require employees to transport large digital files consisting of confidential documents.

2.2 Validation Level Detail

The following table lists the level of validation for each area in FIPS 140-2:

FIPS 140-2 Section Title	Validation Level
Cryptographic Module Specification	2
Cryptographic Module Ports and Interfaces	2
Roles, Services, and Authentication	2
Finite State Model	2
Physical Security	3
Operational Environment	N/A
Cryptographic Key Management	2
Electromagnetic Interference / Electromagnetic Compatibility	3
Self-Tests	2
Design Assurance	2
Mitigation of Other Attacks	N/A

Table 2 – Validation Level by DTR Section

The "Mitigation of Other Attacks" section is not relevant as the module does not implement any countermeasures towards special attacks.

2.3 Cryptographic Algorithms

2.3.1 Approved Algorithms

In FIPS mode of operation, only the following FIPS approved algorithms are to be used[1]:

- AES encryption/decryption
- SHA-256 hashing
- ANSI X9.31 Appendix A.2.4 for PRNG

2.3.2 Algorithm Implementation Certificates

The module's cryptographic algorithm implementations have received the following certificate numbers from the Cryptographic Algorithm Validation Program:

Algorithm Type	Algorithm	Standard	CAVP Certificate	Use
Random Number Generation	ANSI X9.31	ANSI X9.31 A.2.4 (AES)	607	Random Number Generation
Hashing	SHA-256	FIPS 180-3	1016	Message digest
Symmetric Key	AES CBC mode with 256-bit keys	FIPS 197	1081	Encryption / decryption for entire partition
	AES ECB mode with 128-bit keys	FIPS 197	1081	Obfuscate Data Encryption Key

Table 3 – Algorithm Certificates

2.3.3 Non-Approved Algorithms

The module implements the following non-FIPS approved algorithms:

- Hardware-based random number generator (HWRNG)
    - This HWRNG is used only as a seeding mechanism to the FIPS-approved PRNG.

2.4 Cryptographic Module Specification

The module is the Kingston Technology DataTraveler DT4000 Series running firmware version 3.00.1 on hardware controller version AE2251. The module is classified as a multi-chip standalone cryptographic module, and the physical cryptographic boundary is defined as the module's case. The physical boundary is pictured in the image below:

[1] Note that the module enforces this by default

Figure 1 – Physical Boundary

The cryptographic boundary does not include polymer case, and USB cap of the DT4000 series drive. The host application (version 3.0.0.1) is inside the crypto boundary but is excluded from validation. The potting defines the cryptographic boundary and provides sufficient physical security; compromising the exterior metallic casing does not compromise the security of the device. No excluded components process CSPs, plaintext data, or other information that if misused could lead to a compromise.

2.5 Module Interfaces

The interfaces for the cryptographic boundary include physical and logical interfaces. The physical interfaces provided by the module are mapped to four FIPS 140-2 defined logical interfaces: Data Input, Data Output, Control Input, and Status Output. The mapping of logical interfaces to module physical interfaces is provided in the following table:

FIPS 140-2 Logical Interface	Module Physical Interface
Data Input	Data pins within the USB Port
Data Output	Data pins within the USB Port
Control Input	Data pins within the USB Port
Status Output	Data pins within the USB Port LED
Power	Power pin within the USB Port

Figure 2 – Logical Interface / Physical Interface Mapping

The USB 2.0 protocol ensures these logical interfaces are distinct.

2.6 Roles, Services, and Authentication

As required by FIPS 140-2, there are two roles (a Crypto Officer role and User role) in the module that operators may assume. The module supports role-based authentication, and the respective services for each role are described in the following sections.

2.6.1 Operator Services and Descriptions

The services available to the User and Crypto Officer roles in the module are as follows:

Service	Description	Service Input	Service Output	Roles
Decommission Device	Zeroize all keys and CSPs and decommission the module	Password Authentication	Keys/CSPs zeroized and module decommissioned	Crypto Officer
Initialize	Create password and generate keys to place the module in FIPS 140 mode of operation	Enter password	Password stored, self tests run, and keys generated	User
Show Status	Verify self test success/failure	Password Authentication	Status output via LED and alert to host machine GUI	User
Encrypt	Encrypt partition with AES	Password Authentication	Partition encrypted	User
Decrypt	Decrypt AES-encrypted partition when reading from the device	Password Authentication	Partition decrypted and files are readable	User
Format Drive	Erase all files stored on the module and zeroizes keys and CSPs	Zeroization command	Partition formatted and keys/CSPs overwritten with new values	User
Run Self Tests	Performs power on self tests; invoked by inserting module into the host machine	Password Authentication	Status output of results / module disabled in tests fail, allows authentication if tests pass	User

Table 4 – Operator Services and Descriptions

2.6.2 Operator Authentication

The Crypto Officer and User roles authenticate via host machine over the module's USB port. Other than status functions available by viewing LEDs, the services described in Table 4 – Operator Services and Descriptions are available only to authenticated operators.

The module ensures there is no visible display of Crypto Officer or User authentication data during data entry.

2.6.3 Password Strength

User Passwords must be a minimum of 6 characters, which is enforced by the module. Crypto Officer passwords must be 6 characters as specified in the Guidance and Secure Operation section of this document. The password must contain three of the following four characters: lower case letters, upper case letters, numeric characters and/or special characters. Assuming a mix of lower case letters, upper case letters, numeric characters, the password can consist of the following set: {a-zA-Z0-9], yielding 62 choices per character. The probability of a successful random attempt is $1/62^6$, which is less than 1/1,000,000. Assuming 10 attempts per second via a scripted or automatic attack, the probability of a success with multiple attempts in a one-minute period is $600/62^6$, which is less than 1/100,000.

The module will lock an account after 10 consecutive failed authentication attempts; thus, the maximum number of attempts in one minute is 10. Therefore, the probability of a success with multiple consecutive attempts in a one-minute period is $10/62^6$ which is less than 1/100,000.

2.7 Physical Security

The module is a multiple-chip standalone module and conforms to Level 3 requirements for physical security. The module is composed of production-grade components and is completely covered with a hard, opaque potting material. Any attempts to remove the potting will result in permanent damage to the module.

2.8 Operational Environment

The module operates in a limited operational environment and does not implement a General Purpose Operating System.

The module meets the requirements of 47 CFR PART 15 regulation & ANSI C63.4 and ICES-003 for the evaluation of Class B of electromagnetic compatibility. This device complies with Part 15 of FCC Class B rules for home or office use.

2.9 Cryptographic Key Management

The table below provides a complete list of Critical Security Parameters used within the module:

Key/CSP Name	Description / Use	Generation	Storage	Establishment / Export	Destruction	Privileges
Data Encryption Key	AES 256-bit key for encryption / decryption of all files on the drive	Internal generation by X9.31 PRNG.	**Storage**: NVRAM plaintext (obfuscated with AES 128-bit password-derived key[2]). **Association**: The system is the one and only owner. Relationship is maintained by the controller via protected memory. Only a single AES-256 data key to encrypt a whole partition content.	**Agreement**: NA **Entry**: NA **Output**: None	Zeroization command The Crypto Officer decommissions the drive to securely wipe the contents	Crypto Officer D
						User R W D
PRNG Seed	HWRNG providing 256-bit entropy to seed the	Internal generation by HWRNG	**Storage**: RAM plaintext	**Agreement**: NA **Entry**: NA	Reset / reboot the module Generate a new	Crypto Officer D

[2] Not considered a key/CSP per FIPS 140 requirements

Key/CSP Name	Description / Use	Generation	Storage	Establishment / Export	Destruction	Privileges
	X9.31 PRNG		**Association**: The system is the one and only owner.	**Output**: NA	value Zeroization command The Crypto Officer decommissions the drive to securely wipe the contents	User None
PRNG Seed Key	HWRNG providing AES 256-bit seed key for the X9.31 PRNG	Internal generation by HWRNG	**Storage**: RAM plaintext **Association**: The system is the one and only owner.	**Agreement**: NA **Entry**: NA **Output**: NA	Reset / reboot the module Generate a new value Zeroization command The Crypto Officer decommissions the drive to securely wipe the contents	Crypto Officer D User None
Crypto Officer Password	Alphanumeric passwords for authentication to the module.	Not generated by the module; defined by Kingston technical support	**Storage**: NVRAM hashed with SHA-256 **Association**: controlled by the controller	**Agreement**: NA **Entry**: Manual **Output**: NA	The Crypto Officer decommissions the drive to securely wipe the contents	Crypto Officer R W D

Key/CSP Name	Description / Use	Generation	Storage	Establishment / Export	Destruction	Privileges
User Password	Alphanumeric passwords externally generated by a human user for authentication to the module.	Not generated by the module; defined by the human user of the host machine	**Storage**: NVRAM hashed with SHA-256 **Association**: controlled by the controller	**Agreement**: NA **Entry**: Manual **Output**: NA	Zeroization command The Crypto Officer decommissions the drive to securely wipe the contents	Crypto Officer D User R W D

R = Read W = Write D = Delete

Table 5 - Key/CSP Management Details

The module does not support key entry. The module supports entry of passwords for authentication, and these parameters are not distributed outside the cryptographic boundary.

The module will overwrite all keys and CSPs with new values when it receives the zeroization command. Data encrypted with the overwritten Data Encryption Key cannot be decrypted. When the Crypto Officer authenticates and issues a command to zeroize the device, all keys and CSPs will be zeroized, and the module will be decommissioned.

The following keys are excluded from the validation:

Key	Description	Rationale
DEK Encryption Key	128-bit AES key for encrypting the Data Encryption Key	Not considered a key/CSP per FIPS 140 requirements
Password Encryption Key	128-bit AES key for encrypting the User password	Not considered a key/CSP per FIPS 140 requirements

Table 6 – Keys/CSPs Excluded from Validation

2.10 Self-Tests

The module includes an array of self-tests that are run during startup and periodically during operations to prevent any secure data from being released and to ensure all components are functioning correctly. In the event of any self-test failure, the module will output an error dialog and will shutdown. No keys or CSPs will be output when the module is in an error state.

The module does not support a bypass function.

The following sections discuss the module's self-tests in more detail.

2.10.1 Power-On Self-Tests

Power-on self-tests are run upon every initialization of the module and if any of the tests fail, the module will not initialize. The module will enter an error state and no services can be accessed by the users. The module implements the following power-on self-tests:

- Module integrity check via CRC-16
- AES KAT (encryption and decryption)
- SHA-256 KAT
- PRNG KAT

The module performs all power-on self-tests automatically when the module is initialized. All power-on self-tests must be passed before a User/Crypto Officer can perform services. The Power-on self-tests can be run on demand by rebooting the module in FIPS approved Mode of Operation.

An operator can discern that all power-on self-tests have passed via normal operation of the module and presentation of the GUI interface. Additionally, the LED will blink slowly at 3 hertz. If the module fails a POST, a Microsoft Windows error message will display on the screen. In this case the module will not be initialized, and no critical security parameters will be available. The LED will blink rapidly at 16 hertz.

2.10.2 Conditional Self-Tests

Conditional self-tests are test that run continuously during operation of the module. If any of these tests fail, the module will enter an error state. The module can be re-initialized to clear the error and resume FIPS mode of operation. No services can be accessed by the operators. The module performs the following conditional self-tests:

- Continuous RNG test run on output of ANSI X9.31 PRNG
    - Because there is 16-byte random number output after calling RNG each time, there are two calls to generate the AES 256 key. The test is run with each call.
- Continuous test on output of ANSI X9.31 PRNG seed mechanism (HW RNG)

If the module fails a conditional self test, a Microsoft Windows error message will display on the screen.

2.11 Mitigation of Other Attacks

The module does not mitigate other attacks.

3 Guidance and Secure Operation

This section describes how to configure the module for FIPS-approved mode of operation. Operating the module without maintaining the following settings will remove the module from the FIPS-approved mode of operation.

3.1 Crypto Officer Guidance

3.1.1 General Guidance

The Crypto Officer must not disclose passwords and must store passwords in a safe location and according to his/her organization's systems security policies for password storage.

3.2 User Guidance

3.2.1 Module Initialization and Configuration

The User must configure and enforce the following initialization procedures:

1. Verify that the firmware version is 3.00.1. No other version is allowed to be used in FIPS mode of operation.
2. Do not disclose passwords and store passwords in a safe location and according to the organization's systems security policies for password storage.

Note that when the module is plugged into to a host machine for the first time, the User will create a password, and the module will be formatted.

3.2.2 General Guidance

The User must configure and enforce the following initialization procedures in order to operate in FIPS approved mode of operation:

- Verify that the firmware version of the module is Version 3.00.1. No other version can be loaded or used in FIPS mode of operation.
- All operator passwords must be a minimum of 6 characters in length.