DataTraveler 5000 Security Policy

Version 1.1

October 30, 2009

Assembled in the USA
TAA Compliant

Contents

1 Introduction

This Security Policy specifies the security rules under which the DataTraveler 5000 operates. Included in these rules are those derived from the security requirements of FIPS 140-2 and additionally, those imposed by the manufacturer. These rules, in total, define the interrelationship between:

1. Operators,
2. Services, and
3. Critical Security Parameters (CSPs).

Figure 1 DataTraveler 5000 (Topside)

Figure 2 DataTraveler 5000 (Top and Front View)

Figure 3 DataTraveler 5000 (Rear and Underside View)

1.1 DataTraveler 5000 Overview

The DataTraveler 5000 enables security critical capabilities such as operator authentication and secure storage in rugged, tamper-evident hardware. The DataTraveler 5000 communicates with a host computer via the USB interface. DataTraveler 5000 protects data for government, large enterprises, small organizations, and home users. Key features:

- Encryption technology uses Suite B algorithms approved by the U.S. government for protecting both Unclassified and Classified data
- Encrypted file storage on non-removable flash card
- Strong protection against intruder attacks

Access protection is as important as encryption strength. Data encrypted with the DataTraveler 5000 cannot be decrypted until the authorized user gains access to the device.

1.2 DataTraveler 5000 Implementation

The DataTraveler 5000 is implemented as a multi-chip standalone module as defined by FIPS 140-2. The FIPS 140-2 module identification data for the DataTraveler 5000 is shown in the table below:

Part Number	FW Version	HW Version
88007021F	03.00.04	01.00.02

The DataTraveler 5000 is available with a USB interface compliant to the *Universal Serial Bus Specification*, Revision 2.0, dated 23 September 1998. All Interfaces have been tested for compliance with FIPS 140-2. The DataTraveler 5000 also has an LED interface which supplies status output.

1.3 DataTraveler 5000 Cryptographic Boundary

The Cryptographic Boundary is defined to be the physical perimeter of the outer metal case of the DataTraveler 5000. Please see Figures 1. 2, and 3.

No hardware or firmware components that comprise the DataTraveler 5000 are excluded from the requirements of FIPS 140-2.

1.4 Approved Mode of Operations

The DataTraveler 5000 operates only in a FIPS Approved mode. The indicator that shows the operator that the module is in the Approved mode is the "GetCapabilities" command, which shows the module's firmware and hardware versions as well as the product indicator.

The DataTraveler 5000 supports the FIPS 140-2 Approved and FIPS 140-2 non-Approved, but allowed, algorithms in Table 1-1 below.

Table 1-1 Approved Algorithms supported by DataTraveler 5000

Encryption & Decryption
AES -128/192/256 (Certs. #1015 and #1016)
Digital Signatures
ECDSA - key sizes: 256, 384, 521 (Cert. #122)
Key Transport / Key Agreement
EC-Diffie-Hellman (ECDH) - key sizes: 256, 384, 521 (SP 800-56A, vendor affirmed, key agreement; key establishment methodology provides 80 bits of encryption strength)
Hash
SHA-224, SHA-256, SHA-384, SHA-512 (Certs. #972 and #973) SHA-1 (Cert. #974)
RNG
HASH_DRBG (SP 800-90) (Cert. #10)
RNG for Seeding
FIPS 186-2 RNG(Cert. #582)
Other Algorithms – Allowed, but not FIPS 140-2 Approved **Key Transport / Key Agreement**
EC-Diffie-Hellman (ECDH) - key sizes: 256, 384, 521 (key agreement; key establishment methodology provides 80 bits of encryption strength)

2 FIPS 140-2 Security Levels

The DataTraveler 5000 cryptographic module complies with the requirements for FIPS 140-2 validation to the levels defined in Table 2.1. The FIPS 140-2 overall rating of the DataTraveler 5000 is Level 2.

Table 2-1 FIPS 140-2 Certification Levels

FIPS 140-2 Category	Level
1. Cryptographic Module Specification	3
2. Cryptographic Module Ports and Interfaces	2
3. Roles, Services, and Authentication	3
4. Finite State Model	2
5. Physical Security	2
6. Operational Environment	N/A
7. Cryptographic Key Management	2
8. EMI/EMC	3
9. Self-tests	2
10. Design Assurance	3
11. Mitigation of Other Attacks	N/A

3 Security Rules

The DataTraveler 5000 enforces the following security rules. These rules are separated into two categories: 1) rules imposed by FIPS 140-2; and 2) rules imposed by the manufacturer.

3.1 FIPS 140-2 Imposed Security Rules

Table 3-1 FIPS 140-2 Policies and Rule Statements

Policy	Rule Statement
Authentication Feedback	The DataTraveler 5000 shall obscure feedback of authentication data to an operator during authentication (e.g., no visible display of characters result when entering a password).
Authentication Mechanism	The DataTraveler 5000 shall enforce Identity-Based authentication.

Policy	Rule Statement
Authentication Strength (1)	The DataTraveler 5000 shall ensure that feedback provided to an operator during an attempted authentication shall not weaken the strength of the authentication mechanism.
Authentication Strength (2)	The DataTraveler 5000 shall satisfy the requirement for a single–attempt false acceptance rate of no more than one in 1,000,000 authentications.
Authentication Strength (3)	The DataTraveler 5000 shall satisfy the requirement for a false acceptance rate of no more than one in 100,000 for multiple authentication attempts during a one minute interval.
Configuration Management	The DataTraveler 5000 shall be under a configuration management system and each configuration item shall be assigned a unique identification number.
CSP Protection	The DataTraveler 5000 shall protect all CSPs from unauthorized disclosure, modification, and substitution.
Emissions Security	The DataTraveler 5000 shall conform to the EMI/EMC requirements specified in FCC Part 15, Subpart B, Class B.
Error State (1)	The DataTraveler 5000 shall inhibit all data output via the data output interface whenever an error state exists and during self-tests.
Error State (2)	The DataTraveler 5000 shall not perform any cryptographic functions while in an Error State.
Guidance Documentation	The DataTraveler 5000 documentation shall provide Administrator and User Guidance per FIPS 140-2, Section 4.10.4.
Hardware Quality	The DataTraveler 5000 shall contain production quality ICs with standard passivation.
Interfaces (1)	The DataTraveler 5000 interfaces shall be logically distinct from each other.
Interfaces (2)	The DataTraveler 5000 shall support the following five (5) interfaces: • data input • data output • control input • status output • power input.

Policy	Rule Statement
Key Association	The DataTraveler 5000 shall provide that: a key entered into, stored within, or output from the DataTraveler 5000 is associated with the correct entity to which the key is assigned.
Logical Separation	The DataTraveler 5000 shall logically disconnect the output data path from the circuitry and processes performing the following key functions: • key generation, • key zeroization.
Mode of Operation	The DataTraveler 5000 services shall indicate that the module is in an Approved mode of operation with a standard success return code and the output of the "GetCapabilities" command.
Public Key Protection	The DataTraveler 5000 shall protect public keys against unauthorized modification and substitution.
Re-authentication	The DataTraveler 5000 shall re-authenticate an identity when it is powered-up after being powered-off.
RNG Strength	The DataTraveler 5000 shall use a 'seed input' into the deterministic random bit generator of sufficient length that ensures at least the same amount of operations are required to determine the value of the generated key.
Secure Development (1)	The DataTraveler 5000 source code shall be annotated.
Secure Development (2)	The DataTraveler 5000 firmware shall be implemented using a high-level language except limited use of a low-level language to enhance the performance of the module.
Secure Distribution	The DataTraveler 5000 documentation shall include procedures for maintaining security while distributing and delivering the module.
Self-tests (1)	The power up tests shall not require operator intervention in order to run.
Self-tests (2)	The DataTraveler 5000 shall perform the self-tests identified in Section 7.
Self-tests (3)	The DataTraveler 5000 shall enter an Error State and output an error indicator via the status interface whenever self-test is failed.

Policy	Rule Statement
Services	The DataTraveler 5000 shall provide the following services: (see Reference Table 4.2).
Firmware Integrity	The DataTraveler 5000 shall apply a SHA-384 hash to check the integrity of all firmware components.
Status Output	The DataTraveler 5000 shall provide an indication via the "GetUserState" command if all of the power up tests are passed successfully.
Strength of Key Establishment	The DataTraveler 5000 shall use a key establishment methodology that ensures at least the same amount of operations are required to determine the value of the transported/agreed upon key.
Unauthorized Disclosure	The DataTraveler 5000 shall protect the following keys from unauthorized disclosure, modification and substitution: • secret keys • private keys.
Zeroization (1)	The DataTraveler 5000 shall provide a zeroization mechanism that can be performed either procedurally by the operator *or* automatically by the DataTraveler 5000 interface firmware on the connected host platform.
Zeroization (2)	The DataTraveler 5000 shall provide the capability to zeroize all plaintext cryptographic keys and other unprotected critical security parameters within the DataTraveler 5000.

3.2 Manufacturer Imposed Security Rules

Table 3-2 Manufacturer Imposed Policies and Rule Statements

Policy	Rule Statement
Single User Session	The DataTraveler 5000 shall not support multiple concurrent operators.
No Maintenance Interface	The DataTraveler 5000 shall not provide a maintenance role/interface.
No Bypass Mode	The DataTraveler 5000 shall not support a bypass mode.

3.3 Identification and Authentication Policy

The table below describes the type of authentication and the authentication data to be used by operators, by role. For a description of the roles, see section 4.2.

Table 3-3 Identification and Authentication Roles and Data

Role	Type of Authentication	Authentication Data / Identification
Administrator (CO)	Identity-based	Service and ECDSA Signature (384-bits)
User	Identity-based	Service and PIN (minimum 7 to 262 characters)

4 DataTraveler 5000 Roles and Services

4.1 Roles

The DataTraveler 5000 supports two roles, Administrator (Crypto-Officer or CO) and User, and enforces the separation of these roles by restricting the services available to each one. Each role is uniquely identified by the service that has been requested and is associated with the role.

Table 4-1 Roles and Responsibilities

Role	Responsibilities
Administrator	The Administrator is responsible for performing Firmware Updates and setting configuration of the DataTraveler 5000. The DataTraveler 5000 authenticates the Administrator identity by way of a signature verification before accepting any FirmwareUpdate or SetConfiguration commands. The loading of new firmware will invalidate the module unless the firmware has been FIPS 140-2 validated.
User	The User role is available after the DataTraveler 5000 has been initialized. The user can generate and use secret keys for encryption services.

The DataTraveler 5000 authenticates the User identity by password before access is granted.

4.2 Services

The following table describes the services provided by the DataTraveler 5000.

Table 4-2 DataTraveler 5000 Services

Service	CO	User	Unauthenticated	Description
ChangePassword		X		Changes User Password
Format		X		Formats the mounted CDROM
GetCapabilities			X	Returns the current capabilities of the system including: global Information, media storage size and the product name. This service provides a response that indicates the approved mode of operation (see Section 3.1).
GetConfig			X	Returns the card configuration structure
GetUserState			X	Returns the state and the Logon attempts remaining.
Initialize		X		Generates a new encryption key and changes the PIN. Secure channel is required. Formats the media.
LogOff		X		Log Off; Return to unauthenticated state.
LogOn		X		Log on with the user PIN if system is initialized.
MountCDROM		X		Allows the CDROM drive to be mounted as the read/write drive. This permits the CDROM software to be updated by a user application.

Service	CO	User	Unauthenticated	Description
ReadMedia		X		Read user media from SCSI drive.
ReadUserArea			X	Get a block of data from a specified user area.
SelfTest			X	Pass/Fail Test of DataTraveler 5000. Will run the Power On Self Tests again.
SetConfig	X			Writes the card configuration structure if the signature on the structure is valid
SetupBasic SecureChannel			X	Initializes secure channel.
UpdateFirmware	X			Writes signed blocks to the firmware area of the DataTraveler 5000.
WriteMedia		X		Writes user media to SCSI drive.
WriteUserArea		X		Write a block of data to a specified user area. All areas will require the token to be logged on for writes and updates
Zeroize			X	Clears the encryption keys. Requires the Initialize command to be run again.

5 Identification and Authentication

5.1 Initialization Overview

The DataTraveler 5000 modules are initialized at the factory to be in the zeroized state. Before an operator can access or operate a DataTraveler 5000, the User must first initialize the module with a User identity and PIN.

5.2 Operator Authentication

Operator Authentication is accomplished by PIN entry by the User or valid ECDSA signature by the CO. Once valid authentication information has been accepted, the DataTraveler 5000 is ready for operation.

The DataTraveler 5000 stores the number of User logon attempts in non-volatile memory. The count is reset after every successful entry of a User PIN. If an incorrect PIN is entered during the authentication process, the count of unsuccessful logon attempts is incremented by one.

If the User fails to log on to the DataTraveler 5000 in 10 consecutive attempts, the DataTraveler 5000 will block the user's access to the module, by transitioning to the blocked state. To restore operation to the DataTraveler 5000, the operator will have to zeroize the token and reload the User PIN and optional details. When the DataTraveler 5000 is inserted after zeroization, it will power up and transition to the Zeroized State, where it can be initialized by the User.

5.3 Generation of Random Numbers

The Random Number Generators are not invoked directly by the user. The Random Number output is generated by the HASH-DRBG algorithm specified in SP 800-90 in the case of static private keys and associated key wrapping keys, ephemeral keys and symmetric keys.

5.4 Strength of Authentication

The strength of the authentication mechanism is stated in Table 5-1 below.

Table 5-1 Strength of Authentication

Authentication Mechanism	Strength of Mechanism
User Single PIN-entry attempt / False Acceptance Rate	The probability that a random PIN-entry attempt will succeed or a false acceptance will occur is 1.66 x10^{-14}. The requirement for a single–attempt / false acceptance rate of no more than 1 in 1,000,000 (i.e., less than a probability of 10^{-6}) is therefore met.
User Multiple PIN-entry attempt in one minute	DataTraveler 5000 authentication mechanism has a feature that doubles the time of authentication with each successive failed attempt. There is also a maximum bound of 10 successive failed authentication attempts before zeroization occurs. The probability of a successful attack of multiple attempts in a one minute period is 1.66 x10^{-13} due to the time doubling mechanism. This is less than one in 100,000 (i.e.,1×10^{-5}), as required.
Crypto Officer Single attempt / False Acceptance Rate	The probability that a random ECDSA signature verification authentication attempt will succeed or a false acceptance will occur is 1/2^192. The requirement for a single–attempt / false acceptance rate of no more than 1 in 1,000,000 (i.e., less than a probability of 10^{-6}) is therefore met.
Crypto Officer Multiple PIN-entry attempt in one minute	The probability of a successful attack of multiple ECDSA signature authentication attempts in a one minute period is 1/2^192. The computational power needed to process this is outside of the ability of the module. This is less than one in 100,000 (i.e.,1×10^{-5}), as required.

6 Physical Security

The DataTraveler 5000 utilizes production-grade components with an opaque metal enclosure and tamper evident seals. Tamper evident seals are applied during manufacturing. The operator should ensure that the tamper evident seals are intact, with no visible signs of tamper..

The cryptographic boundary for the module is defined as the physical perimeter of the module's metal case, which contains all hardware and firmware required for the performance of all services offered by the module.

Figure 4 DataTraveler 5000 (Tamper Label Placement)

7 Operational Environment

The DataTraveler 5000 is a limited operational environment and only executable code validated by the manufacturer may be loaded and executed on the module; therefore, the operating system requirements of FIPS 140-2 do not apply.

8 Access Control

8.1 Critical Security Parameters (CSPs) and Public Keys

Table 8-1 DataTraveler 5000 CSPs

CSP Designation	Algorithm(s) / Standards	Symbolic Form	Description
Disk Ephemeral Private	SP 800-56A	$d_{e,U}$	ECDH ephemeral private key used to generate shared secret.
Disk Key Encryption Key (DKEK)	AES 256	DKEK	AES key used to unwrap the Disk Encryption Key (DEK) .
Drive Encryption Key (DEK)	AES 512	DEK	A pair of AES 256 keys. The concatenated value is used to encrypt and decrypt the User's encrypted drive.
Hash-DRBG Seed	SP 800-90	S	FIPS 186-2-generated value used to seed the Hash-DRBG RNG.
Hash-DRBG State	SP 800-90	s_{HDRBG}	Hash_DRBG state value.
Master Encryption Key (MEK)	AES 256	MEK	AES 256 wraps / unwraps user's static private keys in storage.
Secure Channel Private	SP 800-56A	$d_{e,SCHP}$	ECDH Ephemeral Transport Private.
Secure Channel Session Key	SP 800-56A	k_{SCSK}	256 bit AES key used to encrypt and decrypt commands and responses to and from the card.
User PIN		PIN	The User's minimum 7 character PIN for authentication to the module.
User's Static Signature Private	X9.62	$d_{ECDSA,s,U}$	ECDSA Static Signature private key.
FIPS 186-2 RNG seed key	FIPS 186-2 – 512 bits		Seed key used to seed the Hash-DRBG.
User's Static Transport Private	SP 800-56A	$d_{s,U}$	ECDH Static Transport private key.

Table 8-2 DataTraveler 5000 Public Keys

Key	Algorithm(s) Standards	Description/Usage
Configuration Update Key	ANSI X9.62	The ECDSA P-384 public Key is used to verify the signature of the CO before the settings are changed.
Card Firmware Update Key	ANSI X9.62	The ECDSA P-384 public Key is used to verify the signature of the CO before loading firmware.

Key	Algorithm(s) Standards	Description/Usage
Disk Ephemeral Public	SP 800-56A	ECDH Ephemeral Transport Public P384. The key is used to generate a shared secret using ECDH with the User's Static Transport Private key.
Secure Channel Host Public	SP 800-56A	ECDH Ephemeral Transport Public P256.
Secure Channel Public	SP 800-56A	ECDH Ephemeral Transport Public P256. The key is used to generate a shared secret between the host and the card.
User's Static Signature Public	SP 800-56A	ECDH Static Signature Public P384. The key for ECDSA.
User's Static Transport Public	SP 800-56A	ECDH Static Transport Public P384. The key for ECDH.

8.2 CSP Access Modes

Table 8-3 DataTraveler 5000 Access Modes

Access Type	Description
Generate (G)	"Generate" is defined as the creation of a CSP
Delete (D)	"Delete" is defined as the zeroization of a CSP
Use (U)	"Use" is defined as the process in which a CSP is employed. This can be in the form of loading, encryption, decryption, signature verification, or key wrapping.

8.3 Access Matrix

The following table shows the services (see section 4.2) of the DataTraveler 5000, the roles (see section 4.1) capable of performing each service, the CSPs (see section 6.1) that are accessed by the service and the mode of access (see section 6.3) required for each CSP. The following convention is used: if the role column has an 'X', then that role may execute the command.

Table 8-4 DataTraveler 5000 Access Matrix

Service Name	Roles			Access to Critical Security Parameters	
	Unauthenti-cated	Administrator (CO)	User	CSPs	Access Mode
ChangePassword			**X**	k_{SCSK} $d_{s,U}$ $d_{ECDSA,s,U}$ $d_{e,U,}$ DKEK DEK PIN	**U** **U** **U** **U** **G, U, D** **U** **D,G**
Format			**X**	$d_{e,U}$ DKEK, DEK	**G, U, D** **G,U,D** **G,U**
Initialize			**X**	k_{SCSK} $d_{s,U}$ $d_{ECDSA,s,U}$ $d_{e,U,}$ DKEK DEK MEK	**U** **G** **G** **G, U, D** **G, U, D** **G** **U**
LogOff			**X**		
LogOn			**X**	k_{SCSK} $d_{s,U}$ DKEK DEK PIN	**U** **U** **G,U,D** **U** **U**
MountCDROM			**X**	DEK	**U**
ReadMedia			**X**	DEK	**U**
SetConfig		**X**		$d_{s,U}$ $d_{ECDSA,s,U}$ DEK	**D** **D** **D**
UpdateFirmware		**X**		$d_{s,U}$ $d_{ECDSA,s,U}$ DEK	**D** **D** **D**
WriteMedia			**X**	DEK	**U**

Service Name	Roles			Access to Critical Security Parameters	
	Unauthenti-cated	Administrator (CO)	User	CSPs	Access Mode
WriteUserArea			**X**		
GetCapabilities	**X**	**X**	**X**		
GetConfig	**X**	**X**	**X**		
GetUserState	**X**	**X**	**X**		
ReadUserArea	**X**	**X**	**X**		
SelfTest	**X**	**X**	**X**	s, s_{HDRBG},	**G**
SetupBasic **SecureChannel**	**X**	**X**	**X**	$d_{e,SCHP}$ k_{SCSK}	**G,D** **G,D**
Zeroize	**X**	**X**	**X**	$d_{s,U}$ $d_{ECDSA,s,U}$ DEK MEK	**D** **D** **D** **D**

9 Self-Tests

The module performs both power-on and conditional self-tests. The module performs the following power-on self-tests:

- Cryptographic Algorithm Tests:
  - AES-128, 192, 256 KATs
  - ECDSA-256, 384, 521 KATs
  - EC-Diffie-Hellman-256, 384, 521 KATs
  - SHA-224 KAT
  - SHA-256 KAT
  - SHA-384 KAT
  - SHA-512 KAT
  - HASH-DRBG KAT
  - FIPS 186-2 DRNG KAT
- Firmware Test
  - SHA-384 Hash

The module performs the following Conditional Tests:

- Firmware Load Test
  - ECDSA P-384 signed SHA-384 hash verification
- Pairwise Consistency Test
  - ECDSA key pair generation
  - EC-Diffie-Hellman key pair generation
- Continuous Random Number Generator Test
  - HASH-DRBG SP800-90
  - FIPS 186-2

10 Mitigation of Other Attacks

No claims of mitigation of other attacks listed in Section 4.11 of FIPS 140-2 by the DataTraveler 5000 are made or implied in this document.

11 Acronyms

AES	Advanced Encryption Standard
CBC	Cipher Block Chaining
CSP	Critical Security Parameter
DPA	Differential Power Analysis
DRBG	Digital Random Bit Generator
DSA	Digital Signature Algorithm
ECB	Electronic Code Book
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
ECMQV	Elliptic Curve Menezes-Qu-Vanstone
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interface
FEK	File Encryption Key
FIPS	Federal Information Processing Standard
HAC	Host Authentication Code
MKEK	Master Key Encryption Key
NDRNG	Non-deterministic Random Number Generator
PC	Personal Computer
PCB	Printed Circuit Board
PIN	Personal Identification Number
RNG	Random Number Generator
RSA	Rivest, Shamir and Adleman Algorithm
SD	Secure Digital (flash memory card)
SDHC	Secure Digital High-capacity
SHA	Secure Hash Algorithm
SPA	Simple Power Analysis
SSD	Solid-state Drive
USB	Universal Serial Bus

References

FIPS 140-2 FIPS PUB 140-2, Change Notice,
Federal Information Processing Standards Publication
(Supersedes FIPS PUB 140-1, 1994 January 11)
Security Requirements For Cryptographic Modules,
Information Technology Laboratory, National Institute of Standards and Technology (NIST), Gaithersburg, MD, Issued May 25, 2001.

FIPS 186-2 **FIPS PUB 186-2,** (+ Change Notice),
Federal Information Processing Standards Publication
DIGITAL SIGNATURE STANDARD (DSS),
National Institute of Standards and Technology (NIST), Gaithersburg, MD, Issued 2000 January 27

SP 800-56A NIST Special Publication 800-56A
Recommendation for Pairwise Key Establishment Schemes Using Discrete Logarithm Cryptography (Revised), Barker, E., Johnson, D., Smid, M., Computer Security Division, NIST, March 2007.

SP 800-90 NIST Special Publication 800-90
Recommendation for Random Number Generation Using Deterministic Random Bit Generators, Barker, E., Kelsey, J., Computer Security Division, Information Technology Laboratory, NIST, June 2006.

X9.62 American National Standards Institute (ANSI)
Public Key Cryptography for the Financial Services Industry, The Elliptic Curve Digital Signature Algorithm (ECDSA), 2005.