Aladdin Knowledge Systems, Ltd

---

eToken PRO
&
eToken PRO HD

FIPS 140-1 Non-Proprietary Security Policy

Level 2 and 3 Validations

February 4, 2003

Table of Contents

1 Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the eToken PRO (16K and 32K) and the eToken PRO (16K and 32K) HD (referred to as the eToken PRO) from Aladdin. This security policy describes how the eToken PRO meets the security requirements of FIPS 140-1, and how to operate the eToken PRO in a secure FIPS mode of operation. This policy was prepared as part of the Level 2 FIPS 140-1 validation of the eToken PRO and Level 3 FIPS 140-1 validation of the eToken PRO HD.

FIPS 140-1 (Federal Information Processing Standards Publication 140-1 — *Security Requirements for Cryptographic Modules*) details the U.S. and Canadian Government requirements for cryptographic modules. More information about the FIPS 140-1 standard and validation program is available on the NIST website at http://csrc.nist.gov/cryptval/.

1.2 References

The Aladdin website contains information on the full line of products at http://www.ealaddin.com/. The eToken PRO product description can be found at: http://www.ealaddin.com/etoken/PRO/default.asp?cf=tl.

1.3 Document Organization

The Security Policy document is one document in a complete FIPS 140-1 Submission Package. In addition to this document, the complete Submission Package contains:

- Vendor Evidence document
- Finite State Machine
- Module Software Listing
- Other supporting documentation as additional references

This Security Policy and other Validation Submission Documentation was produced by Corsec Security, Inc. under contract to Aladdin. With the exception of this Non-Proprietary Security Policy, the FIPS 140-1 Validation Submission Documentation is Aladdin-proprietary and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Aladdin.

1.4 Acronyms and Definitions

Term	Meaning
AC	Access Condition.
API	Application Programming Interface.
AUTH objects	Symmetric and asymmetric keys used for authentication. One of the four Basic Security (BS) object types.
BS objects	Basic Security objects.
CHV	Card Holder Verification.
Cryptoki	Cryptographic token interface. See PKCS#11.
CSE	Current Security Environment.
CSP	Critical Security Parameter.
DES	Data Encryption Standard.
3DES	Triple-DES: Enhanced encryption algorithm based on DES.
DF	Directory File. This is similar to a directory and contains other files.
EF	Elementary File: a regular binary file that contains data, or in the eToken PRO file system, fixed-length records.
eToken PRO	A secure computing and storage device capable of asymmetric key operations.
MAC	Message Authentication Coding.
PIN TEST objects	TEST objects which store operator passwords, and are used for operator authentication.
PKCS#11	PKCS (Public-Key Cryptography System or Cryptoki): API proposed by RSA Labs, which presents a “virtual token” for applications, and management functions to locate and manipulate cryptographic tokens.
PKI	Public Key Infrastructure
PSO objects	Symmetric and asymmetric keys used for general purpose cryptography. One of the four Basic Security (BS) object types.
SE objects	Security environment objects. An SE object is loaded prior to any cryptographic activity and constitutes the current security environment (CSE). It specifies which BS objects will be used for a given cryptographic operation.
SECI	Security Environment Control Information.
SM	Secure Messaging: The ability to protect and/or authenticate traffic between CardOS/M4 and the host, using symmetric DES or 3DES keys in the format of SM BS objects.
SM objects	Symmetric keys used for secure messaging. One of the four Basic Security (BS) object types.
TEST objects	The only objects that can affect the security status of a DF-tree. One of the four Basic Security (BS) object types.
USB	Universal Serial Bus
VPN	Virtual Private Network

2 Aladdin's eToken PRO

The eToken is a fully portable USB device the size of an average house key which offers a cost-effective method for authenticating users when accessing a network and for securing electronic business applications. The eToken PRO is only one of four lines in the eToken family that offers security needs such as secure network logon, secure VPN's, secure email, and strong PKI support.

The eToken PRO offers strong authentication and non-repudiation for sensitive applications such as e-banking, stock trading, ecommerce and financial transactions.

The eToken PRO's secure, on-board RSA 1024-bit key operations enable seamless integration into Public Key Infrastructure (PKI) architectures. The eToken can store users' personal credentials, such as private keys, passwords and digital certificates, inside the protected environment of the Smartcard chip itself. Private keys never leave the token.

The eToken PRO support the following features:

- On-board RSA 1024-bit authentication & digital signing.
- Highly secure, logical & physical smartcard level security, ITSEC E4 certified processor.
- Standard Crypto API connectivity (PKCS#11).
- Secure storage and robust file system.
- Tamper-evident and water-resistant shell. Hardened (HD) versions offer additional physical security (compliant with FIPS 140-1 Level 3 requirements).
- Robust plug-and-play connectivity to mainstream PKI and security clients.
- Standard USB interface.

2.1 Cryptographic Modules

The eToken PRO is a USB device, incorporating a secure USB Micro controller and an off-the-shelf smartcard chip to form a secure computing and storage device capable of symmetric and asymmetric key operations. The eToken PRO offers identity-based authentication using securely entered passwords and advanced cryptographic technology. All authentication objects stored within the eToken PRO memory are physically and logically protected, can only be created and accessed by authorized users, and cannot be read by any operator of the eToken PRO. Cryptographic keys cannot be read under any circumstances, and can only be referenced by applications within the secure environment of the eToken itself.

The eToken PRO has been tested for conformance to both level 2 and level 3 physical requirements. The plastic shell is available in both transparent and opaque constructions, but for FIPS 140-1 compliance, only the opaque token shall be used. The Level 3 module's internal components are additionally encapsulated within a hard, opaque epoxy shell.

The rigid outer casing fully encloses the module establishing the cryptographic boundary; all the functionality discussed in this document is provided by components within the casing. The tokens can be ordered with 16K and 32K bytes of memory.

2.2 Module Interfaces

The eToken PRO provides a single, industry standard USB Type A interface, ensuring all communications securely flow through a single port. This port is the physical interface that is used for data input, data output, control input, and status output. A single LED indicates whether the module is transmitting data, or in the powered on/off state.

Physical Port	FIPS 140-1 Logical Interface
USB Port	Data Input Interface
USB Port	Data Output Interface
USB Port	Control Input Interface
USB Port	Status Output Interface

Table 1 – FIPS 140-1 Logical Interfaces

The following table list the visible status output information conveyed provided by the LED on the eToken PRO.

LED	Indicator	Description
Power Indicator	Red	Power is supplied to the eToken and the eToken is operational
	Blinking Red	Data is being transmitted
	Off	The eToken is not powered on

Table 2 – LED Description

2.3 Roles and Services

The eToken PRO supports identity-based authentication and authenticates operators using passwords. There are two distinct roles that operators may assume: Crypto Officer role and User role. The Crypto Officer role has the ability to configure, initialize and administer the token. The Crypto Officer role corresponds to the Administration phase of the eToken PRO. Crypto Officer role-only services include the use of the CREATE_FILE, DELETE_FILE, and PUT_DATA commands.

2.3.1 Crypto Officer Services

The Crypto Officer role is responsible for the following services:

- Initializing and formatting of the token (using PUT_DATA)
- Administration of eToken Passwords (using PUT_DATA)
- Delete Files and Folders (using DELETE_FILE)
- Change the Display
- Create Binary Files (using CREATE_FILE)

- Read Public and Private Data
- Write Public and Private Data
- Administer Files and Objects (using PUT_DATA)
- Reset security status of the current Directory File

Refer to the website http://www.ealaddin.com/etoken/pro/default.asp?cf=tl and the Developer's Guide for more details.

2.3.2 User Services

The User role corresponds to the Operational phase of the eToken PRO. The User role is responsible for the following services:

- Start the eToken Editor
- Change the eToken User Password
- Change the Display
- Read Public and Private Data
- Write Public and Private Data
- Reset security status of the current Directory File

Refer Submission Document 6A for more details. A complete listing of services available to each role, and the objects affected is shown in Section 4.

2.4 Identification and Authentication (I&A)

When configured in the FIPS mode, the token enforces identity-based authentication of operators using passwords. After initialization, operators use the VERIFY command to authenticate for access to files and commands within the token. The operator must enter the correct password, along with an ID that uniquely references the test object used to verify the password. Once successfully authenticated, the operator has access to all private objects (files and keys) whose access definitions include that specific test object. While the eToken PRO supports creation of multiple PIN Test Objects and thus multiple operators (although not concurrently), the typical configuration includes only two sets of PIN Test Objects defined for two operators.

All transactions with the token (including sending a password using the VERIFY command for authentication) are communicated using Secure Messaging (SM) communications for encryption of the information transferred. SM Encryption (SM_ENC) is performed using DES or 3DES (using the token's SM Mode xCh with SM_ENC) using SM DES/3DES keys initialized by the Crypto Officer. For more information on the initialization of the eToken PRO in FIPS mode, see Section 3.

Each operator authenticating to the User or Crypto Officer roles has a password that is used with the VERIFY command to authenticate the operator. When configured in FIPS mode there are four passwords created: one User-role password, and three Crypto Officer-role passwords (two lifecycle passwords, and one administration token password). The four passwords can be deployed among one or more operators according to an organization's needs; one possible configuration is discussed in the following paragraph.

Two lifecycle passwords allow two separate operators to authenticate as the Crypto Officer to share in managing initialization and configuration of the token. One operator of the token (the end user) can thus possess one lifecycle password and the User-role password, while the other operator (the provider) can possess only Crypto Officer role passwords (a lifecycle password and the administration token password).

The Administration token password allows the Crypto Officer role to Format an initialized token (using DELETE FILE for re-initialization or destruction), or to unblock the User-role password. The passwords (also referred to as a PINs) can contain any value (ASCII or hexadecimal), and can be changed (after successful authentication). Failed user authentication attempts to authenticate are counted, and after enough unsuccessful attempts, User access is blocked. The number of unsuccessful attempts is configurable by the Crypto Officer to be from one to fifteen. Successful login will reset the unsuccessful attempt count, or the Crypto Officer can manually reset the count with the RESET RETRY COUNTER command.

An operator can log out of the token using the RESET SECURITY STATUS command.

2.5 Physical Security

The eToken PRO offers multiple physical enclosures for the module. Two versions of the module's case were tested against FIPS 140-1 physical security Level 2 and Level 3 to meet FIPS requirements. Additionally, two separate memory configurations were tested against all other FIPS 140-1 Level 3 security requirements.

Product Name	Memory Size	Version	Physical Security Level
eToken PRO 16k	16k	4.1.5.4	2
eToken PRO 32k	32k	4.2.5.4	2
eToken PRO 16k HD	16k	4.1.5.4.HD	3
eToken PRO 32k HD	32k	4.2.5.4.HD	3

Table 3 – eToken PRO Versions

The level 2 compliant case (for the eToken PRO 16k and eToken PRO 32k) is made of a one piece, polycarbonate shell. The module is covered by a hard plastic, opaque tamper-evident casing and comes in multiple opaque color options. The only component exposed from the module is the USB port connector. The operator should regularly inspect the token for signs of tampering, which include deep scratches on the surface, cracks, and any physical damage to the appearance of the module, especially around the connector area.

Physical Security Level 3 modules (the eToken PRO 16 k HD and eToken PRO 32 k HD) have the internal components covered with a one piece hardened solid epoxy, preventing attempts to physically access the components or internal critical signals. The Level 3 module is also covered by a hard plastic, opaque tamper-evident casing and comes in the same color options. The only components exposed from the epoxy are the USB port and the LED. Signs of tampering include deep scratches on the surface, cracks, and any physical damage to the appearance of the module.

Neither version of the module contains any removable covers or doors.

2.6 Cryptographic Key Management

The module eToken PRO is a general-purpose cryptographic token designed to store and utilize keys for a user. All objects (keys and passwords) exist in the token as Basic Security (BS) Objects. Public BS Objects can be read (but not changed) by all token users, while private BS Objects can only be accessed by an authorized user (the password is used as an access mechanism). Objects can be zeroized individually using CHANGE_REFERENCE_DATA or PUT DATA_OCI, or as an entire file using DELETE_FILE – see Section 4.

The keys can be stored for RSA PKCS#1 digital signatures/verification (using SHA-1), RSA encryption/decryption (not FIPS-approved), DES encryption and decryption (ECB and CBC modes, as well as DES MAC), and Triple DES encryption and decryption (CBC mode, as well as 3DES-MAC). The following is a listing of the types of key objects in the module.

Table 4 - Key BS Objects

Key	Description
PSO Objects	Symmetric (DES or 3DES) and Asymmetric keypairs (RSA) used for general purpose cryptography
SM Objects	Symmetric keys (DES or 3DES) used for secure messaging between the token and the host computer. 3DES is recommended.
Auth Objects	Symmetric (DES or 3DES) and Asymmetric keypairs (RSA) used for token authentication to the host

For more information on the creation and use of PSO, SM, and Auth objects please refer to the eToken PRO Developer's Guide.

In addition to the key BS Objects listed in Table 4, other Critical Security Parameters (CSPs) contained within the eToken PRO include:

- PIN Test Object(s) storing the lifecycle password(s)
- PIN Test Object storing the Administrator password
- PIN Test Object(s) storing the User password(s)

Section 3.2 shows how PIN Test Objects and other BS Objects are used in the initialization of the module.

2.7 Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC)

The module has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC rules. Thus the module meets FCC requirements in 47 CFR Part 15 for personal computers and peripherals designated for Home use (Class B). As required by FIPS 140-1 level 3 requirements, the module was tested and then verified in the test report as meeting these FCC requirements. The module and its accompanying documentation is labeled in accordance with FCC requirements with the appropriate FCC warnings.

2.8 Self-Tests

The module implements a series of power-up self-tests during the power-up process of USB token insertion. The self-tests include cryptographic known answer tests (KAT) on the FIPS-approved cryptographic algorithms (DES, 3DES, RSA) and on the message digest algorithm (SHA-1). In addition to the cryptographic algorithm test and the software/firmware test, critical functions tests are executed to see if the USB interface and the internal processor have been initialized correctly. Tests may be initiated at any time by removing the module from the USB port and re-inserting it.

3 FIPS-compliant Operation of the Aladdin eToken PRO

FIPS-validated Aladdin eToken PRO modules meet all Level 2 and many Level 3 FIPS 140-1 requirements. FIPS-validated Aladdin eToken PRO HD modules meet all Level 3 FIPS140-1 requirements. See the FIPS 140-1 validation certificates for details.

Follow the instructions below to ensure that the module is operating securely in FIPS mode.

3.1 Selection of Algorithms

The following algorithms are FIPS approved and may be used with the token:

- DES and DES MAC (DES permitted for legacy systems only)
- 3DES and 3DES MAC
- SHA-1
- RSA signing/verification (with SHA-1)

Although the eToken PRO uses RSA PKCS#1, RSA is only FIPS-approved for Digital Signatures. The use of RSA for encryption/decryption is not FIPS-approved.

3.2 System Initialization and Configuration

Module initialization in FIPS mode is performed by a Crypto Officer during the personalization of tokens before delivery to Users. Crypto Officers can use the Aladdin-provided eToken format utilities to automatically configure the token in FIPS mode, or can use their own manual or automated configuration. When using the Aladdin-provided eToken format utility, the CryptoOfficer need only set the passwords, and set the maximum number of allowed login retries (MaxErrorCounter). When not using the Aladdin eToken format utilities, the following changes are required to operate the module in FIPS mode and must be performed by a CryptoOfficer:

- Optionally enable SM mode x4h to encrypt initialization and personalization commands
  - In the main directory on the token (3f00), create the following objects
    - life cycle pin test (lcTest)
    - life cycle pin test secure messaging DES/3DES key (lcSM)
    - life cycle administrator pin test (lcaTest)
    - life cycle administrator pin test secure messaging DES/3DES key (lcaSM)
    - life cycle logical test (lcLogical (lcaTest || lcTest))
    - Set the Access Control to AC.lcycle = lcLogical (all other conditions 0)
  - Create the Aladdin directory on the token (3f00/6666), with the following objects
    - user pin test (uTest) (Contains the User password)
    - user pin test secure messaging DES/3DESdes key (uSM)
    - administrator pin test (aTest) (Contains the Administrator password)
    - administrator pin test secure messaging DES/3DES key (aSM)
    - Set the following properties for Access Control
      - AC.Lcycle = never
      - AC.update = aTest

        - AC.append = uTest
        - AC.deactivate = never
        - AC.reactivate = never
        - AC.del = never
        - AC.admin = never
        - AC.create = uTest
    - Create BSObjects to hold self-test keys
    - Set all MaxErrorCounter to a value from 1 to 15.
- Change the Lifecycle phase from Administration to Operational (Crypto Officer role to User role) using PHASE CONTROL.

3.3 Secure Operation

The User password should be given to the User who must secure it for access to the token. If a default password is used by the Crypto Officer (for token initialization), the User should update the default password immediately.

The User must also periodically inspect the module for tamper evidence and physical damage. If the User loses control of the token for any period of time, the casing should be inspected for tampering. See section 2.4 of this document for details on physical tamper signs.

After initial configuration, the module is delivered to the User in Operational mode. The Crypto Officer has the ability to change the module life cycle back to Administration mode and reconfigure the token, and add new BS Objects as required.

FIPS-compliant operation should include the enabling of Secure Messaging (use of 3DES recommended) and Access Control mechanisms as described above for the input of all BS Objects, including PIN Test Objects. Once the token is initialized, new SM keys should be immediately uploaded to replace the default SM keys, prior to the uploading of PSO BS Objects.

4 Services of the eToken PRO

Table 5 below provides a listing of all the services offered by the FIPS-compliant version of the eToken PRO, what role can invoke each service, and the CSPs are directly affected by each service. Complete details on the token commands can be found in the eToken PRO Developer's Guide, available on the Aladdin website.

Table 5 - Services of the eToken PRO

Command	Description	Available in Administration State (CO role)	Available in Operational State (User role)	CSPs Directly Affected
ACTIVATE_FILE	Reactivates the current file or file tree.	Y	Y	N/A
APPEND_RECORD	Creates a new record in the current EF (Elementary File).	Y	Y	N/A
CHANGE_REFERENCE_DATA*	Changes the data of a TEST PIN object (password).	Y	Y	TEST PIN BS Object
CREATE_FILE	Creates a file.	Y	NO	N/A
DEACTIVATE_FILE	Deactivates a file or file tree.	Y	Y	N/A
DECREASE	Decreases the value of the first record of a *CYCLIC FIXED* file.	Y	Y	N/A
DELETE_FILE	Deletes a file and all objects within the file.	Y**	NO	Any object in the file
DIRECTORY	Reads directory and file information of DFs (Directory Files) and EFs directly below the current DF.	Y	Y	N/A
GET_DATA	Reads system information.	Y	Y	N/A
GIVE RANDOM	Inputs an external random number to the token	Y	Y	N/A
INCREASE	Increases the value of the current record of a *CYCLIC FIXED* file.	Y	Y	N/A
INTERNAL_AUTHENTICATE*	Authenticates a card to the host.	Y	Y	Auth BS Objects
MSE (MANAGE SECURITY ENVIRONMENT)	Loads a *CSE (Current Security Environment)* or sets a component of the *CSE*.	Y	Y	N/A
PHASE CONTROL	Changes from role *ADMINISTRATION* to *OPERATIONAL* and vice versa.	Y	Y	N/A
PSO (PERFORM SECURITY OPERATION)	Performs a cryptographic operation. Each PSO mode performs a different operation, as shown below:	Y	Y	See below
PSO_CCC	COMPUTE CRYPTOGRAPHIC CHECKSUM (MAC)	Y	Y	DES/3DES BS Objects
PSO_CDS	COMPUTE DIGITAL SIGNATURE	Y	Y	RSA BS Objects
PSO_DEC	DECIPHER	Y	Y	DES/3DES BS Objects
PSO_ENC	ENCIPHER	Y	Y	DES/3DES

				BS Objects
PSO_H	HASHING	Y	Y	N/A
PSO_VCC	VERIFY CRYPTOGRAPHIC CHECKSUM	Y	Y	DES/3DES BS Objects
PSO_VDS	VERIFY DIGITAL SIGNATURE	Y	Y	RSA BS Objects
PUT DATA	Installs / administers files and objects. Each PUT DATA mode performs a different function, as shown below:	Y	NO	See below
PUT DATA_FCI	Administers file attributes via FCIs (File Control Information).	Y	NO	N/A
PUT DATA_OCI*	Installs / administers BS objects in the current DF.	Y	NO	BS Objects
PUT_DATA_SECI	Installs / administers SE objects.	Y	NO	N/A
READ BINARY	Reads a binary file.	Y	Y	N/A
READ RECORD	Reads a record from a *LINEAR FIXED, CYCLIC FIXED* or *LINEAR TLV* file.	Y	Y	N/A
RESET_RETRY_COUNTER	Resets the error counter of a BS Object (e.g. a PIN TEST Object) to the defined maximum.	Y**	N	BS Objects
RESET_SECURITY_STATE	Resets the security status of the current DF.	Y	Y	N/A
SELECT FILE	Selects a file.	Y	Y	N/A
UPDATE BINARY	Updates a *BINARY* file.	Y	Y	N/A
UPDATE_RECORD	Overwrites an existing record.	Y	Y	N/A
VERIFY*	Performs a CHV (card holder verification) PIN test to login to the module	Y	Y	Test PIN Objects

* These commands import BS Objects from the host to the module. To remain FIPS-compliant, Secure Messaging using the appropriate SM BS Objects must be activated when invoking these commands.

** Crypto Officer must use the Administration token password