

**Aladdin Knowledge Systems, Ltd.
eToken PRO, eToken PRO HD, eToken NG-OTP, and
eToken NG-FLASH (128 MB, 512 MB, and 1 GB)
(PCB Hardware version: PRO/PRO HD 4.28, NG-OTP 2.25,
NG-FLASH 4.27; Operating System version: CardOS 4.2B)**




**FIPS 140-2
Non-Proprietary Security Policy**

Level 2 and 3 Validations

Document Version 1.0

Prepared for:


Aladdin[®]
SECURING THE GLOBAL VILLAGE
Aladdin Knowledge Systems, Ltd.
35 Efal St.,
Kiryat Arye,
Petach Tikva, Israel 49511
Phone: (972) 3-978-1111
Fax: (972) 3-978-1010
<http://aladdin.com/>

Prepared by:


Corsec[®]
Corsec Security, Inc.
10340 Democracy Lane, Suite 201
Fairfax, VA 22030
Phone: (703) 267-6050
Fax: (703) 267-6810
<http://www.corsec.com>

Revision History

Version	Modification Date	Modified By	Description of Changes
1.0	2007-10-1	Xiaoyu Ruan	Release version

Table of Contents

- 0 INTRODUCTION6**
 - 0.1 PURPOSE.....6
 - 0.2 REFERENCES.....6
 - 0.3 DOCUMENT ORGANIZATION6
- 1 ETOKEN PRO, ETOKEN PRO HD, ETOKEN NG-OTP, AND ETOKEN NG-FLASH.....7**
 - 1.1 OVERVIEW.....7
 - 1.2 MODULE INTERFACES.....9
 - 1.3 ROLES AND SERVICES.....10
 - 1.3.1 *Provider’s Role*.....10
 - 1.3.2 *Crypto-Officer Role*11
 - 1.3.3 *User Role*12
 - 1.3.4 *Authentication*.....13
 - 1.4 PHYSICAL SECURITY13
 - 1.5 OPERATIONAL ENVIRONMENT.....13
 - 1.6 CRYPTOGRAPHIC KEY MANAGEMENT.....13
 - 1.6.1 *Key Generation and Entry*14
 - 1.6.2 *Key Output*.....15
 - 1.6.3 *Key Storage and Zeroization*15
 - 1.7 SELF-TESTS15
 - 1.8 MITIGATION OF OTHER ATTACKS.....16
- 2 SECURE OPERATION.....17**
 - 2.1 PROVIDER ROLE GUIDANCE17
 - 2.2 CRYPTO-OFFICER ROLE GUIDANCE.....17
 - 2.2.1 *Initialization and Management*.....17
 - 2.3 USER ROLE GUIDANCE.....18
- 3 ACRONYMS.....19**

Table of Figures

FIGURE 1 - eTOKEN PRODUCT OFFERING	7
FIGURE 2 - eTOKEN PRO/PRO HD (PCB VERSION 4.28)	8
FIGURE 3 - eTOKEN NG-OTP (PCB VERSION 2.25).....	8
FIGURE 4 - eTOKEN NG-FLASH (PCB VERSION 4.27).....	8
FIGURE 5 - eTOKEN PROPERTIES WINDOW	17

Table of Tables

TABLE 1 - SECURITY LEVEL PER FIPS 140-2 SECTION	9
TABLE 2 - FIPS 140-2 LOGICAL INTERFACES	9
TABLE 3 - MAPPING OF PROVIDER’S SERVICES TO INPUTS, OUTPUTS, CSPs, AND TYPE OF ACCESS.....	10
TABLE 4 - MAPPING OF CRYPTO-OFFICER SERVICES TO INPUTS, OUTPUTS, CSPs, AND TYPE OF ACCESS	11
TABLE 5 - MAPPING OF CRYPTO-OFFICER AND USER ROLE’S SERVICES TO INPUTS, OUTPUTS, CSPs, AND TYPE OF ACCESS	12
TABLE 6 - LIST OF CRYPTOGRAPHIC KEYS, CRYPTOGRAPHIC KEY COMPONENTS, AND CSPs	14
TABLE 7 - ACRONYMS	19

0 Introduction

0.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the eToken PRO (PCB version 4.28), eToken PRO HD (PCB version 4.28), eToken NG-OTP (PCB version 2.25), and eToken NG-FLASH (PCB version 4.27, storage capability 128 MB, 512 MB, and 1 GB) from Aladdin Knowledge Systems, Ltd. All models use Aladdin firmware version 2.7 which runs on the CardOS 4.2B Operating System. This Security Policy describes how the eToken PRO, eToken PRO HD, eToken NG-OTP, and eToken NG-FLASH meet the security requirements of FIPS 140-2 and how to run the module in a secure FIPS 140-2 mode. This policy was prepared as part of the Level 2 and 3 FIPS 140-2 validations of the modules. Notice that PCB stands for Printed Circuit Board.

FIPS 140-2 (Federal Information Processing Standards Publication 140-2 – *Security Requirements for Cryptographic Modules*) details the U.S. Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP) website at: <http://csrc.nist.gov/cryptval/>

The eToken PRO, eToken PRO HD, eToken NG-OTP, and eToken NG-FLASH are referred to in this document as the eTokens, the cryptographic modules, or the modules.

0.2 References

This document deals only with operations and capabilities of the module in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the module from the following sources:

- The Aladdin website (<http://www.aladdin.com/>) contains information on the full line of products from Aladdin.
- The CMVP website (<http://csrc.nist.gov/cryptval/>) contains contact information for answers to technical or sales-related questions for the module.

0.3 Document Organization

The Security Policy document is one document in a FIPS 140-2 Submission Package. In addition to this document, the Submission Package contains:

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

This Security Policy and the other validation submission documentation were produced by Corsec Security, Inc. under contract to Aladdin. With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Validation Documentation is proprietary to Aladdin and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Aladdin.

1 eToken PRO, eToken PRO HD, eToken NG-OTP, and eToken NG-FLASH

1.1 Overview

The eToken product offering provides a robust and flexible framework for integration with many of today's leading security solutions, providing a solution for strong authentication and password management needs. The eToken provides a complete set of easy-to-use password management applications with it that enable the user to securely store and manage all of their logon credentials on a single eToken device. Users no longer need to remember numerous passwords for all of their applications and accounts - just the single eToken password.

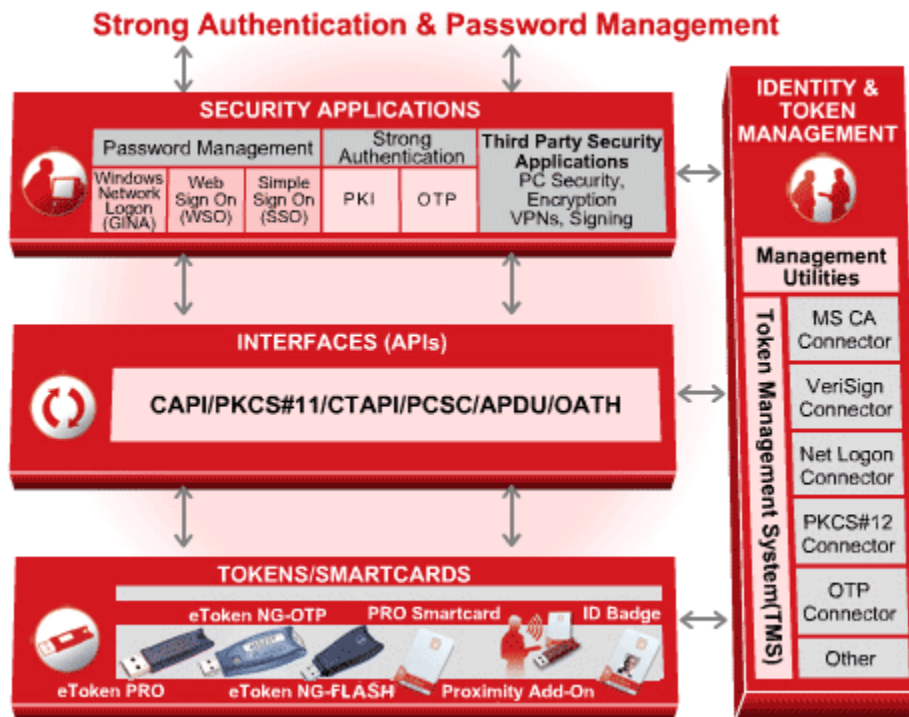


Figure 1 - eToken Product Offering

The eToken works with a variety of third-party applications from leading security companies, providing eToken security in the following areas and more:

- Boot protection
- Disk & file/folder encryption
- Public Key Infrastructure (PKI)
- Email protection
- Single sign-on
- Virtual Private Network (VPN) remote access
- Web & web-based remote access
- Network/workstation logon



Figure 2 - eToken PRO/PRO HD (PCB version 4.28)

The eToken PRO and eToken PRO HD's secure, on-board RSA 1024-bit and 2048-bit key operations enable seamless integration into Public Key Infrastructure (PKI) architectures. The eToken PRO and eToken PRO HD can generate and store users' personal credentials, such as private keys, passwords and digital certificates, inside the protected environment of the smartcard chip itself. Users' private keys never leave the module. The eToken PRO and eToken PRO HD USB devices offer both two-factor and two-way authentication, using advanced cryptographic smartcard technology.



Figure 3 - eToken NG-OTP (PCB version 2.25)

The Aladdin eToken NG-OTP is a hybrid Universal Serial Bus (USB) and One-Time Password (OTP) eToken. The eToken combines the full functionality of the smartcard technology - including PKI encryption and digital signing, secure credential storage, and more - with OTP technology for strong user authentication to network resources in detached mode.



Figure 4 - eToken NG-FLASH (PCB version 4.27)

The Aladdin eToken NG-FLASH provides complete secure access and a portable data storage solution in a single token. The eToken NG-FLASH combines the high security of a smartcard based USB authentication device with the benefits of flash memory. It enables secure access to networks and applications, secure online transactions, data encryption, Personal Computer (PC) boot protection, secure credential storage, mobile mass data storage, and more – all in one compact USB token.

The eToken PRO, eToken PRO HD, eToken NG-OTP, and eToken NG-FLASH are validated at the following FIPS 140-2 Section levels:

Table 1 - Security Level Per FIPS 140-2 Section

Section	Section Title	Level for eToken PRO 4.28 (32K and 64K)	Level for eToken PRO HD 4.28 (32K and 64K)	Level for eToken NG-OTP 2.25 (32K and 64K)	Level for eToken NG-FLASH 4.27 (32K)
1	Cryptographic Module Specification	3	3	3	3
2	Cryptographic Module Ports and Interfaces	2	3	2	2
3	Roles, Services, and Authentication	3	3	3	3
4	Finite State Model	2	3	2	2
5	Physical Security	2	3	2	2
6	Operational Environment	N/A	N/A	N/A	N/A
7	Cryptographic Key Management	2	3	2	2
8	Electromagnetic Interference (EMI) / Electromagnetic Compatibility (EMC)	3	3	3	3
9	Self-Tests	2	3	2	2
10	Design Assurance	3	3	3	3
11	Mitigation of Other Attacks	N/A	N/A	N/A	N/A

1.2 Module Interfaces

The eToken PRO, eToken PRO HD, eToken NG-OTP, and eToken NG-FLASH are multi-chip standalone modules. The cryptographic boundaries of the eToken PRO, eToken PRO HD, eToken NG-OTP, and eToken NG-FLASH are defined by their hard, opaque, tamper-evident cases.

Data input and output utilizing the authentication functionalities of the modules enter and exit the modules through the USB port. The eToken NG-OTP has a Liquid Crystal Display (LCD) screen which is used to display data. Control input consists of all the input that is entered into the modules by a Crypto-Officer via the USB port. The button on the eToken NG-OTP is also a control input which is used to start calculating OTP data. The Light Emitting Diodes (LEDs) are used to display the status of the device. Operating power for the cryptographic modules is also provided by the USB port.

All of these physical interfaces are separated into logical interfaces defined by FIPS 140-2, as described in the following table:

Table 2 - FIPS 140-2 Logical Interfaces

FIPS 140-2 Logical Interface	eToken PRO, eToken PRO HD, eToken NG-OTP, and eToken NG-FLASH Port/Interface
Data Input	USB
Data Output	USB, LCD (eToken NG-OTP only)
Control Input	USB, Button (eToken NG-OTP only)
Status Output	USB, LED
Power	USB

1.3 Roles and Services

The module supports identity-based authentication. There are three roles in the module that operators may assume: a Provider Role, a Crypto-Officer role, and a User role.

1.3.1 Provider’s Role

The Provider initializes the module by issuing the INITIALIZE EEPROM and PERSONALIZE commands. With these commands the StartKey and PackageLoadKey are loaded into the module. At this phase of the lifecycle, the Provider installs the certificate for the root Certificate Authority (CA) into the module and a RSA key pair is generated by the module. The module is then initialized into the FIPS mode of operation and functionalities are enabled for licensed packages. A package can be either licensed or non-licensed packages. A licensed package must also be loaded and activated with the PackageLoadKey, but its functionality will not be available, because the package is still disabled. In order to enable the loaded and activated but disabled package, the package must first be enabled via the ENABLE PACKAGE command. The fact that a specific package is a licensed or non-licensed is maintained in the CardOS V4.2B Packages and Release Notes.

The Provider role is not authenticated because the operation is done in a factory environment and the module is not ready to provide any services. Descriptions of the services available to the Provider role are provided in the Table 3 with all Critical Security Parameters (CSPs) and associated access controls. Provider inputs command with appropriate parameters to access the services of the module and the module outputs the command response.

Table 3 - Mapping of Provider’s Services to Inputs, Outputs, CSPs, and Type of Access

Service	Description	CSP and Type of Access
ALLOCATE TRANSACTION BUFFER	Allocates or frees a transaction buffer	None
CARD AUTHENTICATE	Checks a card’s authenticity before personalization takes place.	None
CHANGE SYSTEM KEY	Replaces a system key.	StartKey –Write
CREATE FILE	Creates a child-file of the current Dedicated File (DF).	None
DELETE FILE	Deletes the file referenced by the File_ID.	None
ENABLE PACKAGE	Enables an already loaded and activated but still disabled license package, whose functionality is not yet available.	PackageLoadKey – Read
ERASE FILES	Erases the following areas in Electronically Erasable Programmable Read-Only Memory (EEPROM): The file system, any existing system or application package(s), and any existing application descriptors.	None
FORMAT	Changes the life cycle phase.	None
GENERATE KEY PAIR	Creates a public key pair.	RSA Key pair – Write
INITIALIZE EEPROM	Loads the following data to the EEPROM area: file system structures, data structures, application descriptors, placeholders, possibly file data, and possibly data of system packages.	StartKey – Write
INITIALIZE END	Finalizes the life cycle phase, internal to the factory environment.	None
LOAD EXECUTABLE	Activates a system package or an application package.	PackageLoadKey – Read
PERSONALIZE	Plugs in the real data in the placeholders.	None
PHASE CONTROL	Changes the global life cycle phase of the module.	None

Service	Description	CSP and Type of Access
PUT DATA	Writes data	None
UNINSTALL PACKAGE	Removes the package with the specified Package_ID from the module.	None

1.3.2 Crypto-Officer Role

The Crypto-Officer is responsible for creating, updating, and managing user accounts. The Crypto-Officer authenticates during session establishment using a Triple Data Encryption Standard (TDES) Message Authentication Code (MAC). Descriptions of the services available to the Crypto-Officer are provided in Table 4 and Table 5. The Crypto-Officer inputs command with appropriate parameters to access the services of the module and the module outputs the command response.

In CardOS 4.2B, two categories, DF and EF (Elementary File), are implemented. EFs may be of the following types: LINEAR FIXED, CYCLIC FIXED, LINEAR TLV, BINARY, and CODE. The Secure Messaging Keys refer to two keys: Secure Messaging Encryption Key and Secure Messaging MAC Key. Both keys are 2-key TDES symmetric keys. Please see Table 6 for details.

Table 4 - Mapping of Crypto-Officer Services to Inputs, Outputs, CSPs, and Type of Access

Command	Description	CSP and Access Type
ACTIVATE FILE	Reactivates the current file in the file system.	Secure Messaging Keys – Read
APPEND RECORD	Creates a new record in the currently selected file.	Secure Messaging Keys – Read
CHANGE KEY DATA	Replaces the object data.	Secure Messaging Keys – Read/Write
DEACTIVATE FILE	Deactivates the current file inside the file system of CardOS V4.2B.	Secure Messaging Keys – Read
DECREASE	Decreases the value of the first record of a CYCLIC FIXED file by the Sub_Value. For CYCLIC FIXED file reference system record which was written in APPEND mode last, is the logically first record.	Secure Messaging Keys – Read
DIRECTORY	Returns information about files.	Secure Messaging Keys – Read
INCREASE	Increases the value of the current record of a CYCLIC FIXED file by the Add_Value.	Secure Messaging Keys – Read
MANAGE CHANNEL	Opens or closes an additional logical channel to the module.	Secure Messaging Keys – Read
MANAGE SECURITY ENVIRONMENT (MSE)	Loads Current Security Environment (CSE).	Secure Messaging Keys – Read
PERFORM TRANSACTION OPERATION	Start or stop protection mechanism.	Secure Messaging Keys – Read
PSO (PERFORM SECURITY OPERATION)	Performs cryptographic operations	Secure Messaging Keys – Read RSA Private Key – Read TDES MAC Key – Read
READ BINARY	Reads data from a BINARY file.	Secure Messaging Keys – Read
READ RECORD	Reads a record from a LINEAR FIXED, CYCLIC FIXED or LINEAR TLV file.	Secure Messaging Keys – Read
RESET RETRY COUNTER	Sets the current error counter. This is a retry counter for object entry.	Secure Messaging Keys – Read

Command	Description	CSP and Access Type
RESET SECURITY STATUS	Resets the security status of the current DF or in the Master File (MF).	Secure Messaging Keys – Read
SET DATA FIELD LENGTH	Sets the length of the Data_Field_Length parameter.	Secure Messaging Keys – Read
SET TRANSACTION STATE	Logs all EEPROM contents, which will be affected by a command with the Setting AutoTR=ON.	Secure Messaging Keys – Read
UPDATE BINARY	Writes the Binary_Data of the command data field into a BINARY file.	Secure Messaging Keys – Read
UPDATE RECORD	Writes the Record_Data of the command data field.	Secure Messaging Keys – Read

1.3.3 User Role

Users are the end users that utilize the module’s authentication functionalities only. They have the permission to read and write data from/to the module. Users authenticate during session establishment using TDES MACs. Descriptions of the services available to the Users are provided in the Table 5 below. The services listed in Table 5 are also accessed by the Crypto-Officer role. Services listed in the table below require input commands with appropriate parameters from the operator and the module outputs the command response.

Table 5 - Mapping of Crypto-Officer and User Role’s Services to Inputs, Outputs, CSPs, and Type of Access

Command	Description	CSP and Access Type
CHANGE KEY DATA	Replaces the object data.	Secure Messaging Keys – Read RSA private key – Write
CHANGE REFERENCE DATA	Replaces the object data of the PIN TEST object.	Secure Messaging Keys – Read
EXTERNAL AUTHENTICATE	Performs a challenge/response test.	Secure Messaging Keys – Read
GET CHALLENGE	Generates the internal random number.	Secure Messaging Keys – Read
GET DATA	Supplies information on the current status of the system. MODE specifies the information to be returned.	Secure Messaging Keys – Read
GIVE RANDOM	Transmits an external random number.	Secure Messaging Keys – Read
INTERNAL AUTHENTICATE	Performs a MAC calculation.	Secure Messaging Keys – Read Authentication Key – Read
SELECT FILE	Selects a file via its file ID.	Secure Messaging Keys – Read
SIGN BY DECRYPTION KEY	Creates a RSA signature of the input data.	Secure Messaging Keys – Read RSA Private Key – Read
DECRYPT BY DECRYPTION KEY	Decrypts the encrypted symmetric key	Secure Messaging Keys – Read RSA Private Key – Read
VERIFY	Performs PIN verification.	Secure Messaging Keys – Read RSA Public Key – Read
GENERATE ONE-TIME PASSWORD	NG-OTP only. Generate a one-time password with the touch of the button.	None
FLASH STORAGE	NG-FLASH only. Stores user-data in flash memory.	None

1.3.4 Authentication

The module performs identity based authentication for the Crypto-Officer and User using TDES MAC. The module performs authentication using a “TEST” object before providing any services to the Crypto-Officer or User. “TEST” is a special type of object enforcing authentication before access. The TEST object contains an ID for the operator and the corresponding TDES key value.

The authentication uses a 112-bit TDES MAC key. The probability for a random attempt to succeed is $1:2^{112}$. A random attempt has to transmit at least 112 bits of data. On a 25 MHz processor used by the module, up to 1.5×10^9 bits of data can be transmitted between the module and the host in a 60-second period. This is equivalent to at most 13,392,857 attempts. However, there exist 2^{112} possibilities. Therefore, in a 60-second period, the probability of successfully guessing the 128-bit TDES MAC key is $13,392,857/2^{112} = 2.58 \times 10^{-27}$.

1.4 Physical Security

The eToken PRO, eToken PRO HD, eToken NG-OTP, and eToken NG-FLASH are multi-chip standalone cryptographic modules. The cryptographic modules, except the eToken PRO HD, are being validated to level 2. The eToken PRO HD is being validated to level 3. The eToken PRO HD does not contain any ventilation holes or slits that could be subject to undetected physical probing. The eToken PRO HD has a hard opaque epoxy over the PCB. The modules are contained entirely within hard and opaque plastic enclosures, which prevent attackers from accessing the internals of the device without leaving tamper evidence on the enclosure.

1.5 Operational Environment

The operational environment requirements do not apply to the eToken PRO, eToken PRO HD, eToken NG-OTP, and eToken NG-FLASH. The modules' firmware packages run on the CardOS 4.2B, a non-modifiable operating system (OS).

1.6 Cryptographic Key Management

The eTokens implement the following FIPS-approved algorithms. Power-up self-tests are performed on these algorithms.

- SHA-1 – Byte oriented (Cert #627)
- TDES – 2-key (112 bits) and 3-key (168 bits) encrypt/decrypt in the CBC mode (Cert #555)
- RSA (PKCS #1) 1024-bit sign/verify (Cert #256)
- PRNG – ANSI X9.31 Appendix A.2.4 (Cert #325)
- TDES MAC for authentication

The module utilizes the following non-FIPS-approved algorithm implementation. The non-FIPS-approved algorithm is available in the FIPS mode of operation.

- RSA (PKCS #1) 1024-bit decryption (key wrapping; key establishment methodology provides 80 bits of encryption strength)

The module supports the following critical security parameters:

Table 6 - List of Cryptographic Keys, Cryptographic Key Components, and CSPs

Key or CSP	Key Type	Generation / Input	Output	Storage	Zeroization	Use
StartKey	2-key TDES MAC key	Externally generated, entered in plaintext	Never exits the module	Stored in plaintext	By erasing the flash	Ensures integrity of system files during package loading
PackageLoadKey	2-key TDES MAC key	Externally generated, entered in plaintext	Never exits the module	Stored in plaintext	By erasing the flash	Ensures integrity of system files during package loading
Secure Messaging Encryption Key	2-key TDES key	Externally generated, entered in plaintext or encrypted form (encrypted with TDES)	Never exits the module	Stored in plaintext	By command or erasing the flash	Encrypts Application Protocol Data Unit (APDU) data
Secure Messaging MAC Key	2-key TDES key	Externally generated, entered in plaintext or encrypted form (encrypted with TDES)	Never exits the module	Stored in plaintext	By command or erasing the flash	Computes MAC of APDU data
Authentication Key	2-key TDES MAC key	Externally generated, entered in plaintext or encrypted form (encrypted with TDES)	Never exits the module	Stored in plaintext	By command or erasing the flash	Involved in authenticating operators to the module
TDES MAC	64-bit MAC based upon Authentication key	Internally generated	Never exits the module	Stored in plaintext	By command or erasing the flash	Authentication
Session Key	2-key or 3-key TDES key	Externally generated, entered in encrypted form (encrypted with RSA)	Never exits the module	Stored in plaintext	When use is over	Decrypts TDES-encrypted data
RSA Private Key	1024 RSA private key	Internally generated or imported in encrypted form	Never exits the module	Stored in plaintext	By command or erasing the flash	Generates signatures, decrypts Session Keys
PRNG Seed	64-bit PRNG seed	Internally generated	Never exits the module	Stored in plaintext	When new seed is generated	Seeds PRNG

1.6.1 Key Generation and Entry

The StartKey and PackageLoadKey, also referred to as System Keys, are externally generated and entered in the module in plaintext in a factory environment. The System Keys are installed before the module is configured into the FIPS mode of operation. Both of the keys are 2-key TDES keys that are used to ensure integrity using TDES MAC algorithm of the application package during installation.

The Secure Messaging Encryption Key is a 2-key TDES key that encrypts APDU content of a secure session. The Provider installs an externally generated Secure Messaging Encryption Key into the module during initialization. The Secure Messaging Encryption Key can be updated with another externally generated 2-key TDES key. The new Secure Messaging Encryption Key is entered into the module encrypted with the current Secure Messaging Encryption Key. At the factory environment during initialization, Secure Messaging Encryption Key and System Keys enter the module in plaintext.

The Secure Messaging MAC Key is a 2-key TDES key that computes the MAC for APDU content of a secure session. The Provider installs an externally generated Secure Messaging MAC Key into the module during initialization. The Secure Messaging MAC Key can be updated with another externally generated 2-key TDES key. The new Secure Messaging MAC Key is entered into the module encrypted with the current Secure Messaging

Encryption Key. At the factory environment during initialization, Secure Messaging MAC Key and System Keys enter the module in plaintext.

Authentication Key is a 2-key TDES MAC that enters the module in plaintext during initialization. A Crypto-Officer may also generate an Authentication Key externally and input it into the module in encrypted form. This MAC key is used to authenticate the users and Crypto-Officer to the module.

The **Session Key** is a 2-key or 3-key TDES key. The key is imported from the host application encrypted with a 1024-bit RSA public key. The host application also sends ciphertext that is encrypted with the Session Key to the module. The module first decrypts the Session Key with its RSA private key and then decrypts the ciphertext with the Session Key. Finally the resultant plaintext is transmitted to the host application.

The modules can generate RSA key pairs or import RSA private keys over a secured session. The Provider generates a RSA key pair during the initialization phase. An ANSI X9.31 PRNG is used in the RSA key generation. This PRNG is FIPS-approved. The RSA key pair is used to authenticate users to external applications. The RSA key pair is also used in the transportation of Session Keys. GENERATE KEY PAIR command generates a new RSA key pair using ANSI X9.31 Appendix A.2.4 PRNG.

1.6.2 Key Output

The StartKey and the PackageLoadKey do not exit the module and the modules do not provide any Application Programming Interface (API) to access them. Secure Messaging Keys are never output by the module. The RSA Public Key exits the module over a secured session, but the Private Key never leaves the module. The Authentication Key and the Session Keys also never exit the module.

1.6.3 Key Storage and Zeroization

System Keys are stored in flash memory in plaintext and they are zeroized by a command in the factory environment or by wiping the modules' memory. Secure Messaging Keys reside in flash memory in plaintext and can be zeroized by issuing a command (in factory environment only) or by wiping the modules' memory. Authentication Key is stored in the module in plaintext in AUTH object. The object can be zeroized by issuing a command (in factory environment only) or erasing the module's memory.

A Session Key is stored in memory in plaintext. It is destroyed as soon as it is no longer needed for decryption.

Similar to the System Keys, RSA key pairs can be zeroized by issuing a command (in factory environment only) to delete the file containing the key pair or by wiping the modules' memory.

The PRNG seed is deleted when a new seed is generated.

1.7 Self-Tests

The eToken PRO, eToken PRO HD, eToken NG-OTP, and eToken NG-FLASH perform the following self-tests at power-up:

- Software integrity check using Longitudinal Redundancy Check (LRC). The LRC algorithm performs successive exclusive-ors on consecutive bytes. The modules perform the LRC algorithm using two bytes at a time, resulting in 16-bit LRC checksums.
- Known Answer Tests (KATs)
 - Triple-DES KAT encrypt/decrypt
 - RSA pair wise consistency check for encrypt/decrypt and sign/verify
 - ANSI X9.31 Appendix A.2.4 PRNG KAT
 - SHA-1 KAT

The eToken PRO, eToken PRO HD, eToken NG-OTP, and eToken NG-FLASH perform the following conditional self-tests:

- Continuous RNG Test for the FIPS approved PRNG and the HW-RNG
- RSA pair wise consistency check

1.8 Mitigation of Other Attacks

This section is not applicable. No claim is made that the modules mitigate against any attacks beyond the FIPS 140-2 level 2 or level 3 requirements for the validations.

2 Secure Operation

The sections below describe how to place and keep the module in a FIPS-approved mode of operation.

2.1 Provider Role Guidance

Module initialization in FIPS mode is performed by a Provider at the factory environment before delivery to a Crypto-Officer. Available services for the Provider role are provided in Table 3.

2.2 Crypto-Officer Role Guidance

The Crypto-Officer is responsible for monitoring the modules and User accounts. Tamper-evidence includes tears, scratches, and other irregularities in the packaging and the modules. Aladdin provides the cryptographic module to a Crypto-Officer along with the eToken Run Time Environment (RTE) software and manual. The eToken RTE is eToken format utility software for eToken to work with host computer. The eToken RTE provides a Graphical User Interface (GUI) which shows eToken properties. The Crypto-Officer may use other utilities and access services provided in the FIPS mode of operation. Please refer to Table 4 and Table 5 for the full command set available to the Crypto-Officer.

2.2.1 Initialization and Management

Upon receiving the modules, the Crypto-Officer should check packages for any sign of tampering. The modules should already be configured for FIPS mode. The Crypto-Officer may determine the FIPS mode of Operation of the module from the eToken Property window. The module’s basic properties include a dedicated field to indicate FIPS mode of operation, marked in red in the Figure 5 below.

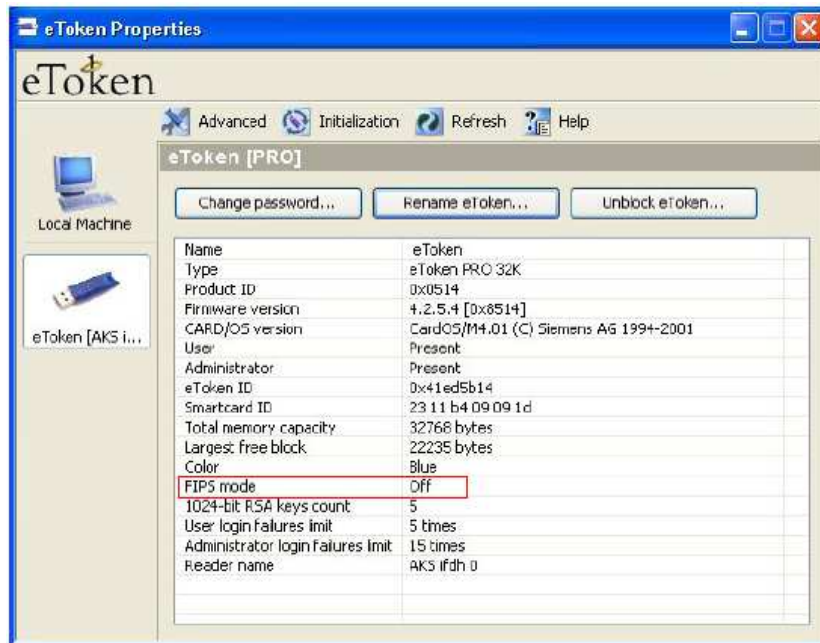


Figure 5 - eToken Properties Window

The “FIPS” field value can be either “On” or “Off.” When the Crypto-Officer receives the module, the “FIPS Mode” field value must indicate “On.”

The Crypto-Officer should periodically inspect the modules for signs of tamper evidence and physical damage. If the User loses control of the eToken for any period of time, the casing should be inspected for tampering.

2.3 User Role Guidance

The User services provided by the modules are described in Table 5. The Users are responsible for keeping the authentication data secure.

3 Acronyms

Table 7 - Acronyms

Acronym	Definition
ANSI	American National Standards Institute
APDU	Application Protocol Data Unit
API	Application Programming Interface
CA	Certificate Authority
CMVP	Cryptographic Module Validation Program
CSP	Critical Security Parameter
CSE	Current Security Environment
DES	Data Encryption Standard
DF	Dedicated File
EEPROM	Electrically Erasable Programmable Read-Only Memory
EF	Elementary File
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FIPS	Federal Information Processing Standards
GUI	Graphical User Interface
HW-RNG	Hardware-Random Number Generator
ID	Identifier
KAT	Known Answer Test
LCD	Liquid Crystal Display
LED	Light Emitting Diode
LRC	Longitudinal Redundancy Check
MAC	Message Authentication Code
NIST	National Institute of Standards and Technology
OS	Operating System
OTP	One Time Password
PC	Personal Computer
PCB	Printed Circuit Board
PKI	Public Key Infrastructure
PRNG	Pseudo Random Number Generator
PSO	Perform Security Operation
RNG	Random Number Generator
RSA	Rivest, Shamir, and Adleman
RTE	Run Time Environment
SHA	Secure Hash Algorithm

Acronym	Definition
TDES	Triple DES
USB	Universal Serial Bus
VPN	Virtual Private Network