

**Aladdin eToken NG-FLASH (Java), Aladdin eToken NG-FLASH  
Anywhere, and Aladdin eToken NG-OTP (Java)**

**FIPS 140-2 Cryptographic Module**

**Security Policy**

Version: 2.0

Date: 20 October 2011

Prepared for:



Prepared by:



Aladdin Public Material - may be reproduced only in its original entirety (without revision)

Aladdin Knowledge Systems, Ltd. 35 Efal St., Kiryat Arye, Petach Tikva, Israel 49511

© Aladdin Knowledge Systems, Ltd., 2011

## CONTENTS

CONTENTS .....	2
1 CRYPTOGRAPHIC MODULE OVERVIEW .....	5
1.1 INTRODUCTION .....	5
1.2 PHYSICAL CRYPTOGRAPHIC MODULE .....	6
1.3 CRYPTOGRAPHIC MODULE BOUNDARY .....	6
1.4 HARDWARE .....	6
1.5 FIRMWARE .....	7
2 SECURITY LEVEL .....	9
3 CRYPTOGRAPHIC MODULE SPECIFICATION .....	10
3.1 PHYSICAL INTERFACES .....	10
3.2 LOGICAL INTERFACES .....	11
4 MODULE CRYPTOGRAPHIC FUNCTIONS .....	12
4.1 RANDOM NUMBER GENERATORS .....	12
4.2 CRYPTOGRAPHIC ALGORITHMS .....	12
4.2.1 Approved .....	12
4.2.2 Non-approved .....	12
4.3 CRITICAL SECURITY PARAMETERS .....	13
4.4 PUBLIC KEYS .....	16
5 ROLES AND SERVICES .....	17
5.1 ROLES .....	17
5.2 IDENTIFICATION .....	19
5.3 ROLE AUTHENTICATION .....	20
5.3.1 Common Claims .....	20
5.3.2 Card Administrator Authentication .....	20
5.3.3 eToken Security Officer Authentication .....	21
5.3.4 Card Holder Authentication .....	22
5.4 SERVICES .....	23
5.4.1 Card Administrator Services .....	23
5.4.2 eToken Security Officer Services .....	24
5.4.3 Card Holder Services .....	24
5.4.4 Public Operator Services .....	25
5.4.5 Relationship between services and CSPs .....	25
5.5 VERIFYING MODULE IS IN APPROVED MODE OF OPERATION .....	28
6 SELF-TESTS .....	30

---

6.1	POWER-ON SELF-TESTS .....	30
6.2	CONDITIONAL SELF-TESTS .....	30
7	SECURITY RULES .....	31
7.1	PHYSICAL SECURITY .....	31
7.2	AUTHENTICATION SECURITY RULES.....	31
7.3	APPLICATION LIFECYCLE SECURITY RULES.....	31
7.4	ACCESS CONTROL SECURITY RULES.....	32
7.5	KEY AND PIN MANAGEMENT SECURITY RULES .....	32
7.5.1	Key and PIN Material .....	32
7.5.2	Key Generation.....	33
7.5.3	Key Derivation.....	33
7.5.4	Key Entry.....	33
7.5.5	Key and PIN Storage.....	34
7.5.6	Key and PIN Output.....	34
7.5.7	Key and PIN Zeroization .....	35
7.6	ELECTROMAGNETIC INTERFERENCE/COMPATIBILITY (EMI/EMC) .....	35
8	MITIGATION OF OTHER ATTACKS .....	36
9	SECURITY POLICY CHECK LIST .....	37
9.1	ROLES AND REQUIRED AUTHENTICATION .....	37
9.2	STRENGTH OF AUTHENTICATION MECHANISMS .....	37
9.3	SERVICES AUTHORIZED FOR ROLES .....	37
9.4	MITIGATION OF ATTACKS.....	37
10	REFERENCES .....	38
11	ACRONYMS AND DEFINITIONS .....	39

**List of Figures**

Figure 1-	Logical CM Structure .....	5
Figure 2 -	Aladdin eToken NG-FLASH (Java) .....	6
Figure 3 -	Aladdin eToken NG-FLASH Anywhere.....	6
Figure 4 -	Aladdin eToken NG-OTP (Java) CM .....	6

**List of tables**

Table 1 -	Supported Cryptographic Services.....	8
Table 2 -	Security Level .....	9
Table 3 -	Physical Interfaces .....	10
Table 4 -	Logical Interfaces .....	11
Table 5 -	Roles.....	19

---

Table 6 - Identification.....	19
Table 7 - Card Administrator Services .....	23
Table 8 - eToken Security Officer Services .....	24
Table 9 - Card Holder Services.....	25
Table 10 - Public Operator Services.....	25
Table 11- Roles and Required Authentication .....	37
Table 12- Strength of Authentication Mechanisms.....	37
Table 13- Services Authorized for Roles.....	37
Table 14 - Mitigation of Attacks .....	37
Table 15 - References .....	38
Table 16 - Acronyms and Definitions.....	39

## 1 CRYPTOGRAPHIC MODULE OVERVIEW

### 1.1 INTRODUCTION

This document defines the Security Policy for the Aladdin eToken NG-FLASH (Java), Aladdin eToken NG-FLASH Anywhere, and Aladdin eToken NG-OTP (Java) Cryptographic Modules (CM). These modules are validated to overall FIPS 140-2 Level 2.

This document contains a description of the CMs, their interfaces and services, the intended operators and the security policies enforced in the approved mode of operation.

The primary purpose of these devices is to serve a wide range of the security-aware applications such as smart card logon, digital signing and so on. The applications work with the devices through the middleware layer (Aladdin eToken PKI Client).

Each CM is a multi-chip standalone USB device and is specifically designed to resist non-evident tampering by both physical and electronic means. All CSPs and services are stored in and provided by an Atmel microcontroller chip. The other chips provide no security relevant functionality.

The CM contains a Java Card applet implementing the Aladdin eToken functionality (Firmware part) running on a GlobalPlatform Java Card operating system (Firmware part) running on an Atmel microcontroller.

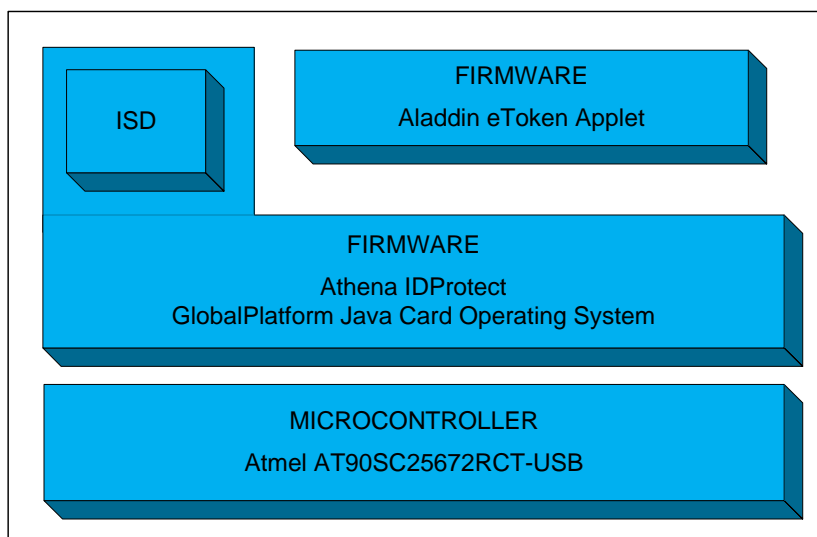


Figure 1- Logical CM Structure

**Hardware:**

- Aladdin eToken NG-FLASH (Java) Version 5
- Aladdin eToken NG-FLASH Anywhere Version 5
- Aladdin eToken NG-OTP (Java) Version 3.0

**Firmware:**

- Athena IDProtect Version 0106.8015.0508 or 0106.8015.0808 (resident in ROM)
- Aladdin eToken Version 1.1 (resident in EEPROM)

## 1.2 PHYSICAL CRYPTOGRAPHIC MODULE



Figure 2 - Aladdin eToken NG-FLASH (Java)



Figure 3 - Aladdin eToken NG-FLASH Anywhere



Figure 4 - Aladdin eToken NG-OTP (Java) CM

## 1.3 CRYPTOGRAPHIC MODULE BOUNDARY

The CM cryptographic boundary is the Aladdin eToken NG-FLASH (Java), Aladdin eToken NG-Flash Anywhere, and Aladdin eToken NG-OTP (Java) devices.

## 1.4 HARDWARE

The primary microcontroller in the Aladdin eToken NG-FLASH (Java) Version 5, Aladdin eToken NG-Flash Anywhere Version 5 and Aladdin eToken NG-OTP (Java) Version 3.0 is the Atmel AT90SC25672RCT-USB Revision D.

The AT90SC25672RCT-USB Revision D is a low-power, high-performance, 8-/16-bit microcontroller with ROM program memory, EEPROM code or data memory, based on the secure AVR enhanced RISC architecture and with a USB 2.0 full speed interface.

By executing powerful instructions in a single clock cycle, the AT90SC25672RCT-USB Revision D achieves throughputs close to 1 MIPS per MHz. Its Harvard architecture includes 32 general-purpose working registers directly connected to the Arithmetic Logical Unit (ALU), allowing two independent registers to be accessed in one single instruction executed in one clock cycle.

The AT90SC25672RCT-USB Revision D uses the secure AVR architecture that allows the linear addressing of up to 8M bytes of code and up to 16M bytes of data as well as a number of new functional and security features.

The AT90SC25672RCT-USB Revision D features 72K bytes of high-performance EEPROM (fast erase/write time, high endurance). This allows system developers to offer their customers a true 64K bytes EEPROM, while still being able to use the remaining 8K bytes for their own purposes (customization and patches, for example). The ability to map the EEPROM in the code space allows parts of the program memory to be reprogrammed in-system.

The cryptographic accelerator featured in the AT90SC25672RCT-USB Revision D is the new AdvX, an N-bit multiplier-accumulator dedicated to performing fast encryption and authentication functions. All cryptographic routines are executed on the secure AVR core which uses the AdvX accelerator during encryption/ decryption. AdvX is based on a 32-bit technology, thus enabling fast computation and low power operation. AdvX supports standard finite field arithmetic functions (including RSA) and arithmetic functions.

The NG-FLASH and NG-Flash Anywhere include a Flash controller and Flash memory. These are neither involved in any services nor perform any cryptographic function and therefore are not security relevant. There are two LEDs: one red, one green. The red is default on and will blink when communicating with the primary microcontroller. The green is default off and will blink when communicating with the Flash controller.

The NG-OTP includes an OTP controller and LCD. These are neither involved in any services nor perform any cryptographic function and therefore are not security relevant.

## 1.5 FIRMWARE

The embedded operating system is GlobalPlatform and Java Card compliant, is loaded on a USB device and supports several USB communication protocols.

### GlobalPlatform

- GlobalPlatform, Card Specification, Version 2.1.1, March 2003
- GlobalPlatform, Card Specification 2.1.1, Amendment A, March 2004

### Java Card

- Runtime Environment Specification, Java Card Platform, Version 2.2.2, March 2006
- Application Programming Interface, Java Card Platform, Version 2.2.2, March 2006
- Virtual Machine Specification, Java Card Platform, Version 2.2.2, March 2006

### Communication

- USB Protocol CCID
- USB Protocol eToken
- USB Protocol GPIO

The GlobalPlatform external interface and internal API allows for application loading and unloading, for secure communication between an application and a terminal and for the use of a PIN in the context of the entire CM. In particular, it allows for the loading of a special application called a Supplementary Security Domain that allows an Application Provider to separate their key space from the Card Administrator.

The Java Card API provides a large set of cryptographic related services. Some of these services rely on hardware.

Support for Random Numbers	DRNG	ANSI X9.31 two key TDES deterministic RNG seeded with the hardware RNG
Support for Message Digest	SHA-1	FIPS 180-2 Secure Hash Standard compliant hashing algorithms
	SHA-256	
Support for Signature	RSA PKCS#1	1024- to 2048-bit in 32-bit increments
Support for Cipher	TDES	112- and 168-bit ECB and CBC
	TDES MAC	Vendor affirmed
	AES	128-, 192- and 256-bit ECB and CBC
	RSA	1024- to 2048-bit in 32-bit increments
Support for On-Card Key Generation	RSA PKCS#1	1024- to 2048-bit in 32-bit increments
Support for Key Establishment	RSA	1024- to 2048-bit in 32-bit increments (strength 80-bits for RSA 1024 to 112-bits for RSA 2048)

Table 1 - Supported Cryptographic Services

The Aladdin eToken Applet is written in Java (as limited by the Java Card standards). The applet specifications are provided in [EJAS]. The eToken file system is organized as described in [EJCA] Section 2.5 *Data layout*.



## 2 SECURITY LEVEL

This section details the security level met by this Cryptographic Module for each Security Requirement.

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

Table 2 - Security Level

### 3 CRYPTOGRAPHIC MODULE SPECIFICATION

This module includes the Issuer Security Domain which allows the Card Issuer to manage the operating system and card content, and the Aladdin eToken Applet that provides the Card Holder services.

The Issuer Security Domain is the on-card representative of the Card Issuer. The ISD has application characteristics such as application AID, application privileges, and Life Cycle State (the Issuer Security Domain inherits the Life Cycle State of the card).

The Aladdin eToken Applet is the on-card representative of the Card Holder. This provides a variety of PKI services to the Card Holder.

If additional applications are loaded into this module, then these applications require a separate FIPS 140-2 validation.

#### 3.1 PHYSICAL INTERFACES

These modules provide the following physical interfaces:

Physical Interface	Description
USBDM	USB D- differential data
USBDP	USB D+ differential data
X <sub>IN</sub>	Crystal (resonator) signal input
X <sub>OUT</sub>	Crystal (resonator) signal output
V <sub>Bus</sub>	Power supply input
GND	Ground (reference voltage)

Table 3 - Physical Interfaces

In addition the NG-OTP provides:

Physical Interface	Description
Pushbutton	Causes a new pseudo-random OTP to be displayed on the LCD.
LCD	Displays a pseudo-random OTP for about 10 seconds each time the pushbutton is pressed.

In addition the NG-FLASH and NG-FLASH Anywhere provides:

Physical Interface	Description
Red LED	Blinks when communicating with the primary microcontroller, default on.
Green LED	Blinks when communicating with the Flash microcontroller, default off.

### 3.2 LOGICAL INTERFACES

The cryptographic module functions as a slave processor to process and respond to the reader commands. ISO/IEC 7816-4 compliant APDU commands are enveloped into the vendor-specific requests (VSR) and passed to the device via USB Control Transfer Endpoint 0. The I/O ports of the platform provide the following logical interfaces:

Logical Interface	Physical Interface	Description
Data In	USBDM, USBDP	APDU commands to the ISD or Aladdin eToken Applet
Data Out	USBDM, USBDP	APDU responses from the ISD or Aladdin eToken Applet
Status Out	USBDM, USBDP	APDU status
Control In	USBDM, USBDP, X <sub>IN</sub> , X <sub>OUT</sub> , V <sub>BUS</sub>	Crystal
Control In	Pushbutton	The OTP provided by the pushbutton and LCD is used for external authentication only and not for any service provided by the CM and so is not security relevant.
Data Out	LCD	
Status Out	Red LED	Blinks when communicating with the primary microcontroller, default on.
Status Out	Green LED	Blinks when communicating with the Flash microcontroller, default off.

Table 4 - Logical Interfaces

## 4 MODULE CRYPTOGRAPHIC FUNCTIONS

The purpose of the Aladdin eToken NG-FLASH (Java), NG-FLASH Anywhere, and Aladdin eToken NG-OTP (Java) CM is serving PKI-enabled PC applications via the middleware layer (Aladdin eToken PKI Client). The host application has flexibility to organize the on-token data and keys according to the application needs; the applet does not enforce particular way of the data organization. However when the PKI Client initializes the applet in the approved mode it enforces data organization as described in [EJCA].

### 4.1 RANDOM NUMBER GENERATORS

The module includes the following random number generators:

- An ANSI X9.31 112-bit key TDES deterministic random number generator (DRNG).  
CAVP RNG Certificate #453
- A hardware random number generator (HRNG) that is used for seeding the DRNG.

### 4.2 CRYPTOGRAPHIC ALGORITHMS

#### 4.2.1 Approved

The module includes the following cryptographic algorithms:

- SHA-1 and SHA-256  
CAVP SHS Certificate #789
- TDES  
CAVP TDES Certificate #681
  - Encrypt/decrypt (for confidentiality purposes)
  - MAC (vendor affirmed, for integrity and authentication purposes)
  - CBC and ECB modes
  - 112- and 168-bit key lengths
- AES  
CAVP AES Certificate #788
  - Encrypt/decrypt
  - CBC and ECB modes
  - 128-, 192- and 256-bit key lengths
- RSA  
CAVP RSA Certificate #375
  - PKCS#1 sign/verify
  - 1024- to 2048-bit key lengths

#### 4.2.2 Non-approved

The module includes the following cryptographic algorithms:

- RSA
  - Key establishment
  - 1024- and 2048-bit key lengths; RSA key agreement; key establishment methodology provides 80 bits to 112 bits of encryption strength

### 4.3 CRITICAL SECURITY PARAMETERS

This module includes the following CSPs.

#### TDES Keys

##### Key Secure Storage Key

This CSP (KSSK) is a 16-byte TDES Key used to encrypt all other secret and private keys of this module when stored in EEPROM (that is, all TDES, AES and RSA keys).

It is generated at first reset of the card using the DRNG.

Keys secured with the KSSK are encrypted when entered / generated and decrypted each time they are used.

##### PIN Secure Storage Key

This CSP (PSSK) is a 16-byte TDES Key used to encrypt all PINs of this module when stored in EEPROM (that is, Java Card OwnerPIN objects).

It is generated at first reset of the card using the DRNG.

PIN values are encrypted when entered and never decrypted. Candidate PINs are encrypted with PSSK to perform the comparison.

##### CA ISD Key Set

This CSP is a set of three TDES keys used to manage GlobalPlatform Secure Channel Sessions between the ISD and the Card Administrator:

- CA-Kenc: Used to derive CA Session Key that will encrypt command data within a Secure Channel Session with C-DECRYPTION Security Level.
- CA-Kmac: Used to derive CA Session Key that will guarantee integrity of any data within a Secure Channel Session with C-MAC Security Level.
- CA-Kkek: Key Encryption Key used to encrypt the CA ISD Key Sets that are loaded in the CM with the PUT KEY command within a Secure Channel Session.

##### CA Session Key Set

This CSP is a set of two TDES keys derived during the GlobalPlatform Secure Channel Session establishment from a selected CA ISD Key Set. These two keys are used to secure exchanges from the Card Administrator to the ISD:

- CA-Senc: Encryption Session Key used to encrypt data exchanged within a Secure Channel Session with C-DECRYPTION Security Level.
- CA-Smac: MAC Session Key used to guarantee integrity of any data exchanged within a Secure Channel Session with C-MAC Security Level and to authenticate the Card Administrator.

##### ESO Key Set

This CSP is set of ten TDES keys initially supplied by the host application during eToken file system initialization. These keys are organized as following:

- ID\_TEST\_ESO: MAC key used to authenticate the ESO role using a challenge-response protocol.
- ID\_SM\_ENC\_IN\_ESO: Decryption key used to decrypt data sent by the host application as a part of the ESO operations.

- ID\_SM\_MAC\_IN\_ESO: MAC key used to guarantee integrity on any data sent by the host application as a part of the ESO operations. This also prevents replay attack as each MAC calculation uses an incrementing counter.
- ID\_SM\_ENC\_OUT\_ESO: Encryption key used to encrypt data sent by the card as a part of the ESO operations.
- ID\_SM\_MAC\_OUT\_ESO: MAC key used to guarantee integrity on any data sent by the card as a part of the ESO operations. This also prevents replay attack as each MAC calculation uses the host challenge.
- ID\_TEST\_ESO\_C: MAC key used to temporarily authenticate the ESO role using a challenge-response protocol during changing of ESO credentials.
- ID\_SM\_ENC\_IN\_ESO\_C: Decryption key used to decrypt the new ESO credentials sent by the host application during changing of the ESO credentials.
- ID\_SM\_MAC\_IN\_ESO\_C: MAC Key used to guarantee integrity of the new ESO credentials sent by the host application during changing of the ESO credentials. This also prevents replay attack as each MAC calculation uses an incrementing counter.
- ID\_SM\_ENC\_OUT\_ESO\_C: Encryption key used to encrypt any data returned from the card during changing of the ESO credentials.
- ID\_SM\_MAC\_OUT\_ESO\_C: MAC Key used to guarantee integrity any replies returned from the card during changing of the ESO credentials. This also prevents replay attack as each MAC calculation uses the host challenge.

The ESO Key Set is organized as two five-key subsets. The first one is used for normal operation (i.e. authentication of the ESO, and encryption and integrity of further ESO operation). During change of the ESO credentials the first subset is used to protect the change of the second and vice versa. The details of this operation are described in [EJCA].

#### CH Key Set

This CSP is set of ten TDES keys initially supplied by the host application during eToken file system initialization. These keys are organized as following:

- ID\_TEST\_CH: MAC key used to authenticate the CH role using a challenge-response protocol.
- ID\_SM\_ENC\_IN\_CH: Decryption key used to decrypt data sent by the host application as a part of the CH operations.
- ID\_SM\_MAC\_IN\_CH: MAC key used to guarantee integrity on any data sent by the host application as a part of the CH operations.
- ID\_SM\_ENC\_OUT\_CH: Encryption key used to encrypt data sent by the card as a part of the CH operations.
- ID\_SM\_MAC\_OUT\_CH: MAC key used to guarantee integrity on any data sent by the card as a part of the CH operations.
- ID\_TEST\_CH\_C: MAC key used to temporary authenticate the CH role using a challenge-response protocol during changing of CH credentials.
- ID\_SM\_ENC\_IN\_CH\_C: Decryption key used to decrypt the new CH credentials sent by the host application during changing of the CH credentials.
- ID\_SM\_MAC\_IN\_CH\_C: MAC Key used to guarantee integrity of the new CH credentials sent by the host application during changing of the CH credentials.

- ID\_SM\_ENC\_OUT\_CH\_C: Encryption key used to encrypt any data returned from the card during changing of the CH credentials.
- ID\_SM\_MAC\_OUT\_CH\_C: MAC Key used to guarantee integrity any replies returned from the card during changing of the CH credentials.

The CH Key Set is organized as two five-key subsets. The first one is used for normal operation (i.e. authentication of the CH, and encryption and integrity of the further CH operation). During change of the CH credentials the first subset is used to protect the change of the second and vice versa. The details of this operation are described in [EJCA].

#### File System Re-initialization Key Set

This CSP is set of two or three TDES keys. All keys have the same random value, generated by the host application during eToken file system initialization. This key set is optional and eToken file-system re-initialization is only possible if this key set exists. The use of this key set optionally requires CH or ESO authentication. These keys are organized as following:

- ID\_TEST\_REINIT: MAC key used to perform challenge-response authentication in order to enable the eToken file system re-initialization.
- ID\_PSO\_ESO\_REINIT: MAC key with the same key material as ID\_TEST\_REINIT protected by the ESO Key Set (optional).
- ID\_PSO\_CH\_REINIT: MAC key with the same key material as ID\_TEST\_REINIT protected by the CH Key Set (optional).

All keys are initialized with the same key material. Since the key material is random, the host application cannot know it. The only way to authenticate with ID\_TEST\_REINIT (and to re-initialize the eToken file system) is to perform firstly authentication of the ESO or CH role and then to use either ID\_PSO\_ESO\_REINIT or ID\_PSO\_CH\_REINIT key (it is used as cryptographic engine with access restricted to the particular role). The details of this operation are described in [EJCA].

#### CH Session Key

The middleware layer (Aladdin eToken PKI Client) uses the CM for establishing TDES keys such as encryption keys for e-mail protection or session keys for VPN communication.

The wrapped session key is passed as an input to the Use CH RSA Key Pair service. The unwrapped key is returned to the middleware. It is neither stored nor used by the CM (neither as a key nor as data). The unwrapped key is stored in RAM and is deleted before the next service is performed.

This key establishment service requires authentication as use of the CH RSA Key Pairs are protected by the CH role (authentication, encryption and integrity of operations) and, optionally, by the Secondary Authentication Secret. The import and export of this CSP (both command and response) is protected with SM.

#### **RSA Keys**

##### CH RSA Key Pair(s)

The Aladdin eToken Applet may contain one or more RSA key pairs in which the private key is a CSP. The number of keys and their location in the eToken file system are application-specific. The CH RSA Key Pairs are protected by the CH role (authentication, encryption and integrity of operations) and, optionally, by the Secondary Authentication Secret.

#### **PINs**

##### Secondary Authentication Secret

This CSP is optional PIN used to protect CH RSA Key Pairs. It may be global (i.e. the same for all keys) or per-key. This PIN belongs to the CH role (i.e. it can be presented only after CH role has been successfully authenticated). The main purpose of the Secondary Authentication Secret is that it should be presented each time before a protected operation can occur (unlike the CH Key Set which remains authorized after successful authentication). The operations with this PIN (i.e. import, authentication and change) are protected by the SM of the CH role. The details of this operation are described in [EJCA].

#### 4.4 PUBLIC KEYS

##### RSA Keys

##### CH RSA Key Pair(s)

The CH RSA Key Pair(s) include the public key.



## 5 ROLES AND SERVICES

### 5.1 ROLES

Cryptographic Officer Roles	
Card Administrator	<p>This role is responsible for managing the security configuration of the module.</p> <p>The Card Administrator authenticates to the module through the GlobalPlatform mutual authentication protocol. This protocol is based on the sharing of a TDES key set between him and the embedded Issuer Security Domain (ISD).</p> <p>Once authenticated, the Card Administrator is able to execute the services provided by the ISD in a Secure Channel Session (see [GP] for more details).</p>
eToken Security Officer	<p>This role is responsible for managing the life cycle of the Card Holder (CH). This is an optional role. The presence of the ESO is defined during eToken file system initialization.</p> <p>It is important to distinguish the ESO and the CA. The CA is responsible for card content; this role is capable of loading/unloading applets to/from the card. The ESO is responsible for management of the lifecycle of the CH Key Set and, optionally, for the eToken file system re-initialization. ESO responsibility lies solely in the logical space of the Aladdin eToken Applet.</p> <p>The ESO authenticates using the ESO Key Set. The authentication is done through the challenge-response protocol specified in Section 5.3.3 <i>eToken Security Officer Authentication</i>. Once authentication is fulfilled, further operations of the ESO role are protected with SM mechanisms described in [EJAS].</p>
User Roles	
Card Holder	<p>This role is associated with the Card Holder.</p> <p>The Card Holder role is defined in the context of the Aladdin eToken Applet and is used to protect keys and data owned by the Card Holder.</p> <p>In terms of host application, it is the most important role since the major purpose of the device is to keep the user-related secure data and cryptographic keys for the PKI-enabled applications.</p> <p>The CH authenticates using the CH Key Set. The authentication is done through the challenge-response protocol specified in Section 0 <i>ESO SM keys</i> have no error counter, but since their use is restricted by the corresponding ESO TEST key they effectively behave as having the same threshold as the corresponding ESO TEST key.</p>

	Card Holder Authentication. Once authentication is fulfilled, further operations of the CH role are protected with SM mechanisms described in [EJAS].
--	-------------------------------------------------------------------------------------------------------------------------------------------------------

No Roles	
Public Operator	No-role operator who does not know any CSPs related to the ISD or Aladdin eToken Applet. This non-authenticated operator can only access non-security relevant services provided by the ISD and Aladdin eToken Applet that do not require any prior authentication.
Maintenance Roles	
None	This CM does not support any maintenance role.

Table 5 - Roles

## 5.2 IDENTIFICATION

This Cryptographic Module performs identity based authentication using cryptographic keys. A unique identifier is associated with each cryptographic key to uniquely identify the off-card entity performing the authentication.

Identity	CSP	Identifier
Card Administrator	CA ISD Key Set	KVN, KID (see [GP])
ESO	ESO Key Set	ID (see [EJCA] Section 3.1 <i>ID Values</i> )
	ID_TEST_ESO	0x21
	ID_SM_ENC_IN_ESO	0x22
	ID_SM_MAC_IN_ESO	0x23
	ID_SM_ENC_OUT_ESO	0x24
	ID_SM_MAC_OUT_ESO	0x25
	ID_TEST_ESO_C	0x2A
	ID_SM_ENC_IN_ESO_C	0x2B
	ID_SM_MAC_IN_ESO_C	0x2C
	ID_SM_ENC_OUT_ESO_C	0x2D
	ID_SM_MAC_OUT_ESO_C	0x2E
CH	CH Key Set	ID (see [EJCA] Section 3.1 <i>ID Values</i> )
	ID_TEST_CH	0x11
	ID_SM_ENC_IN_CH	0x12
	ID_SM_MAC_IN_CH	0x13
	ID_SM_ENC_OUT_CH	0x14
	ID_SM_MAC_OUT_CH	0x15
	ID_TEST_CH_C	0x1A
	ID_SM_ENC_IN_CH_C	0x1B
	ID_SM_MAC_IN_CH_C	0x1C
	ID_SM_ENC_OUT_CH_C	0x1D
	ID_SM_MAC_OUT_CH_C	0x1E

Table 6 - Identification

## 5.3 ROLE AUTHENTICATION

### 5.3.1 Common Claims

Concurrent operators are not supported.

For all role authentications the following properties stand:

- the probability is less than one in 1,000,000 that a random attempt at authentication will succeed
- during any one minute period, the probability is less than 1 in 100,000 that a random authentication attempt will succeed

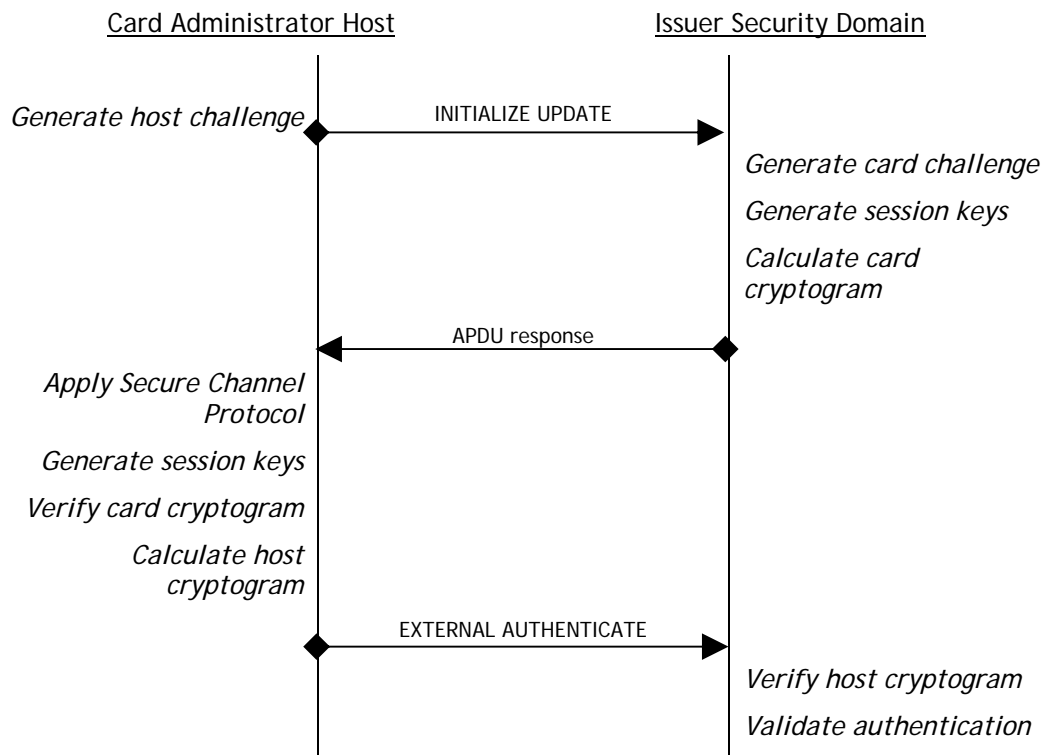
This mechanism includes a counter of failed authentication and a blocking mechanism. The counter is decremented prior to any attempt to authenticate and is only reset to its threshold (maximum value) upon successful authentication. The authentication mechanism is blocked when the associated counter reaches zero.

### 5.3.2 Card Administrator Authentication

The counter threshold is in the range one to 255 with default value 80. This mechanism is called velocity checking (see [GP]).

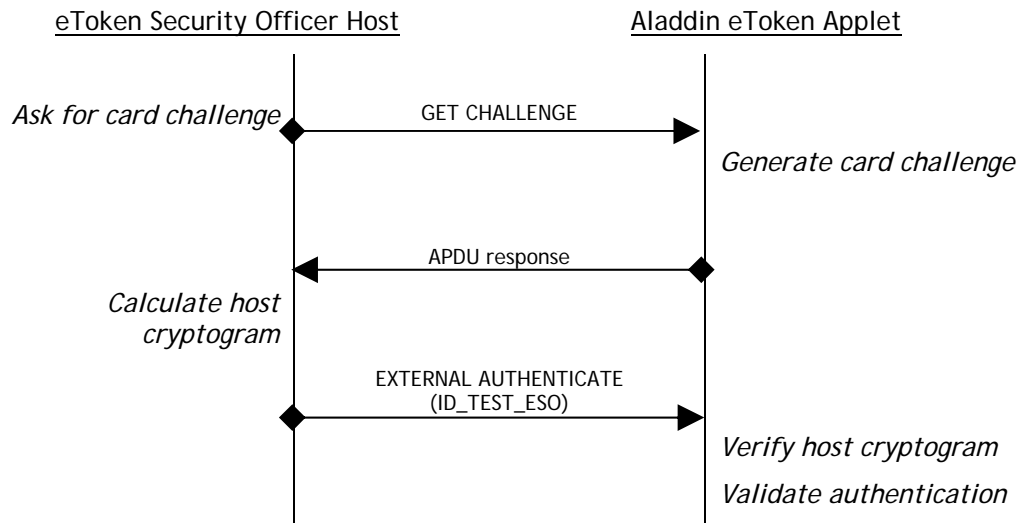
If the authentication mechanism of the ISD is blocked the CM is irreversibly terminated (the KSSK and PSSK are zeroized and the CM enters the GlobalPlatform TERMINATED state in which only the Public Operator GET DATA service is available).

The Card Administrator authenticates by opening a GlobalPlatform Secure Channel Session with the ISD. This Secure Channel Session establishment involves two APDU commands as follows:



### 5.3.3 eToken Security Officer Authentication

The ESO authenticates by opening a SM session with the Aladdin eToken Applet using the ID\_TEST\_ESO key (see ESO Key Set). If the key is blocked, the eToken will continue to provide non-ESO services, but the ESO role cannot be authenticated until eToken file system re-initialization (if allowed). ID\_TEST\_ESO and ID\_TEST\_ESO\_C each have an independent error counter. The error counter is in the range one to 15 with default value 15.

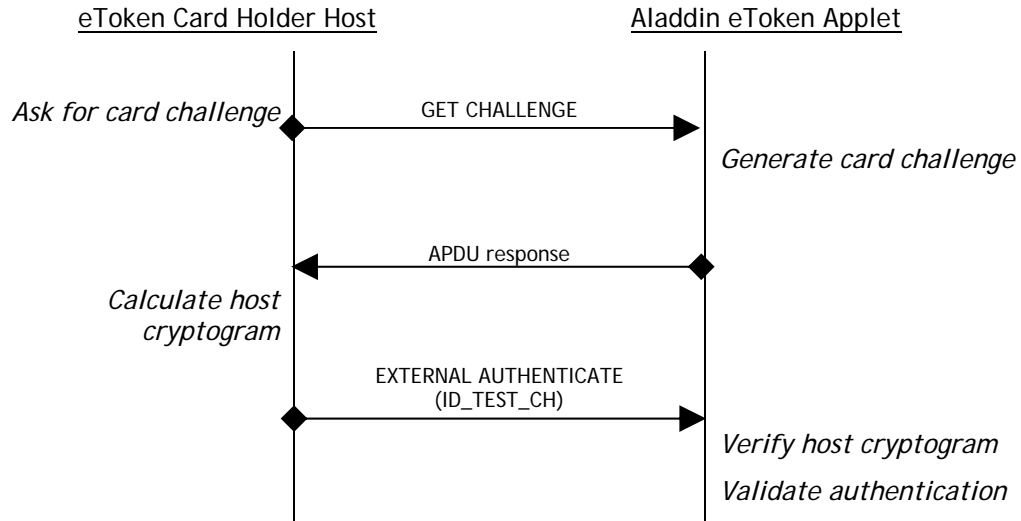


It is assumed that SM keys (ID\_SM\_ENC\_ESO and ID\_SM\_MAC\_ESO) also known to the application. The authentication process does not include them, but the very first operation protected with SM will fail otherwise.

ESO SM keys have no error counter, but since their use is restricted by the corresponding ESO TEST key they effectively behave as having the same threshold as the corresponding ESO TEST key.

### 5.3.4 Card Holder Authentication

The CH authenticates by opening a SM session with the Aladdin eToken Applet using the ID\_TEST\_CH key (see CH Key Set). If the key is blocked, the eToken may operate as usual, but the CH role cannot be authenticated any more until eToken file system re-initialization (if allowed) or unblocking of the CH role by the ESO (if allowed). ID\_TEST\_CH and ID\_TEST\_CH\_C each have an independent error counter. The error counter is in the range one to 15 with default value 15.



It is assumed that SM keys (ID\_SM\_ENC\_CH and ID\_SM\_MAC\_CH) also known to the application. The authentication process does not include them, but the very first operation protected with SM will fail otherwise.

CH SM keys have no error counter, but since their use is restricted by the corresponding CH TEST key they effectively behave as having the same threshold as the corresponding CH TEST key.

## 5.4 SERVICES

### 5.4.1 Card Administrator Services

This role can only be active when the ISD is currently selected. Therefore the service of the Card Administrator are presented in the terms of the [GP]-defined APDU commands.

Authentication	
INITIALIZE UPDATE	CA can initiate a GlobalPlatform Secure Channel Session, setting key set version and index.
EXTERNAL AUTHENTICATE	CA can open a GlobalPlatform Secure Channel Session with the ISD in order to communicate with it in a secure and confidential way.
Card Content Management	
INSTALL	CA can initiate or perform the various steps required for CM content management.
LOAD	CA can transfer a Load File to the CM.
DELETE (card content)	CA can delete an Executable Load File (package) or an Application (applet) or an Executable Load File and its related Applications.
PUT KEY	Regarding ISD keys, CA can either: <ul style="list-style-type: none"> <li>• Replace an existing ISD key with a new key</li> <li>• Replace multiple existing ISD keys with new keys</li> <li>• Add a single new ISD key</li> <li>• Add multiple new ISD keys</li> </ul>
DELETE (key)	CA can delete an ISD key uniquely identified by the KID and KVN.
SET STATUS	CA can modify the Card Life Cycle State or an Application Life Cycle State.
GET STATUS	CA can retrieve Life Cycle status information of the ISD, Executable Load File, Executable Module, Application or Security Domain. No CSPs can be read using this service.
STORE DATA	CA can transfer data to the ISD.
Public Commands	
SELECT	Operator can select an Application. This command also logs out the current role.
GET DATA (ISD)	Operator can retrieve public data from the ISD. No CSPs can be read using this service.

Table 7 - Card Administrator Services

### 5.4.2 eToken Security Officer Services

This role can be active when the Aladdin eToken Applet is currently selected (and if the applet has been initialized with presence of the ESO role).

Mandatory Services	
ESO Logon	Authenticate the ESO role
ESO Credential Change	Change the current ESO Key Set
Optional Services (depending on the eToken file system initialization parameters)	
CH Unlocking	This service is available only if the ESO Key Set exists. Unlock the CH Key Set. The ESO provides the new CH key (that may be changed later by the CH). All CH data and other keys remain untouched.
User Reset	This service is available only if the ESO Key Set exists. Unlock the CH Key Set. The ESO provides the new CH key (that may be changed later by the CH). All CH data and other keys are destroyed.
eToken file system re-initialization	This service is available only if the File System Re-initialization Key Set exists. The data in the Aladdin eToken Applet are cleared and the eToken file system is re-initialized.
Public Commands	
SELECT	Operator can select an Application. This command also logs out the current role.
GET DATA (ISD)	Operator can retrieve public data from the ISD. No CSPs can be read using this service.

Table 8 - eToken Security Officer Services

Sample flows of all described services are presented in [EJCA].

### 5.4.3 Card Holder Services

This role can be active when the Aladdin eToken Applet is currently selected.

Mandatory Services	
CH Logon	Authenticate the CH role
CH Credential Change	Change the current CH Key Set
Generate CH RSA Key Pair	Generate a CH RSA Key Pair
CH Create Secondary Authentication Secret	Import Secondary Authentication Secret
Optional Services (depending on eToken file system initialization parameters)	
Use CH RSA Key Pair	This service is available only if a CH RSA Key Pair exists.



	Use a CH RSA Key Pair to generate/verify signatures or encryption/decryption of keys for key establishment. Encryption/decryption of data is not allowed.
eToken file system re-initialization	This service is available only if the File System Re-initialization Key Set exists.  The data in the Aladdin eToken Applet are cleared and the eToken file system is re-initialized.
Public Commands	
SELECT	Operator can select an Application. This command also logs out the current role.
GET DATA (ISD)	Operator can retrieve public data from the ISD.  No CSPs can be read using this service.

Table 9 - Card Holder Services

Sample flows of all described services are presented in [EJCA].

#### 5.4.4 Public Operator Services

Public Commands	
SELECT	Operator can select an Application.
GET DATA	Operator can retrieve public data from the ISD.  No CSPs can be read using this service.

Table 10 - Public Operator Services

#### 5.4.5 Relationship between services and CSPs

Relationship can be:

- Enter (or establish)
- Write
- Generate
- Execute (computation involving the CSP)
- Delete
- Zeroize

#### Key Secure Storage Key

Service	Type of access
First Card reset	Generate
INITIALIZE UPDATE	Execute
EXTERNAL AUTHENTICATE	Execute
LOAD	Execute
PUT KEY	Execute
SET STATUS (TERMINATED)	Zeroize

PIN Secure Storage Key

Service	Type of access
First Card reset	Generate
Use CH RSA Key Pair	Execute
CH Create Secondary Authentication Secret	Execute
SET STATUS (TERMINATED)	Zeroize

CA ISD Key Set

Service	Type of access	Key
INITIALIZE UPDATE	Execute	CA-Kenc, CA-Kmac
EXTERNAL AUTHENTICATE	Execute	CA-Kenc, CA-Kmac
PUT KEY	Execute/Write	CA-Kenc, CA-Kmac, CA-Kkek
DELETE (key)	Delete	CA-Kenc, CA-Kmac, CA-Kkek

CA Session Key Set

Service	Type of access	Key
INITIALIZE UPDATE	Generate	CA-Senc, CA-Smac
Card reset	Delete	CA-Senc, CA-Smac

In a Secure Channel Session with Security Level C-MAC:

Service	Type of access	Key
DELETE	Execute	CA-Smac
EXTERNAL AUTHENTICATE	Execute	CA-Smac
GET DATA	Execute	CA-Smac
GET STATUS	Execute	CA-Smac
INSTALL	Execute	CA-Smac
LOAD	Execute	CA-Smac
PUT KEY	Execute	CA-Smac
SET STATUS	Execute	CA-Smac
STORE DATA	Execute	CA-Smac

In a Secure Channel Session with Security Level C-DECRYPTION and C-MAC:

Service	Type of access	Key
DELETE	Execute	CA-Senc, CA-Smac

EXTERNAL AUTHENTICATE	Execute	CA-Senc, CA-Smac
GET DATA	Execute	CA-Senc, CA-Smac
GET STATUS	Execute	CA-Senc, CA-Smac
INSTALL	Execute	CA-Senc, CA-Smac
LOAD	Execute	CA-Senc, CA-Smac
PUT KEY	Execute	CA-Senc, CA-Smac
SET STATUS	Execute	CA-Senc, CA-Smac
STORE DATA	Execute	CA-Senc, CA-Smac

ESO Key Set

Service	Type of Access
ESO Logon	Execute
ESO Credential Change	Delete, Enter
CH Unlocking	Execute
User Reset	Execute
eToken file system re-initialization	Zeroize

CH Key Set

Service	Type of Access
CH Unlocking	Delete, Enter
User Reset	Delete, Enter
CH Logon	Execute
CH Credential Change	Delete, Enter
eToken file system re-initialization	Zeroize

File System Re-initialization Key Set

Service	Type of Access
eToken file system re-initialization	Execute

CH Session Key

Service	Type of Access
Use CH RSA Key Pair	Enter, Delete

CH RSA Key Pair(s)

Service	Type of Access
User Reset	Delete
Generate CH RSA Key Pair	Generate
Use CH RSA Key Pair	Execute
eToken file system re-initialization	Zeroize

Secondary Authentication Secret

Service	Type of Access
User Reset	Delete
Use CH RSA Key Pair	Execute
CH Create Secondary Authentication Secret	Enter
eToken file system re-initialization	Zeroize

## 5.5 VERIFYING MODULE IS IN APPROVED MODE OF OPERATION

In order to verify the approved mode of operation:

1. The Card Administrator must select the ISD, send a GET DATA command with the CPLC Data tag '9F7F' and verify that the returned data contains fields as follows (other fields are not relevant here). This verifies the version of the operating system.

Data Element	Length	Value	Version
IC type	2	'0106'	Atmel AT90SC25672RCT-USB Revision D
Operating system release date	2	'8015'	Firmware Version Part 1
Operating system release level	2	'0508' or '0808'	Firmware Version Part 2

2. The Aladdin eToken FIPS 140-2 Approved Mode Indicator application is provided with the CM and must be run. It selects the Aladdin eToken Applet and checks:

- Validity of attributes and access conditions of the ESO Key Set (if it exists).
- Presence, validity of attributes and access conditions of the CH Key Set.
- Validity of attributes and access conditions of the File System Re-initialization Key Set (if it exists).
- Validity of attributes and access conditions of any CH RSA Key Pairs (if any exist), i.e. protection by the CH Role directly or via the Secondary Authentication Secret (if it exists).

- Validity of attributes and access conditions of the Secondary Authentication Secret (if it exists), i.e. protection by the CH Role.

The full sequence of checks (including exact organization of the directory layout) is presented in [EJCA] Section 4.2 *Validation*.

## 6 SELF-TESTS

### 6.1 POWER-ON SELF-TESTS

Each time this cryptographic module is powered up it tests that the cryptographic algorithms still operate correctly and that sensitive data have not been damaged.

#### Cryptographic algorithm testing:

Known Answer Tests (KATs) are conducted for each cryptographic algorithm in one mode of operation. Known input data and answers are stored in EEPROM. The following KATs are performed in random order:

- ANSI X9.31 DRNG,
- SHA-1,
- SHA-256,
- TDES (encrypt and decrypt with 112-bit key in CBC mode),
- AES (encrypt and decrypt with 128-bit key in CBC mode),
- RSA PKCS#1 (sign and verify with 1024-bit private and public key),

KATs are performed prior to the dispatch of the first APDU command for processing. If one of the KATs fails the card goes mute (performs no further data or status input or output and must be reset).

#### Firmware integrity testing:

A standard CRC16 checksum is used to verify that no applications present in EEPROM have been modified. It also checks the integrity of all additions and corrections that have been added to the module (patch code and patch table). ROM code is excluded from firmware integrity verification. If a test fails the card is terminated (the KSSK and PSSK are zeroized and the CM enters the TERMINATED state).

### 6.2 CONDITIONAL SELF-TESTS

#### Key Pair-Wise Consistency Test:

This test is performed during RSA Key Pair generation once the CM has generated the RSA Key Pair values (both signature generation/verification and encryption/decryption are tested). If the test fails the card goes mute.

#### Continuous RNG Tests:

The hardware RNG and DRNG are tested for repetition of serially output 64-bit values. If the test fails the card goes mute.

#### Firmware Load Test:

Application loading follows the GlobalPlatform 2.1.1 specifications: GlobalPlatform Secure Channel Session with TDES MAC (see [GP]). Note that a failed application load rolls back to the state prior to the load starting.

**Note:** *Power-on self-tests on demand: resetting the module is an approved self-test on demand function.*

## 7 SECURITY RULES

This section details the rules that form the policy of the Cryptographic Module.

### 7.1 PHYSICAL SECURITY

The Cryptographic Module (CM) is a multi-chip standalone embodiment with the cryptographic boundary encompassing the devices. Each device is a hard plastic shell containing the Atmel microcontroller chip plus other chips. All CSPs and services are stored in and provided by the Atmel microcontroller chip. The Atmel microcontroller chip is protected by a hard opaque tamper-evident metal active shield. The other chips provide no security relevant functionality.

The CM employs physical security mechanisms in order to restrict unauthorized physical access to the contents of the module and to deter unauthorized use or modification of the module (including substitution of the entire module) when installed.

The Atmel microcontroller chip physical security features meet FIPS-140-2 level 4 requirements with:

- Production-grade component including passivation techniques and state-of-the-art physical security features:
  - Dedicated Hardware for Protection Against SPA/DPA/DEMA Attacks
  - Advanced Protection Against Physical Attack, Including Active Shield
  - Environmental Protection Systems
  - Voltage Monitor
  - Frequency Monitor
  - Temperature Monitor
  - Light Protection
- Opaque coating on chip that deter direct observation within the visible spectrum,

This chip is designed to meet Common Criteria EAL4+

### 7.2 AUTHENTICATION SECURITY RULES

This CM implements authentication mechanisms for each role. Each authentication mechanism includes the verification of the knowledge of a key shared between the device and the external operator, and, for each restricted service, verification that the authentication security status is granted.

Each of these keys has a unique identifier that is used by the external operator to identify them:

- The CA ISD Key Set represents the role of the Card Administrator.
- The ESO Key Set in the Aladdin eToken Applet represents the role of the eToken Security Officer.
- The CH Key Set in the Aladdin eToken Applet represents the role of the Card Holder.

### 7.3 APPLICATION LIFECYCLE SECURITY RULES

Additional applications can be loaded in the module after card issuance as specified in GlobalPlatform. However, these additional applications must be FIPS 140-2 validated before being loaded.

- Application loading is one of the services provided by the operating system that is restricted to the Card Administrator: a Secure Channel Session must be open between the external operator (more precisely the middleware the CA is using to manage card content) and the ISD. Application loading is protected by a TDES MAC on every block of data.
- The application loading service is available before and after card issuance.
- The CA is responsible for application personalization and lifecycle management following GlobalPlatform.
- The CA is responsible for creating as many instances of loaded applets as required, according to card resources.

The module's FIPS 140-2 validation is no longer valid once a non-validated applet is loaded.

## 7.4 ACCESS CONTROL SECURITY RULES

This module manages sensitive data and services whose access is controlled by the following rules:

- CA ISD Key Set must be loaded through a GlobalPlatform Secure Channel Session ensuring their integrity and confidentiality (112-bit TDES encryption and a TDES based MAC).
- Aladdin eToken Applet Key Sets are loaded during initialization process. This is done in a secure environment. The future changes of these Key Sets in the field are protected by Secure Messaging using the current key sets.

## 7.5 KEY AND PIN MANAGEMENT SECURITY RULES

### 7.5.1 Key and PIN Material

This card supports the following CSPs:

Key name (CSP)	Type	Length	Strength
Key Secure Storage Key	TDES	112-bits	80-bits
PIN Secure Storage Key	TDES	112-bits	80-bits
CA ISD Key Set	TDES	112-bits	80-bits
CA Session Key Set	TDES	112-bits	80-bits
ESO Key Set	TDES (10 keys)	112-bits 168-bits	80-bits 112-bits
CH Key Set	TDES (10 keys)	112-bits 168-bits	80-bits 112-bits
File System Re-initialization Key Set	TDES	112-bits 168-bits	80-bits 112-bits
CH Session Key	TDES	112-bits 168-bits	80-bits 112-bits
CH RSA Key Pair(s)	RSA	1024-bits to 2048-bits in 32-bit increments	80-bits to 112-bits
Secondary Authentication Secret	PIN	Minimum 32-bits	Minimum 32-bits



This card can also support a range of symmetric and asymmetric keys:

Key name	Type	Length	Strength
TDES keys	TDES	112-bits 168-bits	80-bits 112-bits
AES keys	AES	128-bits 192-bits 256-bits	128-bits 192-bits 256-bits
RSA keys	RSA	1024-bits 2048-bits	80-bits 112-bits

### 7.5.2 Key Generation

#### Key Secure Storage Key

#### PIN Secure Storage Key

These keys are generated at first reset of the card using the DRNG.

#### CH RSA Key Pair(s)

These key pairs are generated upon application request using the generate CH RSA Key Pair service after CH authentication.

### 7.5.3 Key Derivation

#### CA Session Key Set

[GP] ISD Session keys are derived by the operating system upon opening a Secure Channel Session (successful mutual-authentication):

- CA-Smac Session Key: generated from CA-Kmac, used for protecting data integrity in GlobalPlatform Secure Channel Session secure mode (MAC).
- CA-Senc Session Key: generated from CA-Kenc, used for protection data confidentiality in GlobalPlatform Secure Channel Session mode (Encryption).

This is the standard GlobalPlatform version 2.1.1 SCP01 method of opening a Secure Channel Session with the module which involves key derivation.

### 7.5.4 Key Entry

#### CA ISD Key Set

The first key set is entered in the factory (a secure environment) in plaintext.

Subsequently these keys are entered in the module using the PUT KEY service for:

- Replacing an existing key with a new key
- Replacing existing key set with new key set
- Adding a single new key
- Adding a new key set

The CM enforces confidentiality while entering Security Domain secret keys using key encryption following [GP] (FIPS approved algorithms and operation mode). The CM provides no Security

---

Domain secret key output. All secret values of these keys are entered encrypted with the TDES CA-Kkek identified during the GlobalPlatform Secure Channel Session initialization, when one of the Security Domain key sets is selected.

#### ESO Key Set

The first key set is entered in the factory (a secure environment) in plaintext.

They may be changed later by using the ESO Credential Change service which uses SM after ESO authentication.

#### CH Key Set

The first key set is entered in the factory (a secure environment) in plaintext.

They may be changed later by using the CH Credential Change service which uses SM after CH authentication. They may be modified by using the during the CH Unlocking service after ESO authentication. They may be re-entered by using the User Reset service after ESO authentication.

#### File System Re-initialization Key Set

This key set is entered in the factory (a secure environment) in plaintext.

#### CH Session Key

This key is established using the Use CH RSA Key Pair service.

#### Secondary Authentication Secret

This PIN may be imported by a host application using the CH Create Secondary Authentication Secret service. This uses SM after successful CH authentication and so is protected by ID\_SM\_ENC\_IN\_CH.

### 7.5.5 Key and PIN Storage

#### Key Secure Storage Key (KSSK)

#### PIN Secure Storage Key (PSSK)

These two keys are stored plaintext in EEPROM.

#### CA ISD Key Set

These keys are stored encrypted with the TDES key KSSK in EEPROM. The CM also applies an integrity checksum to these keys.

#### ESO Key Set

#### CH Key Set

#### File System Re-initialization Key Set

#### CH RSA Key Pair(s)

#### Secondary Authentication Secret

These CSPs are stored using the mechanisms of the underlying JVM.

### 7.5.6 Key and PIN Output

The CH Session Key is output when using the Use CH RSA Key Pair service for key establishment: the Card Holder role is authenticated and the output is protected by SM.

The public part of a CH RSA Key Pair can be output from the module.

### 7.5.7 Key and PIN Zeroization

The CM offers services to zeroize all the persistent keys and PINs:

- The KSSK and PSSK are zeroized when Card lifecycle state is set to TERMINATED. The Card Administrator can achieve this explicitly using the SET STATUS command, or a severe security event may occur (failure of an integrity check on patches, EEPROM code, PINs or Keys). By zeroizing the KSSK and the PSSK, all other Keys and PINs stored in the module are made irreversibly unusable.

The CM offers services to zeroize all the session keys:

- When a Secure Channel Session is closed for any reason other than power-off, the CM overwrites the session keys with random data from the DRNG. When a Secure Channel Session is closed due to a power-off, the session keys are lost as they are stored in RAM. The RAM is actively cleared to zero on the next power-on.

The CM offers services to zeroize Key and PIN by removal:

- When the Aladdin eToken Applet is re-initialized or when Keys and PINs owned by it are removed using the User Reset or eToken file system re-initialization service their storage is zeroized.

## 7.6 ELECTROMAGNETIC INTERFERENCE/COMPATIBILITY (EMI/EMC)

The Cryptographic Module conforms to the EMI/EMC requirements specified by part 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class B.

## 8 MITIGATION OF OTHER ATTACKS

Typical smart card attacks are Simple Power Analysis, Differential Power Analysis, Timing Analysis and Fault Induction that may lead to revealing sensitive information such as PIN and Keys by monitoring the module power consumption and timing of operations or bypass sensitive operations.

This Cryptographic Module is protected against SPA, DPA, Timing Analysis and Fault Induction by combining State of the Art firmware and hardware counter-measures.

The Cryptographic Module is protected from attacks on the operation of the IC hardware. The protection features include detection of out-of-range supply voltages, frequencies or temperatures, detection of illegal address or instruction, and physical security. For more information see specification AT90SC Vulnerability Analysis Lite, General Business Use, AT90SC\_EVA\_Lite\_V1.0 (17 Jul 06).

All cryptographic computations and sensitive operations such as PIN comparison provided by the Cryptographic Module are designed to be resistant to timing and power analysis. Sensitive information of the embedded operating system is securely stored and integrity protected. Sensitive operations are performed in constant time, regardless of the execution context (parameters, keys, etc.), owing to a combination of hardware and firmware features.

The Cryptographic Module does not operate in abnormal conditions such as extreme temperature, power and external clock, increasing its protection against fault induction.

## 9 SECURITY POLICY CHECK LIST

### 9.1 ROLES AND REQUIRED AUTHENTICATION

Role	Type of Authentication	Authentication Data
Card Administrator	TDES authentication	CA ISD Key Set
eToken Security Officer	TDES authentication	ESO Key Set
Card Holder	TDES authentication	CH Key Set

Table 11- Roles and Required Authentication

### 9.2 STRENGTH OF AUTHENTICATION MECHANISMS

Authentication Mechanism	Strength of Mechanism
TDES authentication with CA ISD Key Set	$2^{80}$
TDES authentication with ESO Key Set	$2^{80}$
TDES authentication with CH Key Set	$2^{80}$
TDES authentication with File System Re-initialization Key Set	$2^{80}$
PIN authentication with Secondary Authentication Secret	$2^{32}$

Table 12- Strength of Authentication Mechanisms

All these authentication mechanisms implement a limited retry counter.

### 9.3 SERVICES AUTHORIZED FOR ROLES

Role	Authorized Services
Card Administrator	Section 5.4.1 lists authorized services for this role
eToken Security Officer	Section 5.4.2 lists authorized services for this role
Card Holder	Section 5.4.3 lists authorized services for this role

Table 13- Services Authorized for Roles

### 9.4 MITIGATION OF ATTACKS

Other Attacks	Mitigation Mechanism	Specific Limitations
Simple Power Analysis	Counter Measures against SPA	N/A
Differential Power Analysis	Counter Measures against DPA	N/A
Timing Attacks	Counter Measures against TA	N/A
Fault Induction	Counter Measures against FI	N/A

Table 14 - Mitigation of Attacks

## 10 REFERENCES

The following standards are referred to in this Security Policy.

Acronym	Full Specification Name
[FIPS140-2]	FIPS 140-2 Security Requirements for Cryptographic modules, May 25, 2001
[JCRE]	Java Card™ 2.2.1 Runtime Environment Revision 1.0, 18 May 2000
[JCAPI]	Java Card™ 2.2.1 Application Programming Interface Revision 1.0, 18 May 2000
[JCVM]	Java Card™ 2.2.1 Virtual Machine Revision 1.0, 18 May 2000
[GP]	GlobalPlatform Card Specification, Version 2.1.1, March 2003
[EJAS]	eToken Java Applet V1.1 (FIPS) Specifications, Version 1.24, 26/03/2008 (File name: eToken Java Applet Specification.doc)
[EJCA]	eToken Applet FIPS Certification, Version 1.7, 12-Oct-2008 (File name: eToken Applet FIPS 140-2 PKI On Card Application.doc)
[7816-4]	ISO/IEC 7816-4, Second edition 2005-01-15, Identification cards – Integrated circuit(s) cards with contacts – Part 4: Interindustry commands for interchange
[USB20]	Universal Serial Bus Revision 2.0 specification See <a href="http://www.usb.org/developers/docs/">http://www.usb.org/developers/docs/</a>

Table 15 - References

## 11 ACRONYMS AND DEFINITIONS

Acronym	Definition
AdvX	Advance Crypto
API	Application Programming Interface
AVR	Automatic Voltage Regulation
CA	Card Administrator
CH	Card Holder (user)
CM	Cryptographic Module
CSP	Critical Security Parameter
DRNG	Deterministic Random Number Generator
GP	GlobalPlatform
HRNG	Hardware Random Number Generator
ISD	Issuer Security Domain
KSSK	Key Secure Storage Key
KID	Key Identifier, see [GP]
KVN	Key Version Number, see [GP]
LCD	Liquid Crystal Display
OTP	One Time Password
PKCS	Public Key Cryptography Standard
PSSK	PIN Secure Storage Key
RNG	Random Number Generator
SO	Security Officer (administrator)
SM	Secure Messaging
SSD	Supplementary Security Domain

Table 16 - Acronyms and Definitions

[END OF THE DOCUMENT]