eToken

FIPS 140-2 Level 3
Non-Proprietary Security Policy

DOCUMENT NUMBER:	002-010837-001
AUTHOR:	Chris Brych / Danny Tabak
DEPARTMENT:	Program Management R&D
LOCATION OF ISSUE:	Ottawa
DATE ORIGINATED:	July 9, 2012
REVISION LEVEL:	B
REVISION DATE:	July 3 , 2013
SUPERSESSION DATA:	A
SECURITY LEVEL:	FIPS 140-2 Level 3

SafeNet, Inc. reserves the right to make changes in the product or its specifications mentioned in this publication without notice. Accordingly, the reader is cautioned to verify that information in this publication is current before placing orders. The information furnished by SafeNet, Inc. in this document is believed to be accurate and reliable. However, no responsibility is assumed by SafeNet, Inc. for its use, or for any infringements of patents or other rights of third parties resulting from its use.

PREFACE

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

- The SafeNet internet site contains information on the full line of security products at www.safenet-inc.com.
- For answers to technical or sales related questions please refer to the contacts listed below or on the SafeNet internet site at http://www.safenet-inc.com/contact-us/

SafeNet Contact Information:	
SafeNet, Inc. (Corporate Headquarters)	4690 Millennium Drive Belcamp, Maryland 21017 USA **Telephone:** 410-931-7500 **TTY Users:** 800-735-2258 **Fax:** 410-931-7524
SafeNet Sales:	
U.S.	(800) 533-3958
International	(410) 931-7500
SafeNet Technical Support:	
U.S.	(800) 545-6608
International	(410) 931-7520
SafeNet Customer Service:	
U.S.	(866) 251-4269
EMEA	+44 (0) 1276 60 80 00
APAC	852 3157 7111

Table of Contents

Table of Tables

Table of Figures

1 Introduction

1.1 General

This document defines the Security Policy for the SafeNet, Inc. eToken single-chip module.

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

The Module contains a Java Card applet suite implementing the SafeNet eToken functionality running on a GlobalPlatform Java Card operating system running on an INSIDE Secure microcontroller.

The primary purpose of the Module is to provide security functions for the host application. This includes authentication, digital signing, encryption and decryption.

The applications work with the Module through the SafeNet Authentication Client middleware: (SAC). The SafeNet eToken Applet Suite is the on-card representative of the Card Holder. This provides a variety of SAC services to the Card Holder.

This Security Policy is organized as follows:

- Module Overview and general specification (Sections 1-4)
- Platform FIPS 140-2 specification (Section 5)
- eToken Applet Suite FIPS 140-2 specification (Section 6)
- Other Module level FIPs 140-2 compliance information (Sections 7- 10)
- Lists of acronyms and references

This organization reflects the structure of the Module and the use of a previously validated platform and its associated specification and Security Policy information. The total set of CSPs, roles, authentication methods and services is the superset of the Platform information in Section 5 and the eToken Applet Suite information in Section 6.

1.2 High-Level Module Architecture

The Module is a single chip micro-controller. The Module architecture consists of three high-level architectural components:

- Platform (GlobalPlatform operational environment, inclusive of Card Manager and Java Card API)
- SafeNet eToken Applet
- Microsoft Smart Card Minidriver compliant Applet (has no security functionality)

The purpose of the GlobalPlatform operational environment is to provide common smart card operational environment facilities and services in accordance with the GlobalPlatform Specification [Global Platform]. The Card Manager manages the Applet Suite Life Cycle state and card content. The Java Card API provides a library of standard smartcard functionality.

2 FIPS 140-2 Security Levels

The FIPS 140-2 security levels for the Module are as follows:

Security Requirement	Security Level
Cryptographic Module Specification	3
Cryptographic Module Ports and Interfaces	3
Roles, Services, and Authentication	3
Finite State Model	3
Physical Security	4
Operational Environment	N/A
Cryptographic Key Management	3
EMI/EMC	3
Self-Tests	3
Design Assurance	3
Mitigation of Other Attacks	3

Table 1 – Security Level of Security Requirements

3 Hardware and Physical Cryptographic Boundary

The Module is a single-chip implementation that meets commercial-grade specifications for power, temperature, reliability, and shock/vibrations. The Module uses standard passivation techniques and is protected by passive shielding (metal layer coverings opaque to the circuitry below) and active shielding (a grid of top metal layer wires with tamper response). A tamper event detected by the active shield places the Module permanently into the “Tamper is detected” error state.

The Module is designed to be embedded into a mobile device, for example, a smart card or USB token. The physical form of the Module is represented in Figure 1. In production use, the module is wire-bonded to a frame connected to the ports and interfaces. The Module will be enclosed in epoxy, for example, as a smart card module or in chip packaging such as SOIC8 or QFN44.

The Module hardware and physical cryptographic boundary is pictured below. The chip is approximately 2mm square.

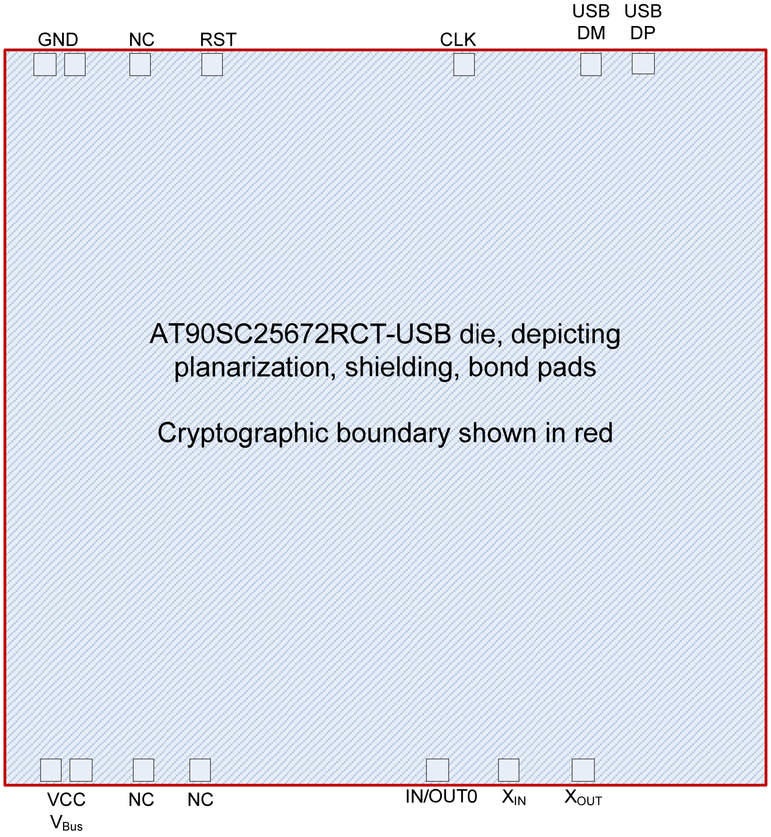
GND
NC
RST
CLK
USB DM
USB DP
AT90SC25672RCT-USB die, depicting planarization, shielding, bond pads
Cryptographic boundary shown in red
VCC V_{Bus}
NC
NC
IN/OUT0
X_{IN}
X_{OUT}

Figure 1 – Hardware and Physical Cryptographic Boundary

3.1 Ports and Interfaces

The Module functions as a slave device to process and respond to commands.

This module provides a contact interface that is fully compliant with ISO/IEC 7816.

Interface	Description
CLK	External Clock signal
GND	Ground
VCC	Supply Voltage Power
IN/OUT0	Input/Output
RST	External Reset signal

Table 2 – ISO/IEC 7816 Physical Interfaces

This module supports two transmission half-duplex oriented protocols: T=0 and T=1.

Up to 256 bytes of data can be exchanged through one TPDU command.

The I/O ports of the platform provide the following logical interfaces:

Interface	ISO/IEC 7816
Data In	IN/OUT0
Data Out	IN/OUT0
Status Out	IN/OUT0
Control In	INOUT0, CLK and RST

Table 3 – ISO/IEC 7816 Logical Interfaces

This module provides a contact interface that is fully compliant with USB 2.0.

Interface	Description
USBDM	USB D- differential data
USBDP	USB D+ differential data
V_{Bus}	Power supply input
GND	Ground (reference voltage)
LED	LED indicator

Table 4 – USB Physical Interfaces

The I/O ports of the platform provide the following logical interfaces:

Interface	USB
Data In	USBDM, USBDP
Data Out	USBDM, USBDP
Status Out	USBDM, USBDP, LED
Control In	USBDM, USBDP, V_{Bus}

Table 5 – USB Logical Interfaces

4 Firmware and Logical Cryptographic Boundary

Figure 2 depicts the Module block diagram, including the relationship of Module hardware and firmware, and interactions with the logical interfaces.

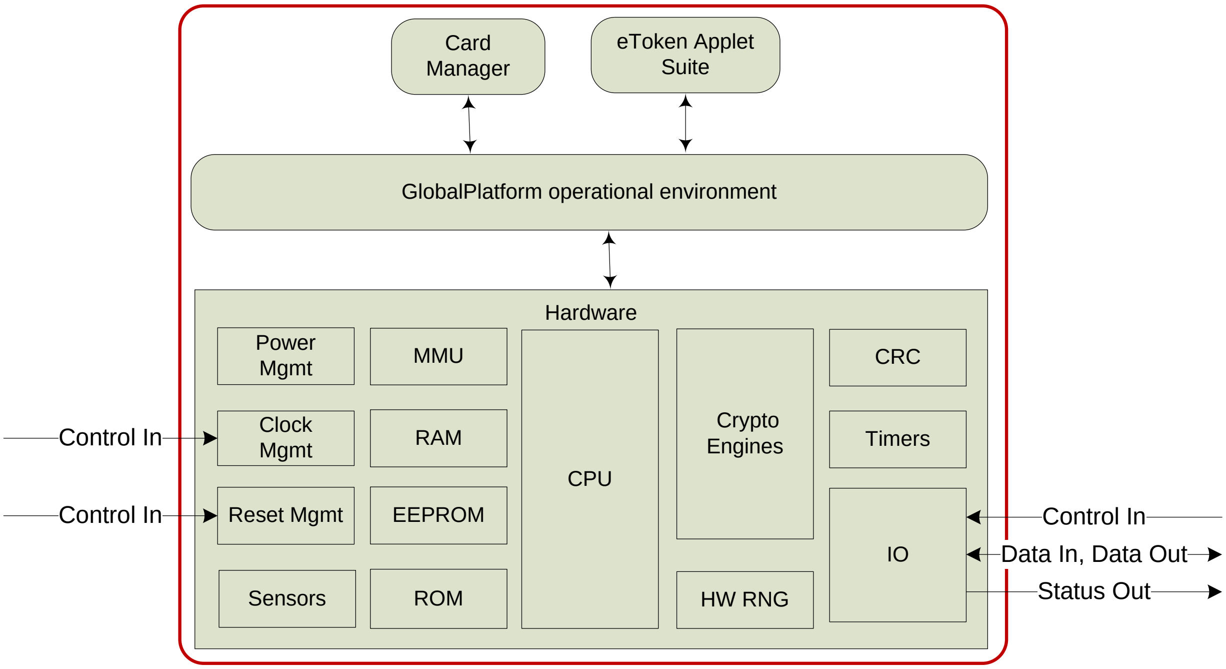

Figure 2 - Module Block Diagram

- Memory sizes: 72 KB EEPROM; 256 KB ROM; 8 KB RAM

4.1 Versions

The hardware and firmware version numbers for the Module are provided below:

Firmware: Athena IDProtect 0106.0113.2109 with SafeNet eToken Applet Suite 1.2.9
Hardware (single chip): Inside Secure AT90SC25672RCT-USB

5 Platform 140-2 Specification

5.1 Cryptographic Functionality

The Module implements the FIPS Approved and Non-FIPS Approved but allowed cryptographic functions listed in tables below.

Algorithm	Description	Certificate #
DRBG	[SP800-90] DRBG_HASH	98
SHA	[FIPS180-3] Secure Hash Standard compliant one-way (hash) algorithms. The Module supports SHA-1, SHA-224, SHA-256. (SHA-384 and SHA-512 are not callable by any module service.)	1465
TDEA	[SP800-67] Triple Data Encryption Algorithm. The Module supports the 2-Key and 3-Key options; in ECB and CBC modes.	1087
TDEA MAC	[FIPS113] TDEA Message Authentication Code. Vendor affirmed, based on validated TDEA.	Vendor Affirmed (TDEA Certificate #1087)
AES	[FIPS197] Advanced Encryption Standard algorithm. The Module supports AES-128, AES-192 and AES-256; in ECB and CBC modes.	1654
RSA	[FIPS186-2] RSA signature generation and verification. The Module supports [PKCS#1] version 1.5 and 2.1 and supports 1024- and 2048-bit RSA keys.	824

Table 6 – FIPS Approved Cryptographic Functions

Algorithm	Description
HW RNG	Hardware RNG; minimum of 64 bits per access. The HW RNG output is used to seed the FIPS approved DRBG.
AES-CMAC[1]	[SP800-38B] AES CMAC (untested). The module supports AES CMAC with AES-128, AES-192 and AES-256 for GlobalPlatform SCP03.
AES	[AESKeyWrap] AES Key Wrap. The Module supports AES key wrapping with AES-128, AES-192 and AES-256 for GlobalPlatform SCP03.
RSA Key Gen	RSA key pair generation, 1024- and 2048-bit keys.
RSA Key Decrypt	The module supports non-SP 800-56B compliant RSA key decapsulation using 1024- and 2048-bit keys.

Table 7 – Non-FIPS Approved But Allowed Cryptographic Functions

NOTE: [1] The AES CMAC implementation is embedded within the SCP functionality and was not CAVP validated, but is not required for secure operation of the module or to meet FIPS requirements.

5.2 Critical Security Parameters

Platform-specific CSPs are specified below:

Key	Description / Usage
OS-DRBG_SEED	384 bit random value from HW RNG used to seed the DRBG
OS-DRBG_STATE	880 bit value of current DRBG state
OS-MKEK	AES-128 key used to encrypt all secret and private key data stored in the EEPROM
OS-PKEK	AES-128 key used to encrypt all PINs stored in the EEPROM
ISD-KENC	AES-128, 192 or 256 key used by the CM role to derive ISD-SENC as specified by GlobalPlatform SCP03
ISD-KMAC	AES-128, 192 or 256 key used by the CM role to derive ISD-SMAC and ISD-SRMAC as specified by GlobalPlatform SCP03
ISD-KDEK	AES-128, 192 or 256 data decryption key used by the CM role to decrypt CSPs as specified by GlobalPlatform SCP03
ISD-SENC	AES-128, 192 or 256 session encryption key used by the CM role to encrypt / decrypt Secure Channel Session data as specified by GlobalPlatform SCP03
ISD-SMAC	AES-128, 192 or 256 session MAC key used by the CM role to verify inbound Secure Channel Session data integrity as specified by GlobalPlatform SCP03
ISD-SRMAC	AES-128, 192 or 256 session MAC key used by the CM role to verify outbound Secure Channel Session data integrity as specified by GlobalPlatform SCP03

Table 8 - Module Critical Security Parameters (Platform)

5.3 Public Keys

Platform-specific public keys used by the Module are specified below:

Key	Description / Usage
ISD-DAP	RSA 1024 GlobalPlatform Data Authentication Public Key used to verify the signature of packages loaded into the Module.

Table 9 - Public Keys (Platform)

5.4 Error States

The Module has three error states:

Error state	Description
Tamper is detected	The hardware detects that it has been tampered with and will not power-on. It is not possible to exit this state (it persists even after a reset: POWER_OFF then POWER_ON).
CM is mute	CM enters a state that forbids the execution of any further code. It is possible to exit this state with a reset: POWER_OFF then POWER_ON.
ISD is terminated	The CSPs are zeroized and the Card Life Cycle state is set to TERMINATED. Only the GET DATA APDU can be processed. It is not possible to exit this state (it persists even after a reset: POWER_OFF then POWER_ON).

Table 10 – Error States

There also exists a transient error state when the module has received an unsupported, unrecognized or improperly formatted command. The Module returns an error status word as specified in ISO/IEC 7816-4, exits the error state and returns to an idle state awaiting the next command.

5.5 Key and CSP Zeroization

The Module offers services to zeroize all CSPs in EEPROM:

- OS-MKEK and OS-PKEK are zeroized when the CM enters the “ISD is terminated” error state. The Card Manager can achieve this explicitly using the SET STATUS command, or a severe security event may occur (failure of the integrity check on code located in EEPROM or of a CSP). By zeroizing these keys all other CSPs stored in EEPROM are made irreversibly undecipherable.

The Module offers services to zeroize all CSPs in RAM:

- Card Reset zeroizes all CSPs in RAM as the data values held in RAM are lost at power-off and RAM is actively cleared to zero at the next power-on.
- When a Secure Channel Session is closed for any reason other than Card Reset, the CM overwrites the session keys with zeroes.

By zeroizing OS-MKEK and OS-PKEK and performing a Card Reset all CSPs stored in the Module are effectively destroyed.

5.6 Self-Tests

5.6.1 Power-On Self-Tests

Each time the Module is powered on it tests that the cryptographic algorithms still operate correctly and that sensitive data have not been damaged. Power-on self–tests are available on demand by power cycling the Module.

On power-on or reset, the Module performs the self-tests described in Table 11 below. All KATs must be completed successfully prior to any other use of cryptography by the Module.

The error state entered by the Module in case of self-tests failure is "CM is mute".

Test Target	Description
Firmware Integrity	16 bit CRC performed over all code located in EEPROM. This integrity test is not required or performed for code stored in masked ROM code memory.
DRBG	Performs the DRBG KAT and health test monitoring functions.
SHS	Performs separate SHA-1 and SHA-256 KATs.
TDEA	Performs separate encrypt and decrypt KATs using 3-Key TDEA in CBC mode.
AES	Performs separate encrypt and decrypt KATs using an AES-128 in CBC mode.
RSA	Performs a pairwise consistency KAT (RSA PKCS#1 sign and verify) using an RSA 2048 bit key pair.

Table 11 – Power-On Self-Test

5.6.2 Conditional Self-Tests

Each time the Module is powered on it performs the DRBG health test monitoring functions.

On every generation of 64 bits of random data by the HW RNG the Module performs a stuck fault test to assure that the output is different from the previous value. In case of failure the Module enters the "CM is mute" error state.

On every generation of 256 bits of random data by the DRBG, the Module performs a stuck fault test to assure that the output is different from the previous value. In case of failure the Module enters the "CM is mute" error state.

When an asymmetric key pair is generated (for RSA) the Module performs a Pairwise Consistency Test (PCT). In case of failure the invalid key pair is zeroized and the Module enters the "CM is mute" error state.

When a signature is generated (for RSA) the Module performs a PCT using the associated public key. A PCT is also performed during the RSA KAT.

Every CSP is protected with a 16 bit CRC. The integrity is checked when a CSP is used. In case of failure the Module enters the "ISD is terminated" error state.

When new firmware is loaded into the Module using the LOAD command, the Module verifies the integrity of the new firmware by verifying an RSA signature of the new firmware using the ISD-DAP RSA 1024 public key; the new firmware in this scenario is signed by an external entity using the private key corresponding to ISD-DAP. If the signature verification fails the Module returns an error and does not load the firmware.

5.7 Platform Roles, Authentication and Services

Table 12 lists all Platform-specific operator roles supported by the Module.

The Module does not support a maintenance role.

The Module supports concurrent operators on multiple Logical Channels. However, neither the ISD nor eToken Applet Suite are multi-selectable (they cannot be simultaneously selected on two Logical Channels). Therefore there cannot be two concurrent operators using the ISD nor two concurrent operators using the eToken Applet Suite. It is however possible to select the ISD on the Basic Channel and eToken Applet Suite on Supplementary Channel 1 (or vice versa).

The Module clears previous authentications on power cycle.

5.7.1 **Platform Roles**

Platform-specific roles provided by the Module are described in Table 12.

Role ID	Role Description
CM	Card Manager (the Cryptographic Officer role for FIPS 140-2 validation purposes). This role is responsible for managing the security configuration of the Module, including issuance and management of Module data via the ISD. The CM is authenticated using ISD-SENC as specified by GlobalPlatform SCP03. Once authenticated, the Card Manager is able to execute the services provided by the ISD in a Secure Channel Session (see [GlobalPlatform] for more details).

Table 12 – Platform-specific Roles Description

The Module includes the Issuer Security Domain, which allows the Card Manager to manage the operating system and content.

5.7.2 **Platform Authentication**

The GlobalPlatform SCP03 authentication method is performed when the EXTERNAL AUTHENTICATE service is invoked after successful execution of the INITIALIZE UPDATE command.

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. The default threshold is 80.

The ISD-KENC and ISD-KMAC keys are used along with other information to derive the ISD-SENC and ISD-SMAC / ISD-SRMAC keys, respectively. The ISD-SENC key is used to create a cryptogram; the external entity participating in the mutual authentication also creates this cryptogram. Each participant compares the received cryptogram to the calculated cryptogram and if this succeeds, the two participants are mutually authenticated (the external entity is authenticated to the Module in the CM role).

Based on the shortest length of ISD-SENC and ISD-SMAC / ISD-SRMAC (AES-128), the Module's security strength is determined to be 128 bits:

- The probability that a random attempt at authentication will succeed is 1/2^128, less than one in 1,000,000 as required for FIPS 140-2.
- Based on the maximum count value of the failed authentication blocking mechanism, the probability that a random attempt will succeed over a one minute period is 255/2^128, less than 1 in 100,000 as required by FIPS 140-2.

5.8 Platform Services

All services implemented by the Platform are listed in the tables below, along with the usage of CSPs by each service. Table 13 lists all unauthenticated services implemented by the platform. Table 14 lists all authenticated services implemented by the platform.

Service	Description
Card Reset (Self-test)	Power cycle the Module by removing power from the module and then supplying it. On the first Card Reset, the Module generates OS-MKEK and OS-PKEK. On every Card Reset, the Module generates OS-DRBG_SEED and OS-DRBG_STATE from the HW RNG and invokes the Power-On Self-Tests.
INITIALIZE UPDATE	Initialize the Secure Channel Session; to be followed by EXTERNAL AUTHENTICATE. Uses OS-MKEK to decrypt ISD-KENC and ISD-KMAC for use. Uses ISD-KENC and ISD-KMAC to derive ISD-SENC and ISD-SMAC / ISD-SRMAC. Uses ISD-SENC to generate the card cryptogram.
EXTERNAL AUTHENTICATE	Authenticates the operator and establishes a Secure Channel Session. Must be preceded by a successful INITIALIZE UPDATE. Uses ISD-SMAC to verify the command MAC, and ISD-SENC to verify the host cryptogram.
GET DATA	Retrieve a single data object. Uses no CSPs.
MANAGE CHANNEL	Open a Supplementary Logical Channel. Uses no CSPs.
SELECT	Select an applet Uses no CSPs.

Table 13 - Unauthenticated Services and CSP Usage

Service	Description	CM
INSTALL	Install an applet to EEPROM. Uses ISD-SENC and ISD-SMAC / ISD-SRMAC in the Secure Channel Session.	X
LOAD	Load an applet code to EEPROM. Uses ISD-SENC and ISD-SMAC / ISD-SRMAC in the Secure Channel Session. Uses ISD-DAP to verify the integrity of the loaded firmware.	X
PUT KEY	**SCP03 key set** Load a Card Manager SCP03 key set to EEPROM. Uses ISD-SENC and ISD-SMAC / ISD-SRMAC in the Secure Channel Session. Uses OS-MKEK to decrypt ISD-KDEK for use. Uses ISD-KDEK to decrypt the loaded SCP03 key set. Creates a new or replaces the existing ISD-KENC, ISD-KMAC and ISD-KDEK SCP03 key set. Uses OS-MKEK to encrypt ISD-KENC, ISD-KMAC and ISD-KDEK for storage. **ISD DAP key** Load a Card Manager DAP key to EEPROM. Uses ISD-SENC and ISD-SMAC / ISD-SRMAC in the Secure Channel Session. Replace the existing ISD-DAP key.	X
DELETE	**Card content** Delete an applet and/or applet code from EEPROM. Uses ISD-SENC and ISD-SMAC / ISD-SRMAC in the Secure Channel Session. **SCP03 key set** Delete a Card Manager SCP03 key set from EEPROM. Uses ISD-SENC and ISD-SMAC / ISD-SRMAC in the Secure Channel Session. Zeroizes an ISD-KENC, ISD-KMAC and ISD-KDEK SCP03 key set.	X
GET STATUS	Retrieve information about the Module. Uses ISD-SENC and ISD-SMAC / ISD-SRMAC in the Secure Channel Session.	X
SET STATUS	Modify the card or applet Life Cycle state. Uses ISD-SENC and ISD-SMAC / ISD-SRMAC in the Secure Channel Session.	X
STORE DATA	Add or change data in the Card Manager data store. Uses ISD-SENC and ISD-SMAC / ISD-SRMAC in the Secure Channel Session.	X

Table 14 –Platform (Card Manager) Authenticated Services and CSP Usage

5.9 Approved Mode Indicator

The Module always runs in the Approved mode of operation once configured as described in Section 10.2.

To obtain the indicator of the approved mode of operation, two independent steps are performed.

To verify the firmware operating system and the applet suite, SELECT the ISD, send a GET DATA command with the CPLC Data tag '9F7F' and verify that the returned data contains fields as follows.

Data Element	Length	Value	Associated Version
IC type	2	'0106'	Smart Card Chip Version
Operating system release date	2	'0113'	Firmware Version Part 1
Operating system release level	2	'2109'	Firmware Version Part 2

Table 15 – Versions and Mode of Operations Indicators

The second step is to run the SAC status function, a command sequence that traverses the filesystem and validates that the configuration is compliant with system and FIPS 140-2 requirements. The module can only be initialized and configured using the SAC, as described in Section 10.2.

6 eToken Applet Suite Specification

The eToken Applet Suite includes two applets: a Microsoft Smart Card Minidriver applet, and the eToken applet. The Minidriver Applet allows Microsoft CSP or CNG compliant middleware to identify the card by retrieving fixed data without authentication. The Minidriver Applet stores no CSPs, and provides no roles, authentication or cryptographic services.

The eToken applet provides configurable authentication, access control and secure data management services. The eToken applet uses the cryptographic algorithm and key management functions implemented by the Platform. No eToken Applet Suite CSPs can be exported from the Module.

6.1 Critical Security Parameters

The eToken Applet Suite CSPs are described in logical groups below.

Secure Messaging Key Set

The Secure Messaging Key Set comprises five 3-key TDEA keys initially supplied by the host application during eToken file system initialization:

- ID_AUTH_OP: MAC key used to authenticate the ESO or CH role using a challenge-response protocol.
- ID_SM_ENC_IN_OP: Decryption key used to decrypt data sent by the host application as a part of the operator operations.
- ID_SM_MAC_IN_OP: MAC key used to guarantee integrity on any data sent by the host application as a part of the operator operations. This also prevents replay attack as each MAC calculation uses an incrementing counter.
- ID_SM_ENC_OUT_OP: Encryption key used to encrypt data sent by the Module as a part of the operator operations.
- ID_SM_MAC_OUT_OP: MAC key used to guarantee integrity on any data sent by the Module as a part of the operator operations. This also prevents replay attack as each MAC calculation uses the host challenge.

The Module implements six instances of the Secure Messaging Key Set: two for the ESO role and two for the CH role. For each role, one key set is used for normal operation (i.e. authentication of the operator, and encryption and integrity of further operator operation); the second key set is used during Secure Messaging Key Set updates

File System Re-initialization Key

The Module may incorporate a MAC key ID_TEST_REINIT, used as a secondary authentication token to perform the eToken File System Re-initialization service. This key is optional.

If the key exists, usage of this key may be available to CH role, ESO role or both. If the key is available in a particular role, the role may perform file system reinitialization.

File System Re-initialization – Applet Start Key Set

The Applet Start key comprises two 3-key TDEA keys – ASK_MAC key and ASK_ENC encryption Key. The ASK_MAC Key is used to protect the integrity and authenticate the File System Re-initialization and Change Applet Key services. The ASK_ENC key encrypts the new Key Applet Start Key Set during the Change Applet Key service. In the case where File System Re-initialization Key does not exist, it is possible to perform File System Re-Initialization using the Applet Start Key Set.

Secondary Authentication Secret

This CSP is a 3-key TDEA MAC key (SEC_AUTH) for use in a challenge response protocol. The Secondary Authentication Secret is used as the second level of authentication for cryptographic operations with AES and TDES keys and RSA key pairs.

CH RSA Key Pair(s)

The eToken Applet Suite implements 0 to n (limited only by available memory) RSA-1024 or -2048 key pairs (CH_RSA_KEY_PRIVATE, CH_RSA_KEY_PUBLIC) used by the CH role in the *Perform Security Operation* service. RSA keys may be used for digital signatures as well as for key decapsulation. However, the key decryption mechanism is not used to establish keys into the module, only to provide key decryption as a service to the caller.

CH Symmetric Keys

The eToken Applet Suite implements 0 to n (limited only by available memory) AES-128, AES-192, AES-256 or 3-key TDEA keys (CH_SYMMETRIC) for use by CH role in the *Perform Security Operation* service.

6.2 eToken Applet Roles

Applet Suite-specific roles provided by the Module are described in Table 16 – Applet-specific Roles description.

This Module 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.

Role ID	Role Description
CH	Card Holder (User role for FIPS 140-2 validation purposes). The Card Holder role is defined in the context of the SafeNet eToken Applet Suite and is used to protect keys and data owned by the Card Holder.
ESO	eToken Security Officer This role is responsible for managing the life cycle of the Card Holder (CH).
FSI	File System Initializer. This role is responsible for the eToken Applet Suite File System Re-initialization in the case where the File System Re-initialization Key does not exist. In additional to the File System initialization, this role is capable of changing the Applet Start Key Set values.

Table 16 – Applet-specific Roles description

The ESO or CH authenticates by opening a SM session with the eToken Applet using a challenge response mechanism with the ID_AUTH_OP key, which has an associated error counter in the range one to 15 with default value 15.

The FSI role is authenticated using the ASK_MAC key and utilizing a challenge response mechanism.

In all cases, the minimum challenge size is a single 64-bit block, therefore the probability of false authentication is 1/2^64 or approximately 5.4E-20.

For ESO or CH authentication, the error counter limits the probability of false authentication in a one minute period to 15/2^64 or approximately 8.1E-19

For FSI authentication, the serial communications rate limits the maximum rate of authentication attempts in a one minute period to 1000 attempts, therefore the probability of false authentication is 1000/2^64 or approximately 5.4E-17

6.3 Services

Service	Description	ESO	CH	FSI
Operator Logon	Authenticate the CH or ESO role. Uses ID_AUTH_OP key from Secure Messaging Key Set to authenticate operator.	X	X	
Credential Change	Change the current Secure Messaging Key Set. Uses ID_SM_ENC_IN_OP and ID_SM_MAC_IN_OP from Secure Messaging Key Set to decrypt and verify MAC value on new credentials.	X	X	
CH Unlocking	Unlock the CH Key Set. The ESO provides the new CH key set. All CH data and other keys remain untouched. Uses ID_SM_ENC_IN_OP and ID_SM_MAC_IN_OP from Secure Messaging Key Set to decrypt and verify MAC value on new CH key set.	X		
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 set. All CH data and other keys are zeroized. Uses ID_SM_ENC_IN_OP and ID_SM_MAC_IN_OP from Secure Messaging Key Set to decrypt and verify MAC value on new CH key set.	X		
File System Re-initialization	The data in the SafeNet eToken Applet are cleared and the eToken file system is re-initialized. Zeroizes all keys stored in the eToken file system. If ID_TEST_REINIT key is present in the module, requires this key to authenticate usage of this service. The ID_TEST_REINIT key may be available in CH role, ESO role or both. If ID_TEST_REINIT key is not present in the module, this service may be executed from the FSI role. ASK_ENC key from Applet Start Key set is used to authenticate FSI role.	X	X	X
Generate CH RSA Key Pair	Generate a CH RSA Key Pair. Generates RSA Key Pair, including CH_RSA_KEY_PRIVATE and CH_RSA_KEY_PUBLIC keys.		X	
Create Secondary Authentication Secret	Import Secondary Authentication Secret SEC_AUTH. Updates SEC_AUTH. Uses ID_SM_ENC_IN_OP and ID_SM_MAC_IN_OP from Secure Messaging Key Set to decrypt and authenticate the new value.		X	

Service	Description	ESO	CH	FSI
Perform Security Operation	Use a CH RSA Key Pair to generate/verify signatures or decryption of symmetric keys, or use AES and TDES keys for encryption/decryption. Key decryption does not establish a CSP into the Module. Uses CH_RSA_KEY_PRIVATE, CH_RSA_KEY_PUBLIC or CH_SYMMETRIC keys, depending on operation type.		X	
Store and read data	Store and read data objects. Uses the Secure Messaging key set to encrypt/decrypt and authenticate data on input/output.		X	
Import symmetric keys	Import AES and TDES symmetric keys into the module using secure messaging. Writes CH_SYMMETRIC keys. Uses the Secure Messaging key set to encrypt/decrypt and authenticate keys on input/output.		X	
Import RSA key pair	Import RSA key pair. Writes CH_RSA_PRIVATE_KEY. Uses the Secure Messaging key set to encrypt/decrypt and authenticate keys on input/output.		X	
Manage filesystem	Create files, delete files, admin files, list directories, resize filesystem, wipe filesystem. Uses the Secure Messaging key set to encrypt/decrypt and authenticate commands on input/output.	X	X	
Manage objects	Admin object, get object info, list objects. Uses the Secure Messaging key set to encrypt/decrypt and authenticate commands on input/output.	X	X	
Export public key	Export public key. The service does not utilize any CSPs.	X	X	X
Set/read volatile data	Set or read application-specific volatile data for the applet	X	X	X

Table 17 – Applet Suite Services and CSP Usage

In addition to the authenticated services, the module provides the Mindriver Information Service when the Minidriver Applet is selected. This service is available without authentication. It provides non-security relevant information used by the host operating system to recognize the module.

The Minidriver Information Service does not utilize any CSPs.

7 Operational Environment

The Module is designated as a limited operational environment under the FIPS 140-2 definitions. The Module includes a firmware load service to support necessary updates. New firmware versions within the scope of this validation must be validated through the FIPS 140-2 CMVP. Any other firmware loaded into this Module is out of the scope of this validation and requires a separate FIPS 140-2 validation.

8 Electromagnetic Interference and Compatibility (EMI/EMC)

The 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.

9 Mitigation of Other Attacks Policy

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 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. This chip is Common Criteria certified; more information is available her http://www.commoncriteriaportal.org/products/.

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.

10 Security Rules and Guidance

10.1 Security Rules

The Module implementation enforces the following security rules:

- No additional interface or service is implemented by the Module which would provide access to CSPs.
- Data output is inhibited during key generation, self-tests, zeroization, and error states.
- There are no restrictions on which CSPs are zeroized by the zeroization service.
- The Module does not support manual key entry, output plaintext CSPs or output intermediate key values.
- Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the Module.
- Application loading is one of the services provided by the operating system that is restricted to the Card Manager: a Secure Channel Session must be open between the external operator (more precisely the middleware the CM is using to manage content) and the ISD. Application loading is protected by ISD-DAP.
- The application loading service is available before and after Module issuance.
- The CM is responsible for application personalization and lifecycle management following GlobalPlatform.

10.2 Initial configuration of the module

The Module requires configuration using SafeNet Authentication Client tools. These tools enforce Module configuration compliant with system and FIPS 140-2 requirements.

11 Acronyms and References

Acronym	Full Specification Name
API	Application Programming Interface
CM	Card Manager, see [GlobalPlatform]
CSP	Critical Security Parameter
DAP	Data Authentication Pattern, see [GlobalPlatform]
DPA	Differential Power Analysis
HID	Human Interface Device
IC	Integrated Circuit
ISD	Issuer Security Domain, see [GlobalPlatform]
KAT	Known Answer Test
PCT	Pairwise Consistency Test
PKI	Public Key Infrastructure
SAC	SafeNet Authentication Client middleware.
SCP	Secure Channel Protocol, see [GlobalPlatform]
SPA	Simple Power Analysis

Table 18 - Acronyms

Acronym	Full Specification Name
[FIPS113]	Computer Data Authentication
[FIPS140-2]	Security Requirements for Cryptographic Modules
[FIPS180-3]	Secure Hash Standard (SHS)
[FIPS186-2]	Digital Signature Standard (DSS)
[FIPS186-3]	Digital Signature Standard (DSS)
[FIPS197]	Advanced Encryption Standard (AES)
[PKCS#1]	RSA Cryptography Standard, Version 1.5 and 2.1
[SP800-56A]	Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography
[SP800-67]	Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher
[SP800-89]	Recommendation for Obtaining Assurances for Digital Signature Applications
[SP800-90]	Recommendation for Random Number Generation Using Deterministic Random Bit Generators
[SP800-131A]	Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths

Table 19 – References (Cryptography)

Acronym	Full Specification Name
[JavaCard]	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
[GlobalPlatform]	GlobalPlatform Consortium: GlobalPlatform Card Specification 2.1.1, March 2003, http://www.globalplatform.org GlobalPlatform Consortium: GlobalPlatform Card Specification 2.1.1 Amendment A, March 2004 GlobalPlatform Consortium: GlobalPlatform Card Technology, Secure Channel Protocol 03, Card Specification v 2.2 – Amendment D, Version 1.1, September 2009
[ISO7816]	ISO/IEC 7816-1: 1998 Identification cards -- Integrated circuit(s) cards with contacts -- Part 1: Physical characteristics ISO/IEC 7816-2:2007 Identification cards -- Integrated circuit cards -- Part 2: Cards with contacts -- Dimensions and location of the contacts ISO/IEC 7816-3:2006 Identification cards -- Integrated circuit cards -- Part 3: Cards with contacts -- Electrical interface and transmission protocols ISO/IEC 7816-4:2005 Identification cards -- Integrated circuit cards -- Part 4: Organization, security and commands for interchange
[ISO14443]	ISO/IEC 14443-1:2008 Identification cards -- Contactless integrated circuit cards -- Proximity cards -- Part 1: Physical characteristics ISO/IEC 14443-2:2001 Identification cards -- Contactless integrated circuit(s) cards -- Proximity cards -- Part 2: Radio frequency power and signal interface ISO/IEC 14443-3:2001 Identification cards -- Contactless integrated circuit(s) cards -- Proximity cards -- Part 3: Initialization and anticollision ISO/IEC 14443-4:2008 Identification cards -- Contactless integrated circuit cards -- Proximity cards -- Part 4: Transmission protocol
[USB20]	Universal Serial Bus Revision 2.0 specification See http://www.usb.org/developers/docs/

Table 20 – References (Platform)

Acronym	Full Specification Name
[EJAS]	eToken Java Applet Specification Version 1.2 Revision B, Revision 1.13, 08/08/2011

Table 21 – References (Applet)