Valid S/A

IDflex V

FIPS 140-2 Cryptographic Module

Security Policy

Document Version: 1.0

Date: May 2, 2012

Valid S/A, Av. Paulista, 1000, térreo, São Paulo-SP 01310-100, Brazil

Table of Contents

Table of Tables

Table of Figures

1 Introduction

1.1 General

This document defines the Security Policy for the Valid S/A IDflex V Cryptographic Module, hereafter denoted *the Module*. The Module is validated to FIPS 140-2 Level 3.

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.

1.2 High-Level Module Architecture

The Module is a single chip smart card micro-controller. The Module architecture consists of two High-Level architectural components:

- Platform (Card Manager and GlobalPlatform operational environment)
- LASER PKI Applet

The purpose of the GlobalPlatform operational environment is to provide common smart card operational environment facilities and services in accordance with the GlobalPlatform Specification. The Card Manager manages the Applet Life Cycle state.

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

The purpose of the Applet is to provide services to the end user according to the user product requirements.

According to the requirements of FIPS 140-2 both the Platform and the Applet are tested during the FIPS 140-2 conformance testing. The FIPS 140-2 conformance certificate is issued for a Cryptographic Module, which is a combination of the Platform and the Applet. For product upgrades, only FIPS 140-2 validated Applets can be installed on the Module.

1.3 Java Card API

The Java Card API is an internal API utilized by the Applet in order to execute services provided by the Platform. The Java Card API is not exposed to external applications or end users.

1.4 Structure of this Security Policy

As the Module is logically separated into the Platform and the Applet, this Security Policy document logically separates FIPS 140-2 related information items into Platform-specific information (see Sections 5-7) and Applet-specific information (see Sections 8-10). The required FIPS 140-2 information should then be viewed as a superposition of the Platform-specific and Applet-specific Information Items.

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	3
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 smart card. 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.

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

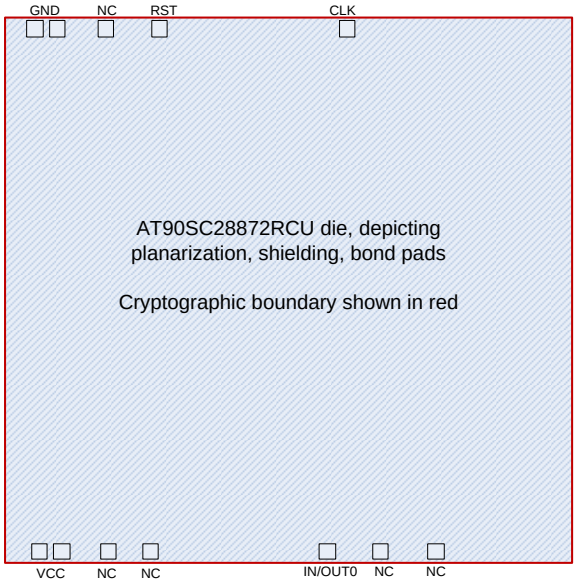


Figure 1 – Hardware and Physical Cryptographic Boundary

3.1 Physical Security Policy

Physical inspection at the Module boundary is not practical after packaging. Physical inspection of Modules for tamper evidence is performed using a lot sampling technique during the assembly process. The Module also provides a transport key to protect against tampering during manufacturing and the protections listed in Section 10 below.

3.2 Ports and Interfaces

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

3.2.1 ISO/IEC 7816

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	IN/OUT0, CLK and RST

Table 3 – ISO/IEC 7816 Logical Interfaces

4 Firmware and Logical Cryptographic Boundary

4.1 Operational Environment

Figure 2 depicts the Module operational environment. The Applet in the figure is the LASER PKI Applet.

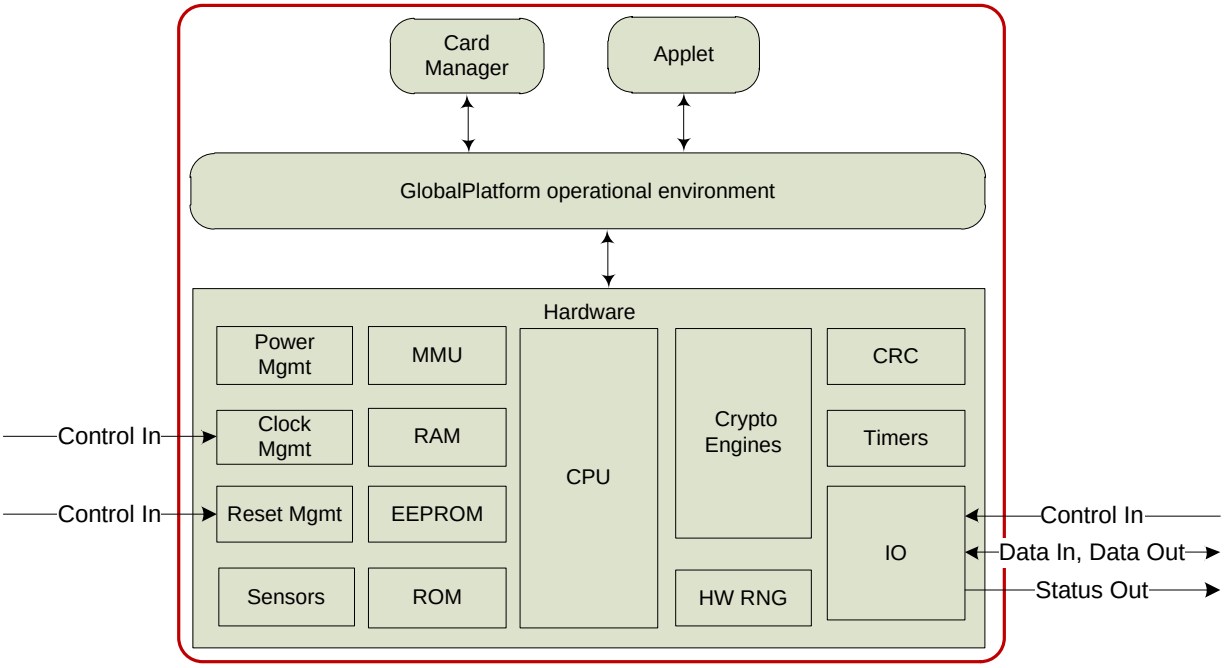


Figure 2 - Module Block Diagram

- 72 KB EEPROM; 256 KB ROM; 8 KB RAM

4.2 Versions

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

Hardware: Inside Secure AT90SC28872RCU Rev. G
Firmware: Valid IDflex V 010B.0352.0005 with LASER PKI Applet 3.0

5 FIPS 140-2 Compliance (Platform)

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. The Module supports a SHA-256 based Hash_DRBG.	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.	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] RSASSA-PSS and RSASSA-PKCS1-v1_5 with 1024- and 2048-bit RSA keys.	824
ECDSA	[FIPS186-3] Elliptic Curve Digital Signature Algorithm. The Module supports the NIST defined P-256 and P-384 curves for signature generation and verification, and key pair generation. The Module also allows domain parameters as supplied by the calling application for signature generation and verification, and key pair generation. The Module performs domain parameter validity testing in accordance with [FIPS186-3] and [SP800-89].	214
ECC CDH	[SP800-56A] The Section 5.7.1.2 ECC CDH Primitive only. The module supports the NIST defined P-256 and P-384 curves.	2

Table 4 – 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	[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	ANSI X9.31 RSA key pair generation (untested). The Module supports 1024- and 2048-bit RSA key generation.

EC Diffie-Hellman	[SP800-131A] EC Diffie-Hellman. The module supports all NIST defined P curves.

Table 5 – Non-FIPS Approved But Allowed Cryptographic Functions

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 EEPROM
OS-PKEK	AES-128 key used to encrypt all PINs
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 6 - 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 7 - 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 command can be processed. It is not possible to exit this state (it persists even after a reset: POWER_OFF then POWER_ON).

Table 8 – 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 the Module performs the self-tests described in Table 9 below. Every Known Answer Test (KAT) must be completed successfully prior to any other use of cryptography by the Module.

The error state entered by the Module in case of power-on 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.

Test Target	Description
SHS	Performs separate SHA-1, SHA-256 and SHA-512 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 KAT (RSA PKCS#1 sign and verify) using an RSA 2048 bit key pair.
ECDSA	Performs a KAT (ECDSA sign and verify) using an ECC P-256 key pair.
ECC CDH	Performs an ECC CDH KAT using an ECC P-256 key pair.

Table 9 – 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 or ECC) 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 or ECDSA) the Module performs a PCT using the associated public key. This PCT is also performed during the RSA and ECDSA 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 a signature of the new firmware using the ISD-DAP 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 Standards Compliance

The Platform and the Applet are compliant with various standards.

The Module implementation is compliant with the following standards for the Platform:

- [JavaCard]
- [GlobalPlatform]
- [ISO7816] Parts 1-4

6 Roles, Authentication and Services (Platform)

6.1 General

Table 10 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 LASER PKI Applet 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 LASER PKI Applet. It is however possible to select the ISD on the Basic Channel and the LASER PKI Applet on Supplementary Channel 1 (or vice versa).

The Module clears previous authentications on power cycle.

6.2 Roles

Platform-specific roles provided by the Module are described in Table 10.

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 10 – Roles (Platform)

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

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

6.3 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 called “velocity checking” by GlobalPlatform. The counter is decremented prior to any attempt to authenticate and is only reset to its threshold (maximum value) upon successful authentication. The Module enters the “ISD is terminated” error state 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 velocity checking 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.

6.4 Services

All services implemented by the Platform are listed in the tables below. Each service description also describes all usage of CSPs by the service.

6.4.1 Unauthenticated Services

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 11 - Unauthenticated Services and CSP Usage

6.4.2 Authenticated Services

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

Service	Description	CM
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 12 – Authenticated Services and CSP Usage

7 Approved Mode of Operation (Platform)

The Module always runs in the Approved mode of operation.

7.1 Verification of Approved Mode

It is possible to verify that the Module is in the approved mode of operation.

SELECT the ISD and 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	Associated Version
IC type	2	'010B'	Inside Secure AT90SC28872RCU Rev. G
Operating system release date	2	'0352'	Firmware Version Part 1
Operating system release level	2	'0005'	Firmware Version Part 2

Table 13 – Versions and Mode of Operations Indicators

8 FIPS 140-2 Compliance (Applet)

8.1 LASER PKI Applet Description

The Module includes an Applet called LASER that performs PKI operations. It is similar to a [SP800-73-3] conformant PIV Applet except the VERIFY command is performed with Secure Messaging to allow FIPS 140-2 Level 3 validation.

8.2 Critical Security Parameters

LASER PKI Applet-specific CSPs are specified below.

Key	Description / Usage
SM-ECDH	Secure Messaging ECC CDH Z Function P-256 Key Establishment Key
SM-KENC	Secure Messaging 2-Key TDEA CBC encryption key
SM-KMAC	Secure Messaging 2-Key TDEA MAC key
CH-LPIN	8 character string Local PIN
PU-PUK	8 character string PIN Unblocking Key
CH-GPIN	8 character string Global PIN
CH-RPAK	RSA 1024, 2048 Authentication Key (9A)
CH-EPAK	ECDSA P-256 Authentication Key (9A)
LA-SCMK	3-Key TDEA, AES-128, AES-192, AES-256 Card Management Key (9B)
CH-RDSK	RSA 2048 Digital Signature Key (9C)
CH-EDSK	ECDSA P-256, P-384 Digital Signature Key (9C)
CH-RKDK	RSA 2048 Key Management Key (9D) Up to 20 copies of this key may be stored in retired key locations ‘82’ though ‘95’.
CH-EZPVK	ECC CDH Z Function P-256, P-384 Key Management Key (9D) Up to 20 copies of this key may be stored in retired key locations ‘82’ though ‘95’.
CH-SCAK	3-Key TDEA, AES-128, AES-192, AES-256 Card Authentication Key (9E)
CH-RCAK	RSA 2048 Card Authentication Key (9E)
CH-ECAK	ECDSA P-256 Card Authentication Key (9E)

Table 14 - Critical Security Parameters (Applet)

8.3 Public keys

The LASER PKI Applet specification defines the generation of asymmetric key pairs for authentication (9A), digital signature (9C), key management (9D, with retired copies in 82-95) and card authentication (9E). When the GENERATE ASYMMETRIC KEY PAIR service is called, the public keys listed above are returned by the LASER PKI Applet. An external entity (e.g., a card management system) is responsible for packaging the public key in an X509 certificate and storing it in the corresponding X509 certificate container in the LASER PKI Applet. The LASER PKI Applet does not make use of the public key after generation, and does not define any other usage of public keys.

LASER PKI Applet-specific public keys used by the module are specified below.

Key	Description / Usage
SM-PECDH	Public Secure Messaging ECC CDH Z Function P-256 Key Establishment Key
CH-RAPK	Public RSA 1024, 2048 Authentication Key (9A)
CH-EAPK	Public ECDSA P-256 Authentication Key (9A)
CH-RSVK	Public RSA 2048 Digital Signature Key (9C)
CH-ESVK	Public ECDSA P-256, P-384 Digital Signature Key (9C)
CH-RKDK	Public RSA 2048 Key Management Key (9D)
CH-EZPBK	Public ECC CDH Z Function P-256, P-384 Key Management Key (9D)
CH-RAPK	Public RSA 2048 Card Authentication Key (9E)
CH-EAPK	Public ECDSA P-256 Card Authentication Key (9E)

Table 15 - Public Keys (Applet)

9 Roles, Authentication and Services (Applet)

9.1 Roles

Role ID	Role Description
CH	Card Holder (the User role for FIPS 140-2 validation purposes). The Card Holder uses the Module for an identity token. Authenticated using the VERIFY service with CH-LPIN or CH-GPIN.
LA	LASER Administrator. The LASER Administrator is responsible for configuration of the LASER PKI Applet using the PUT DATA and GENERATE ASYMMETRIC KEY PAIR services. Authenticated using the GENERAL AUTHENTICATE service with LA-SCMK.
PU	PIN Unblocking User. The PIN Unblocking User can unblock the Local or Global PIN with the RESET RETRY COUNTER service, or update the PU-PUK with the CHANGE REFERENCE DATA service. Authenticated using the RESET RETRY COUNTER or CHANGE REFERENCE DATA service with PU-PUK.

Table 16 – Roles (Applet)

9.2 Authentication

9.2.1 LASER PKI Applet PIN Comparison Authentication

This authentication method compares a PIN value sent to the Module to the stored CH-LPIN, CH-GPIN or PU-PUK values; if the two values are equal, the operator is authenticated. This method is used in the VERIFY and CHANGE REFERENCE DATA services to authenticate to the CH role, and by the CHANGE REFERENCE DATA and RESET RETRY COUNTER services to authenticate to the PU role.

For the CH-LPIN and CH-GPIN, the Module enforces a minimum character length of 6 characters and requires the new CH-LPIN entered using the CHANGE REFERENCE DATA and RESET RETRY COUNTER services to use only numeric characters. Based on this, the strength of the CH-LPIN and CH-GPIN authentication methods is as follows:

- The probability that a random attempt at authentication will succeed is 1/10^6, one in 1,000,000 as required for FIPS 140-2.
- Based on the approved threshold of 5 for failed CHANGE REFERENCE DATA and RESET RETRY COUNTER attempts, the probability that a random attempt will succeed over a one minute period is 5/10^6, meeting 1 in 100,000 as required by FIPS 140-2.

For the PU-PUK, the Module enforces a minimum character length of 4 characters entered using the CHANGE REFERENCE DATA service allowing all characters except the 0xFF character. Based on this, the strength of the PU-PUK authentication method is as follows:

- The probability that a random attempt at authentication will succeed is 1/255^4, meeting one in 1,000,000 as required for FIPS 140-2.
- Based on the approved threshold of 5 for failed CHANGE REFERENCE DATA attempts, the probability that a random attempt will succeed over a one minute period is 5/255^4, meeting 1 in 100,000 as required by FIPS 140-2.

9.2.2 LASER PKI Applet PIN Comparison Confidentiality

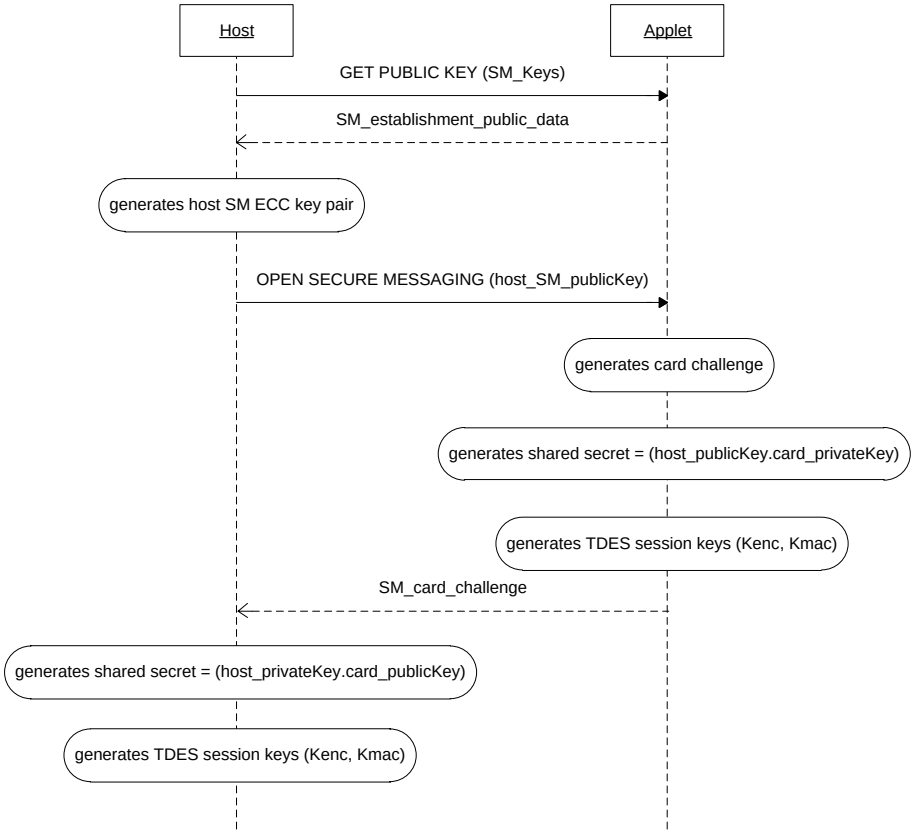
The LASER PKI Applet is able to open a Secure Messaging (SM) session with an external entity in order to establish a confidential (unauthenticated) path between the external entity and the card. The LASER PKI Applet and external entity are then able to exchange sensitive data that remains secret (encryption) and reliable (signature).

The VERIFY, CHANGE REFERENCE DATA and RESET RETRY COUNTER services contain PINs (CH-LPIN, CH-GPIN and PU-PUK) and so can only be performed in an SM session.

Key Establishment uses the ECC CDH Z function. The LASER PKI Applet owns an ECC CDH P-256 Key Pair that was generated and certified at personalization (SM-ECDH). For each SM session, the host generates its own ECC DH Key Pair.

The process to establish a Secure Messaging session is a DH protocol with card authentication uses the following commands:

- GET PUBLIC KEY: to read the SM establishment data (SM-PECDH) from the card
- OPEN SECURE MESSAGING: to transfer the host public key, generate the shared secret and establish the SM session keys



The shared secret = (host_privateKey).(card_publicKey) = (host_publicKey).(card_privateKey).

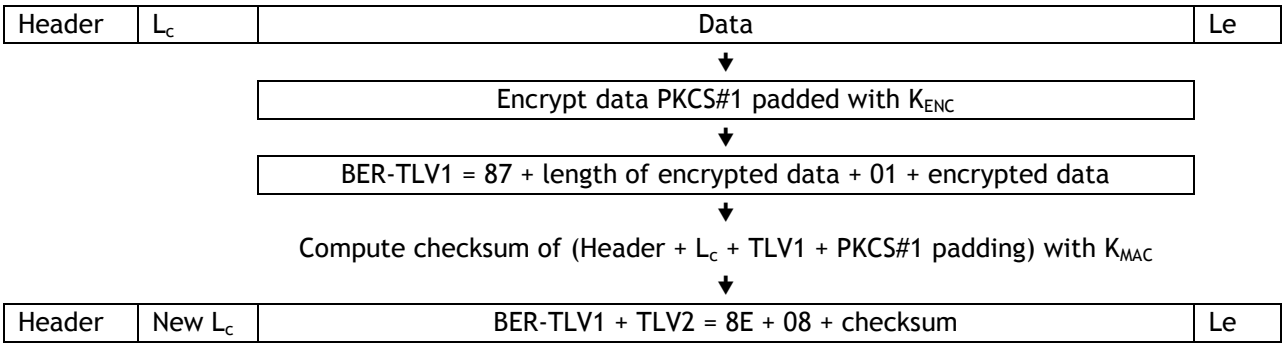
TDEA Session keys are derived from the shared secret: one for data encryption and one for data signature (SM-KENC and SM-KMAC). There is no failure counter as the establishment always succeeds.

The shared secret is 32 bytes long and the generation of the session keys is performed as follows:

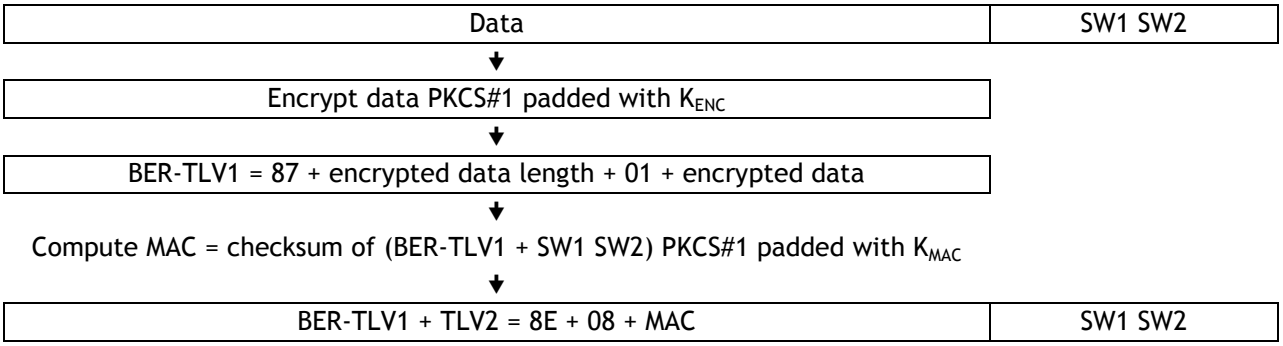
- Compute SM-KENC - form a 2-Key TDEA key with the bytes 0..15 of the shared secret XOR bytes 0..15 of the card challenge
- Compute SM-KMAC - form a 2-Key TDEA key with the bytes 16..31 of the shared secret XOR bytes 16..31 of the card challenge

SM then applies to data in and data out: both are encrypted and signed. The SM CLA byte is OC_H.

Command:



Response:



SM-KENC and SM-KMAC are used for the confidentiality and integrity of the authentication process described in Section 9.2.1 LASER PKI Applet PIN Comparison Authentication. They are therefore protected by the counters associated with the PINs which have a maximum value of 15. This means these keys are limited to (far) less than 2^20 uses which meets the transition restrictions in [SP800-131A].

9.2.3 LASER PKI Applet Symmetric Cryptographic Authentication

This authentication method decrypts (using LA-SCMK) an encrypted challenge sent to the module by an external entity and compares the challenge to the expected value.

The strength of authentication for this authentication method is based on the strength of LA-SCMK; the weakest option is 3-Key TDEA with a security strength of 112 bits with a block size of 64 bits, hence the associated strength of this authentication method is:

- The probability that a random attempt at authentication will succeed is 1/2^64, meeting 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 255/2^64, meeting 1 in 100,000 as required by FIPS 140-2

9.3 Services

All services implemented by the Applet are listed in the tables below. Each service description also describes all usage of CSPs by the service.

9.3.1 Unauthenticated Services

There are no unauthenticated services.

9.3.2 Authenticated Services

Service	Description	CH	PU	LA
CHANGE REFERENCE DATA	Open SM Session by establishing the SM-KENC and SM-KMAC session keys with algorithm ECC CDH using SM-ECDH. Change the CH-LPIN, CH-GPIN or PU-PUK. This service requires authentication of the PIN to be changed. Successful execution of this service with the CH-LPIN or CH-GPIN is an instance of the VERIFY authentication method; that is, the CH has been authenticated. Uses SM-KENC and SM-KMAC for confidentiality and integrity. Uses OS-PKEK to encrypt the candidate PIN for authentication with CH-LPIN, CH-GPIN or PU-PUK, and to encrypt the new CH-LPIN, CH-GPIN or PU-PUK for storage.	X	X	
GENERAL AUTHENTICATE	As defined in [SP800-73] for the Contact interface, this service has several different usages depending on the command tags embedded in the command, and also on the prior execution of other commands in a protocol. This service does not require prior authentication when used for LA role authentication (executes using LA-SCMK) or for authentication of the card to the external system (executes using CH-ECAK, CH-RCAK, or CH-SCAK). When authenticated to the CH role, and when invoked with a challenge or witness tag, executes the specified algorithm using CH-EPAK, CH-RPAK, CH-RKDK, as specified in the command. When authenticated to the CH role *immediately prior* to invocation of this service, and when invoked with a challenge or witness tag, executes the specified algorithm using CH-EDSK, CH-RDSK, as specified in the command. When authenticated to the CH role, and when invoked with the exponentiation tag, executes the ECC CDH primitive using CH-EZPVK, as specified in the command. When invoked for nonce generation in a challenge executes using OS-DRBG_STATE.	X		X
GENERATE ASYMMETRIC KEY PAIR	When authenticated to the LA role, generates new RSA or ECC key pairs. Writes the CH-EPAK, CH-RPAK, CH-EDSK, CH-RDSK, CH-RKDK, CH-EZPVK, CH-ECAK, CH-RCAK, as designated in the command. When used with the CH-RKDK or CH-EZPVK, only the current key location may be specified; the retired key locations '82' through '95' cannot be overwritten with this command. Outputs the corresponding public key.			X
GET DATA (LASER variant)	Retrieve a single data object managed by the LASER PKI Applet access control conditions. If the VERIFY(PIN) security condition is met, access to containers with the PIN condition are allowed. Containers with the ALWAYS access control condition are always allowed.	X		
PUT DATA	An operator authenticated to the LA role can replace the contents of LASER Data objects using this command. This service does not use any CSPs.			X

Service	Description	CH	PU	LA
RESET RETRY COUNTER	Open SM Session by establishing the SM-KENC and SM-KMAC session keys with algorithm ECC CDH using SM-ECDH. Change the CH-LPIN. This service requires authentication of PU-PUK. Executes using PU-PUK, updates the counter associated with CH-LPIN. Uses SM-KENC and SM-KMAC for confidentiality and integrity. Uses OS-PKEK to encrypt the candidate PIN for authentication with PU-PUK, and to encrypt the new CH-LPIN for storage.		X	
VERIFY	Open SM Session by establishing the SM-KENC and SM-KMAC session keys with algorithm ECC CDH using SM-ECDH. Performs VERIFY authentication; executes using CH-LPIN or CH-GPIN as specified in the command. Uses SM-KENC and SM-KMAC for confidentiality and integrity. Uses OS-PKEK to encrypt the candidate PIN for authentication with CH-LPIN or CH-GPIN.	X		

Table 17 –Authenticated Services and CSP Usage

10 Approved Mode of Operation (Applet)

The Module always runs in the Approved mode of operation.

10.1 Verification of Approved Mode

SELECT the LASER PKI Applet and send a GET DATA (LASER variant) command with the tag '0003' and verify that the returned data contains fields as follows. This verifies the version of the LASER PKI Applet. These bytes use a coding internal to Valid S/A. The LASER PKI Applet version 3.0 is coded '00030037'.

Data Element	Length	Value
Applet Version	4	'00030037'

11 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.

12 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.

13 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 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. 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 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.

14 Security Rules and Guidance

14.1 Security Rules (General)

The Module implementation enforces the following security rules:

- The Module does not output CSPs (plaintext or encrypted).
- The Module does not support manual key entry.
- The Module does not output intermediate key values.
- 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.
- Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the Module.

Additional applications can be loaded in the Module after issuance as specified in GlobalPlatform. However, any other firmware loaded into this Module is out of the scope of this validation and requires a separate FIPS 140-2 validation.

- 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.

15 References

15.1 Acronyms

The following acronyms are referred to in this Security Policy.

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
IC	Integrated Circuit
ISD	Issuer Security Domain, see [GlobalPlatform]
KAT	Known Answer Test
PCT	Pairwise Consistency Test
PKI	Public Key Infrastructure
SCP	Secure Channel Protocol, see [GlobalPlatform]
SPA	Simple Power Analysis

Table 18 – Acronyms

15.2 References (Cryptography)

The following Cryptography standards are referred to in this Security Policy.

Standard	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]	PKCS #1 v2.1: RSA Cryptography Standard June 2002
[SP800-38B]	Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication
[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

Standard	Full Specification Name
[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
[AESKeyWrap]	http://csrc.nist.gov/groups/ST/toolkit/documents/kms/AES_key_wrap.pdf

Table 19 – References (Cryptography)

15.3 References (Platform)

The following Platform-related standards are referred to in this Security Policy.

Standard	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

Table 20 – References (Platform)

15.4 References (Applet)

The following LASER PKI Applet-related standards are referred to in this Security Policy.

Standard	Full Specification Name
[FIPS201-1]	Personal Identity Verification (PIV) Of Federal Employees and Contractors, March 2006
[SP800-73-3]	Interfaces for Personal Identity Verification - Part 1: End-Point PIV Card Application Namespace, Data Model and Representation, February 2010 Interfaces for Personal Identity Verification - Part 2: End-Point PIV Card Application Card Command Interface, February 2010

Standard	Full Specification Name
[SP800-78-3]	Cryptographic Algorithms and Key Sizes for Personal Identity Verification, December 2010

Table 21 – References (Applet)