# Security Policy
# For
# Cyberflex Access 64K V2
# With
# PKI Applets

# FIPS140-2 Level 2

# Cyberflex Access 64K V2 With PKI Applets
# Cryptographic Module Security Policy

**Table of Contents**

# 1. INTRODUCTION

## 1.1. Scope

This document defines the Security Policy for the Cyberflex Access 64K V2 cryptographic module with the PKI Applets (HW P/N A1002631, FW Versions Hardmask 1V3, PKI Applet 1.11, PIN Manager Applet 1.6) hereafter referred to as the CA64KV2-PKI. The cryptographic module is an IC (figure 1) with its embedded firmware, designed to be put on a plastic card to produce the Cyberflex Access 64K V2 smart card as shown in figure 2.

The CA64KV2-PKI is submitted for validation, in accordance with FIPS140-2 Level 2 standard.

A description of the security requirements for the cryptographic module and a qualitative description of how each security requirement is achieved are included. In particular, this security policy specifies the security rules with which the cryptographic module must operate.

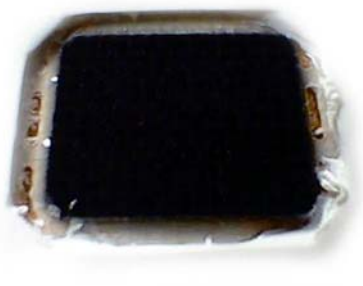

Figure 1


Figure 2

## 1.2. Dependencies

The CA64KV2-PKI relies upon on an independent FIPS validation of the underlying cryptographic algorithms and security functions implemented on the Cyberflex Access 64K V2 cryptographic module. This underlying hardware module provides its own Security Policy (and related documents). http://csrc.nist.gov/cryptval/140-1/1401val2005.htm#572

## 1.3. Terminology

In this document the CA64KV2-PKI module may sometimes be referred to as the *module* or *cryptographic module*. References to the underlying Cyberflex Access 64K V2 module or its Security Policy or related documents) appear as *base module* or *base cryptographic module.*

# 2. OVERVIEW

The cryptographic module contains a microprocessor and EEPROM to provide processing capability and memory for storing instructions and data.

The cryptographic module brings new services, as well as increased security, portability, and convenience, to computer applications.

The cryptographic module combines the advantages of the Java programming language and cryptographic services with those of the micro module. Security comes from both software and hardware. Data integrity and security are provided through cryptographic services, Java Card ™ features, and the Systems Software. In addition, the base cryptographic module hardware provides tamper-resistance and tamper-evidence features, that meet FIPS140-2 Level 3 physical requirements.

The base cryptographic module contains an implementation of the Java Card ™ specification (JC) Version 2.1.1 and of the Open Platform (OP) Version 2.0.1 specification, which defines a secure infrastructure for post-issuance programmable smart cards. The JC specification defines Java Card™ Application Programming Interface (API), which can be used by applets developers to take advantage of the various on-board cryptographic services. The base cryptographic module is a “post issuance programmable” cryptographic module. It includes a virtual machine interpreter that allows programs (applets) written in Java to be loaded onto the base cryptographic module and placed into execution. The OP specification defines a life cycle for OP compliant smart cards. State transitions between states of the life cycle involve well-defined sequences of operations. Once applets are loaded and the base cryptographic module is initialized, external applications communicate with cryptographic module through a secure channel that is established as part of the cryptographic module’s initialization process when it is inserted into a Card Acceptance Device (CAD), or card reader. The Secure channel is established by the Cryptographic Officer with the Open Platform Card Manager application on the cryptographic module. Through the Card Manager, a secure communication pathway can be established with any of the applets on the cryptographic module. Each applet can provide additional “command services” which can be accessed by external applications.

The base cryptographic module, validated to FIPS 140-2, is the Java Card platform, without any applet. The cryptographic module is the Java Card platform, with PKI and PIN Management applets. Any other applets that are loaded post validation must also be validated to FIPS140-2 in order to keep valid the cryptographic module validation. If an applet is loaded on this cryptographic module, the cryptographic module loses its FIPS validation.

# 3. SECURITY LEVEL

The cryptographic module is designed and implemented to meet the Level 2 requirements of FIPS140-2. The individual security requirements, specified for FIPS 140-2, meet the level specifications indicated in the following table.

| Security Requirements Section | Level |
|---|---|
| Cryptographic Module Specification | 2 |
| Cryptographic Module Ports and Interfaces | 2 |
| Roles, Services, and Authentication | 3 |
| Finite State Model | 2 |
| Physical Security | 3 |
| Operational Environment | N/A |
| Cryptographic Key Management | 2 |
| EMI/EMC | 3 |
| Self Tests | 2 |
| Design Assurance | 3 |
| Mitigation of other attacks | 2 |

# 4. CRYPTOGRAPHIC MODULE SPECIFICATION

The cryptographic module supports a command set aimed at allowing the mutual authentication of identities using strong cryptography with “card acceptance devices” in ISO mode (and PCs or other terminals that they might be connected to). Specifically, the TDES algorithm is used within authentication commands between the cryptographic module and the “card acceptance device” environment to authenticate identities. Establishment of identities using these commands is then used to fulfill “access conditions” which limit the ability of the external world to access information and/or commands on the cryptographic module.

This validation effort will be aimed at the Systems software, virtual machine, and Card Manager application with PKI and PIN Management applets.

The cryptographic module is a single chip implementation. The cryptographic module adheres to the various ISO/IEC specifications for Integrated Circuit Chip (ICC) based identification cards. The “cryptographic boundary” for the cryptographic module vis-à-vis the FIPS 140-2 validation is the “module edge”. The module is comprised of the chip (ICC), the hard opaque epoxy, the contact faceplate, and the micro-electronic connectors between the chip and contact pad.

The cryptographic module is comprised of the following elements:

- Hardware IC referenced as A1002631. The IC referenced A1002631 delivers an answer to the MaskTrack command containing 00 0A.
- System software is installed in Read Only Memory (ROM) as part of the chip manufacturing process (known as Hard mask) and in Electrically Erasable, Programmable Read Only Memory (EEPROM) for system options and additional customized software (known as soft mask). The firmware is designated by two version numbers: one for the Hard Mask (HM) and one for the Soft Mask (SM). Note that in the smart card world, Hard Mask refers to software stored in ROM; in other guises, this might be referred to as “firmware”. When all the software is put in ROM, there is no SM. These hard mask and soft mask identification numbers are returned in the response to the MaskTrack command. Currently, one version is available: - HM1v3, no SM, delivering an answer to the MaskTrack command containing 01 03 00 00
- Applets that are to be loaded on the base cryptographic module:
  PKI applet version 1.11
  PIN Management applet version 1.6

## *4.1. MODULE INTERFACES*

The electrical and physical interface of the cryptographic module is comprised of the 5-electrical contacts from the surface of the module to the chip. These contacts conform to the following specifications.

### 4.1.1. Physical Interface description

The cryptographic module supports eight contacts that lead to pins on the chip. Only five of these are connected. The location of the contacts complies with [ISO7816-2] standard. Minimum contact surface area is 1.7mm * 2.0 mm.
Contact dimensions are standard credit card compliant as per ISO/IEC 7816-1 standard:

| Dimension | Value |
|---|---|
| Length | 85.5mm |
| Width | 54.0mm |
| Thickness | 0.80mm |

### 4.1.2. Electrical specifications

#### 4.1.2.1. Specific electrical functions of the contacts:

| Contact | Function |
|---|---|
| C1 | Vcc supply voltage 3 to 5V +/- 10% |
| C2 | RST (Reset) |
| C3 | CLK (Clock) |
| C4 * | Reserved for Future Use (RFU) |
| C5 | GND (Ground) |
| C6 * | Not used |
| C7 | I/O bi-directional line |
| C8 * | Reserved for Future Use (RFU) |

“ * ” - C4, C6 and C8 are disconnected.

#### 4.1.2.2. ICC supply current:

Maximum value: 10 mA at 5MHz (3mA type), short time peak value according to ISO 7816-3. The communication between the reader and the cryptographic module is based on a standardized, half-duplex character transmission, ISO 7816 protocol, T=0 or T=1.

### 4.1.3. Logical Interface Description

Once electrical (physical) contact and data link layer contact is established between the module and the reader, the module functions as a “slave” processor to implement and respond to the card reader commands. The cryptographic module adheres to a well-defined set of state transitions. Within each state, a specific set of commands is accessible.
The details of these commands are listed hereafter. This module also provides an additional set of internal services through the Java Card ™ APIs.

The logical interfaces are connected to the physical interfaces as follows:

| Logical interface | Physical interface |
|---|---|
| Data input | C7 |
| Data output | C7 |
| Status output | C7 |
| Control input | C2, C3, and C7 |
| Power input | C1 and C5 |

# 5. ROLES & SERVICES

## 5.1. Roles

The base cryptographic module defines distinct roles.

- ***Cryptographic Officer:*** This role is the internal security controller. The Cryptographic Officer establishes his identity on the module by demonstrating to the Card Manager application that he possesses the knowledge of a TDES key set stored within the Card Manager. By successfully executing a series of commands, the Cryptographic Officer establishes a secure channel to the Card Manager. The establishment of this channel includes mutual authentication of identities between the Cryptographic Officer and the Card Manager. Once the secure channel is established, the Card Manager grants authorization (on the module) to information and services. The Card Manager Security Domain corresponds to the Card Issuer Security Domain.
- ***User/Applet Provider:*** The Applet Provider is the applet developer that uses the Java API, provided on the base module. The cryptographic services provided by the cryptographic module are delivered through the use of appropriate APIs. An applet has its own Security Domain (Applet Provider Security Domain).
- ***Card Holder Role:*** This role is provided to enable the user of the card to be authenticated.
- ***Card Administrator:*** This role is provided to enable the administrator of the card to be authenticated.
- ***Non-Authenticated Role:*** This role is provided services that can be performed without requiring authentication.

**Identity Based Authentication for Base Cryptographic Module**

- ***Identification.*** The operator identifies himself by selecting his application and the key set inside the application. The application of Cryptographic Officer is the Card manager. The application of the User/Applet Provider is his own applet. The selection of the application is done by a SELECT command. The selection of the key set is done in the INITIALIZE UPDATE, the first command of the two commands that open the Secure Channel.
- ***Authentication.*** The operator authenticates himself using a mutual authentication comprising two commands INITIALIZE UPDATE and EXTERNAL AUTHENTICATION. During this mutual authentication, the operator has to encrypt a message sent by the card, proving knowledge of the TDES key set, which was referenced during the identification.

**Identity Based Authentication for the Applets**

- ***Identification.*** The Card Holder and Administrator identify themselves by selecting the correct user identifier in the authorization API to either the PKI or PIN Management applet instances.
- ***Authentication.*** The operator authenticates himself using a PIN. For the role to be authenticated, the entered PIN must match a previously configured PIN value for that user. The configured PIN value is held within the PIN Management applet instance.

Notes:

1. The Card Holder is the end user of the cryptographic module who is responsible for insuring the ownership of his cryptographic module. The Card Holder is authenticated by verification of a PIN. Dedicated services are prepared on the cryptographic module to manage the Card Holder PIN.
2. The applets downloaded onto the cryptographic module may define other distinct roles that will be part of the applets validation, including the Cardholder, who is responsible for insuring the ownership of his cryptographic module and for not communicating his PIN. The Card Holder will then be authenticated by verification of a PIN.

The Card Manager is the controlling application on the base cryptographic module. It is invoked following every cryptographic module reset and initialization operation.

## *5.2. Services*

### 5.2.1. Cryptographic Module Services

| Services | Description |
|---|---|
| Allocate Key Pair | Allocate a key pair object of a specified type. |
| Change ATR | This command allows modifying the ATR. |
| Change PIN | Change a PIN by specifying Security Domain, PIN number, PIN length and new PIN. Used to unblock Blocked PIN |
| Delete | Used by the Crypto Officer (or the owner of a Security Domain with Delegated Management privilege) to delete a Load File (package), an Application (applet instance) or a Security Domain. |
| External Authenticate (OP) | Authenticate the host, to establish the Secure Channel, and to determine the level of security required for all subsequent commands within the Secure Channel. A previous and successful execution of the INITIALIZE UPDATE command is required prior to processing this command. |
| External Authenticate (Applet) | Authenticates the host using Applet specific keys. |
| File Size | To retrieve the size of the specified file in conjunction with Get Response command. |
| Free Key Pair | Erases contents of Private key and frees the handle. |
| Generate Key Pair | Generate RSA key pair and associate with a allocated key object |
| Get Challenge | Retrieve challenge data from the card to be used for subsequent External Authenticate. |
| Get Data (OP) | The GET DATA command is used to retrieve a single data object. This command is available outside of a Secure Channel (no security condition). However, if issued within a Secure Channel, it must follow the same security level as defined in EXTERNAL AUTH. No CSP are accessible with this command. |
| Get Data (Applet) | Retrieve data element and output selected keys. This is limited by the permission set for the data. No private data is accessible to non-authenticated users. |
| Get Install Data | This function returns the install data that was passed into Install, except for the Personalization PIN value. |
| Get PIN Policy | Returns the PIN policy. |
| Get PIN State | Obtain the PIN state. |
| Get Response | Used in conjunction with other services to output response data. |
| Get Size | This command is provided to retrieve the available EEPROM memory size. |

| | |
|---|---|
| Get Status | This command is used to retrieve Card Manager or Applications information according to a given search criteria. |
| Get Version | This function returns the 2-byte version number of the selected applet. |
| Initialize Update | Initiate a Secure Channel with the Card Manager or a Security Domain. The base cryptographic module and host session data are exchanged, and session keys are generated in the base cryptographic module upon completion of this command. However, the Secure Channel is not considered open until completion of a successful EXTERNAL AUTHENTICATE command that must immediately follow the INITIALIZE UPDATE command. |
| Install | Install an application or a Security Domain requires the invocation of several different internal functions. The INSTALL command is used to instruct the Card Manager (or a Security Domain with Delegated Management privilege) as to which installation step it shall perform during an application installation process. |
| Internal Authentication | Used to authenticate cryptographic module to host system |
| Load | Loads the byte-codes of the Load File (package) defined in the previously issued INSTALL command. |
| Log Out All | Logs out all identities managed by the applet. |
| Manage Applet | Establish a reference to a Shareable Applet Interface |
| Manage Session | Manage a secure messaging session. This command is used to open or close a secure messaging session associated with the PIN manager applet. |
| Mask Track | This command allows the reading of up to 10 traceability data bytes. This command is used to determine that the configuration of the module is consistent with the FIPS approved mode of operation. |
| PIN Change/ Unblock | This command is used by the Crypto Officer to store, replace or unblock PINs, including the Global PIN (Card Holder PIN). |
| Put Data | This command is used to store or replace one tagged data object provided in the command data field. This is limited by the permission set for the data. |
| Put DES Key | Add or replace Security Domain key sets, except for the RSA DAP or DM public key. |
| Put Key | Load the TDES key for External Authenticate usage and re-set the External Authenticate attempt counter. |
| Put RSA Key | Add a key set containing only the RSA DAP or DM public key. |
| Read Binary | Reads data from currently selected CCI file, from specified offset. . This is limited by the permission set for the data. |

| | |
|---|---|
| Read Serial Number | This command is provided to retrieve the chip Serial Number, which identifies the chip and therefore the cryptographic module as unique. |
| Select | Selection of an application (Card Manager, Security Domain or Applet). The Card Manager may be selected either for the loading of a Load File or for installing a previously loaded application (or Security Domain). |
| Set Status | Modify the life cycle state of the base cryptographic module or the life cycle state of an application. Used to set status to terminate Destroying EEPROM content |
| Sign | Sign data. The result is retrieved by a Get Response |
| Unwrap Private Key Init | Initiates private key unwrapping. Key Type and Key Number specify the private key object that will receive the unwrapped private key material. |
| Unwrap Private Key | Part of a private key unwrapping, initiated by Unwrap Private Key Init. This allows entry of private key material. |
| Verify PIN | Verify the specified PIN by specifying Security Domain, PIN number, PIN length and PIN. |
| Write Binary | Writes data to currently selected CCI file, from specified offset. . This is limited by the permission set for the data. |

### 5.2.2. Relationship of Roles and Services

| Services | Crypto -Officer (Card Manager Security Domain) | User/Applet Providers (Applet Security Domain) | Card Holder | Card Administrator | Non-Authenticated |
|---|---|---|---|---|---|
| Allocate Key Pair | | | X | | |
| Change ATR | X | X | | | |
| Change PIN [4] | X | X | X | X | |
| Delete | X | X [1] | | | |
| External Authenticate (OP) | X | X | | | |
| External Authenticate (Applet) | | | | X | |
| File Size | X | X | X | X | X |

| Services | Crypto -Officer (Card Manager Security Domain) | User/Applet Providers (Applet Security Domain) | Card Holder | Card Administrator | Non-Authenticated |
|---|---|---|---|---|---|
| Free Key Pair [3] | | | X | X | |
| Generate Key Pair [3] | | | X | X | |
| Get Challenge | X | X | X | X | X |
| Get Data (OP) [5] | X | X | X | X | X |
| Get Data (Applet) [5] | X | X | X | X | X |
| Get Install Data | X | X | X | X | X |
| Get PIN policy | X | X | X | X | X |
| Get PIN State | X | X | X | X | X |
| Get Response | X | X | X | X | X |
| Get Size | X | X | | | |
| Get Status | X | X | | | |
| Get Version | X | X | X | X | X |
| Initialize Update | X | X | X | X | X |
| Install | X | X [1] | | | |
| Internal Authenticate | X | X | X | X | |
| Load | X | X [1] | | | |
| Log Out All | X | X | X | X | X |
| Manage Applet | X | X | | | |
| Manage Session | X | X | X | X | X |
| Mask Track | X | X | X | X | X |
| PIN Change/Unblock | X | | | | |
| Put Data [5] | X | X | X | X | X |
| Put DES Key | X | X | | | |
| Put Key | X | X | | | |
| Put RSA Key [2] | X | X | | | |
| Read Binary [5] | X | X | X | X | X |
| Read Serial | X | X | X | X | X |

| Services | Crypto -Officer (Card Manager Security Domain) | User/Applet Providers (Applet Security Domain) | Card Holder | Card Administrator | Non-Authenticated |
|---|---|---|---|---|---|
| Number | | | | | |
| Select | X | X | X | X | X |
| Set Status | X | X | | | |
| Sign | | | X | | |
| Unwrap Private Key Init | | | X | X | |
| Unwrap Private Key | | | X | X | |
| Verify PIN | | | X | X | |
| Write Binary [5] | X | X | X | X | X |

1 INSTALL, LOAD & DELETE commands are available to Security Domains having the Delegated Management privilege.
2 The Put RSA Key command is only used to import the RSA Public Key used for DAP or Delegated Management
3. Dependant upon permissions defined under allocate key pair
4. Dependant upon PIN permission set. E.g. Only the owner or Administrator of the PIN can update the PIN.
5. This is limited by the permission set.

### 5.2.3. CSP/Service Access

| CSP | Service | Access |
|---|---|---|
| TDES CO Master Keys | PUT DES KEY | Write |
| TDES CO Master Keys | INITIALIZE UPDATE & EXTERNAL AUTH | Execute |
| TDES CO Master Keys: $K_{KEK}$ | PUT KEY | Execute |
| TDES CO Session Keys | INITIALIZE UPDATE & EXTERNAL AUTH | Create |
| TDES CO Session Key: $K_{enc}$ | Message encryption | Execute |
| TDES CO Session Key: $K_{mac}$ | Message integrity | Execute |
| TDES CO DM Key | PUT DES KEY | Write |
| TDES CO DM Key | DM Receipt computation | Execute |
| TDES User Master Keys | PUT KEY | Write |
| TDES User Master Keys | INITIALIZE UPDATE & EXTERNAL AUTH | Execute |
| TDES User Master Key: $K_{KEK}$ | PUT KEY | Execute |
| TDES User Session Keys | INITIALIZE UPDATE & EXTERNAL AUTH | Create |
| TDES User Session Key: $K_{enc}$ | Message encryption | Execute |
| TDES User Session Key: $K_{mac}$ | Message integrity | Execute |
| TDES User “OP DAP DES” Key | PUT DES KEY | Write |
| TDES User “OP DAP DES” Key | “OP DAP” verification | Execute |
| Global PIN | GLOBAL PIN CHANGE/UNBLOCK | Write |
| TDES Applet Session Keys | INITIALIZE UPDATE & EXTERNAL AUTH | Create |
| TDES Applet Session Keys | GET DATA | Output |
| TDES Applet Session Key: $K_{enc}$ | Message encryption | Execute |
| TDES Applet Session Key: $K_{mac}$ | Message integrity | Execute |
| Card Holder PIN | VERIFY PIN | Execute |
| Card Holder PIN | CHANGE PIN | Write, Erase |
| Card Administrator PIN | VERIFY PIN | Execute |
| Card Administrator PIN | CHANGE PIN | Write, Erase |
| Secure Messaging TDES session key | MANAGE SESSION | Write |
| Secure Messaging TDES session key | VERIFY PIN | Execute |
| Secure Messaging TDES session key | CHANGE PIN | Execute |
| Secure Messaging TDES session key | UNWRAP PRIVATE KEY | Execute |

| | | |
|---|---|---|
| Secure Messaging TDES session key | GET DATA | Execute |
| Secure Messaging TDES session key | PUT DATA | Execute |
| RSA Secure Messaging Private Key | MANAGE SESSION | Execute |
| RSA Secure Messaging Private Key | GET DATA | Write |
| RSA Secure Messaging Private Key | PUT DATA | Write |
| RSA Private Key | SIGN | Execute |
| RSA Private Key | GENERATE KEY PAIR | Create |
| RSA Private Key | FREE KEY PAIR | Erase |
| RSA Private Key | UNWRAP PRIVATE KEY | Write |
| RSA Private Key | PUT DATA | Write, Erase, Create |

## *5.3. Card Cryptographic Functions*

The purpose of the base cryptographic module is to provide a FIPS validated platform for the applets that may in turn provide cryptographic services to end-user applications. The keys represent the identity of the roles involved in controlling the cryptographic module. TDES, AES, RSA and SHA-1 algorithms are provided as services to applets that may be loaded onto the cryptographic module. These algorithms are presented via the Java Card API and shall be used only in a FIPS approved mode of operation. Validation of the use of these cryptographic services in a Java Card applet are subject to a separate validation involving the applets. This cryptographic module validation does include such applets (PKI and PIN Management).

The previously validated Cyberflex Access 64K V2 module provides cryptographic functions as follows:

- TDES (2 keys TDES) [Cert.#312]:
  - The TDES (CBC mode) algorithm is used
    - for authenticating the Crypto Officer (EXTERNAL AUTH command)
    - for encrypting data flow from the off module to the on-module environment. The reverse direction is not encrypted; i.e. the status words returned in response to an APDU are not encrypted.
    - As a TDESMAC to authenticate the originator and to the verification the integrity of the message
  - TDES is also used together with DES CBC as an EDC cf.6.3.2
  - TDES functions are also provided as services to applets, through Java APIs.
- AES 128 [Cert.#220]:
  - The AES functions are only provided as services through Java APIs to applets.
- SHA-1 [Cert.#301]:
  - The SHA-1 function is used in the RSA signature.
  - It is used in the DAP and the DM.
  - It is also provided as a service through Java APIs to applets.
- RSA PKCS1 (1024, 2048 bit keys) [Cert.#51]:
  - RSA is used for the “OP RSA DAP” as described in section 6.1.3.2.
  - RSA is used for the DM as described in section 6.1.3.3.

- RSA functions are also provided as services to applets, through Java APIs. The applet shall use RSA only for “key wrapping” or “signature”.
- DRNG ANSI X9.31 [Cert.#64]:
- The DRNG function is used to generate a nonce during the INITIALIZE UPDATE command.
- It is also provided as a service through Java APIs to applets.

The following are non-Approved cryptographic functions provided by the Cyberflex Access 64K V2 module allowed for use in the Approved mode of operation.

- Hardware RNG
  - Used in the Approved mode of Operation as a seeding source.

- DES [Cert.#293] (Note: DES and DES MAC cannot be used in the Approved mode of operation except for the generation of EDC cf.6.3.2.)
  - DES functions are also provided as services to applets, through Java APIs.
  - DES MAC

The following are non-Approved cryptographic services and shall not be used in the FIPS Approved mode of operation.

- AskRandom

### 5.3.1. Services used by PKI and PIN Management Applets

The following cryptographic services are used by the PKI and PIN Management applets:

- Key Generation:
  - RSA key pair generation: this API generates a pair of RSA keys.
- Key Wrapping:
  - RSA algorithm API supports key wrapping/unwrapping for the key establishment. Key wrapping uses an RSA public key. Key unwrapping uses an RSA private key. –
- Message Digest:
  - SHA-1: this API performs a SHA-1 Message Digest,
- Random Numbers Generation:
  - Secure Random Generation: this API generates a random data, using ANSI X9.31 FIPS140-2 approved method (Deterministic RNG).
- Signature and Verification:
  - RSA SHA-1 PKCS1 mode. Signature uses an RSA private key. Verification uses an RSA public key.
- Origin authentication and Data integrity verification:
  - TDES: these APIs offer TDES MAC in CBC mode with various padding (no padding, ISO9797 M1 and M2),
  - RSA SHA-1 PKCS1 mode. Verification uses an RSA public key.
- PIN
  - PIN APIs are available for applets to authenticate the cardholder. The Global PIN is not utilized by the applets.

## *5.4. Self-Tests*

### 5.4.1. Power Up Self Tests

The cryptographic module performs the required set of self-tests at power-up time. When the cryptographic module is inserted into a reader, once power is applied to the module' electrical (contact) interface, a "Reset" signal is sent from the reader to the module. The cryptographic module then performs a series of GO/NO-GO tests before it responds (as specified by ISO/IEC 7816) with an Answer To Reset (ATR) packet of information. These tests include:

- RAM functional test & clearing at Reset,
- EEPROM Firmware integrity check with a 39/32 Systematic ECC (7 additional bits for every 32 bits). This ECC check is activated by the reading of the whole firmware.
- Algorithm (known answer) tests for:
  - CRC16,
  - TDES (ECB & CBC mode encrypt/decrypt),
  - AES (ECB & CBC mode encrypt/decrypt),
  - SHA-1 Hashing,
  - RSA PKCS1 sign and verify.
  - DRNG

If any of these tests fail, the cryptographic module will respond with an ATR and a status indication of self-test error. Then, the cryptographic module will go mute. No data of any type is transmitted from the cryptographic module to the reader while the self-tests are being performed.

### 5.4.2. Conditional Tests

- RSA Key generation:

  A pair wise consistency check is performed during key generation. It is done in both directions: sign then verify for signature usage; encrypt then decrypt for key wrapping usage. Note that this operation can only be activated by an applet. It is therefore out of the scope of this validation.

- Random Number Generator:

  NDRNG: A 16 bits continuous testing is performed during each use of the Hardware non deterministic RNG. The NDRNG is used to generate seed values to feed the DRNG. DRNG: A 64 bits continuous testing is performed during each use of the FIPS140-2 approved deterministic RNG.

- Software/Firmware load test:

  A TDES CBC MAC is verified whenever an applet is loaded onto the base cryptographic module. This MAC is linked to the secure messaging. An optional DAP verification is made. The algorithm used is an RSA signature or an algorithm using DES for the first n-1 blocks and a TDES for the last block.

## *5.5. Critical Security Parameters:*

### 5.5.1. Cryptographic Keys:

- The base cryptographic module contains the following keys:
    1. TDES Transport Key Set, used to protect the cryptographic module during its delivery. This Key Set will then be superseded by the Crypto Officer Security Domain keys,
    2. TDES Crypto Officer Security Domain keys, used for OP authentication
    3. TDES Session keys
    4. TDES Delegated Management (DM) keys

- Key sets of each applet Security Domain:
    5. TDES Applet Security Domain keys used for OP authentication
    6. TDES Applet Session keys
    7. TDES DAP keys
    8. Secure Messaging TDES session keys

- Applet RSA Keys
    9. RSA Secure Messaging Private key
    10. RSA Private Keys

Security Domains allow a number of distinct identities to be established on the base cryptographic module. These are identities that control access to the various applets stored on the cryptographic module. A Security Domain represents the identity of an application (applet) operator.

### 5.5.2. Other CSPs

The cryptographic module includes other types of CSPs:

- A Global Personal Identification Number (PIN),

  The Global PIN is 7-12 numeric character string that is not used by the cryptographic module.

- A Card Holder PIN to authenticate the Card Holder managed by the PIN Management Applet,

  The Card Holder PIN is variable sized alpha-numeric character string that is used through a dedicated applet API to authenticate the Cardholder to the cryptographic module. That is, by successfully entering a PIN sequence, a cardholder can prove knowledge of a shared secret (the PIN) and thereby authenticate to the cryptographic module. The Card Holder PIN cannot be verified without a PIN Management Applet being loaded on the base cryptographic module.

- An Administrator PIN used by the Administrator to unblock a blocked Card Holder PIN,

  The Administrator PIN is variable sized alpha-numeric character string that is used through a dedicated applet API to authenticate the Administrator to the cryptographic module. That is, by successfully entering a PIN sequence, an Administrator can prove knowledge of a shared secret (the PIN) and thereby authenticate to the cryptographic module. The Administrator PIN cannot be verified without a PIN Management Applet being loaded on the base cryptographic module.

#### 5.5.2.1. Public Keys

The Public keys are not CSPs.

1. RSA DM key
2. RSA DAP keys
3. RSA Secure Messaging Public key
4. RSA Public Key

# 6. SECURITY RULES

## *6.1. FIPS Mode of Operation*

The cryptographic module operates in the Approved Mode of Operation when configured and managed according to this security policy's cryptographic module specification and the defined security rules as follows:

1. The FIPS 140-2 validated Cyberflex Access 64K v2 must be configured and continue to operate in the FIPS Approved mode of operation per the Cyberflex Access 64K v2 security policy. Any deviation invalidates the FIPS 140-2 validation of the cryptographic module.

2. The cryptographic module must be configured as the following operational platform:
   - FIPS 140-2 validated Cyberflex Access 64K v2[1]
     - Hardware Version: A1002631
     - Hardmask 1V3
   - PKI Applet 1.11
   - PIN Manager Applet 1.6

3. The use of single key DES and DES MAC shall not be depended upon to provide protection in the FIPS Approved Mode of Operation.[2] DES and DES MAC can only be used for the generation of EDC.

4. The module shall not perform cryptographic functions for the protection of data that provide less than 80 bits of security.[3]

5. The module shall not perform non-Approved cryptographic functions or services in the Approved mode of operation unless explicitly allowed. For a listing, please reference Section 5.3.

6. The module shall be operated according to the rules defined in Sections 6.3, 6.4 and 6.5

7. The module shall not share DRNG seed and seed keys between the Approved mode and non-Approved mode of operation.

[1] Reference: FIPS 140-2 Certificate #572, http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm#572
[2] Reference: NIST CMVP DES Transition Plan, Federal Register, Vol. 70, No. 96 - May 19, 2005 – Notices http://csrc.nist.gov/groups/STM/common_documents/DESTranPlan.pdf
[3] Reference: NIST Special Publication 800-57, Recommendation for Key Management Part 1 http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57-Part1-revised2_Mar08-2007.pdf

## *6.2. Identification & Authentication Security Rules*

The module implements specific methods for identifying and authenticating the different roles. The implementation consists of the binding of Identity-based Access Control Rules to each service that requires authentication. For the Approved Mode of Operation, all processes that affect the security of the cryptographic module shall be performed by an authorized role.

### 6.2.1. User Identification and Authentication

User/Applet Provider Authentication: The User/Applet Provider must prove the possession of the Applet Security Domain Key Set composed of 3 TDES keys. Two keys are used to authenticate the command payload. A third key is used to encrypt keys transported within the APDU command. This is the same process as the Crypto Officer authentication (Initialize Update & External Authenticate commands) but it uses the TDES keys of the Applet Security Domains.

### 6.2.2. Cryptographic Officer Identification & Authentication

Crypto Officer Authentication: The Cryptographic Officer must prove the possession of the base cryptographic module Manager Key Set composed of 3 TDES keys. Two keys are used to authenticate the command payload. A third key is used to encrypt keys transported within the APDU command (Initialize Update & External Authenticate commands).

### 6.2.3. Card Holder Identification and Authentication

Card Holder Authentication: The Card Holder must identify them self and prove the possession of the Card Holder PIN.

### 6.2.4. Card Administrator Identification and Authentication

Card Administrator Authentication: The Card Administrator must identify them self and prove the possession of the Card Administrator PIN.

### 6.2.5. Key Attempt Counter

- **Attempt Counter**: An attempt counter is associated with each key set of a Security Domain or the Crypto-module Manager.
- **Initialization**: This counter is set to 3 at the creation of the key set and at each successful authentication using this key set.
- **Decrementing**: This counter is decremented by 1 at each unsuccessful authentication using this key set. When the counter reaches 0, the key set is blocked, which means that it cannot be used any more for authentication.

### 6.2.6. PIN Attempt Counter

- **Attempt Counter**: An attempt counter is associated with each PIN.
- **Initialization**: This counter is configured to an initial value at the creation of the PIN and at each successful authentication using this PIN.
- **Decrementing**: It is decremented by 1 at each unsuccessful authentication using this PIN. When the counter reaches 0, the PIN is blocked, which means that it cannot be used any more for authentication unless a higher authority unblocks it.

## *6.3. Applet Loading Security Rules*

### 6.3.1. Integrity and Confidentiality of the loading

Only applets validated to FIPS 140-1 or 140-2 shall be loaded onto the cryptographic module.
Applets can only be loaded through a secure channel; i.e. they pass from the off module to the on-module environment in an encrypted and MACed form. The addition of application code to the module configuration invalidates the FIPS 140-2 validation and the new configuration must be re-evaluated in order to maintain compliance.

This is the only mandatory rule. It guarantees the integrity and the confidentiality of the applet during its loading. The DAP and Delegated Management features described below are considered optional but complimentary for use by the Cryptographic Officer/User and are consistent with operation of the module in the FIPS Approved Mode.

### 6.3.2. Applet Loading with "OP DAP"

In this case, the Issuer (Crypto Officer) loads the applet owned by the Applet provider. The Issuer knows that the applet is correct because he loads it inside a secure channel with his own keys, thereby ensuring the applet Origin and Integrity. The cryptographic module provides a mechanism designated as "DAP" in OP 2.0.1' to give the same confidence to the Applet provider.

This mechanism uses a DAP, computed off-module by the Applet provider and loaded by the Issuer along with the applet. This DAP is then verified on-module with the Applet Provider 's keys, thereby ensuring that the applet loaded onto the module is the one given by the Applet Provider. The DAP verification is done systematically at the end of the loading, without any additional command.

The cryptographic module provides two methods of DAP implementation, "OP DAP DES" and "OP DAP RSA". Only one of them is used when loading an applet.

- The "OP DAP DES" works as an EDC that verifies the integrity of the applet on behalf of the applet provider. It is made of a series of DES computations, ended by a TDES computation. All the DES and TDES operations use the TDES DAP secret key. This TDES DAP key is loaded by the User/Applet Provider in his Security Domain, with the PUT DES KEY command. This TDES DAP key cannot be updated.
- The "OP DAP RSA" is a signature verification, which is a stronger mechanism than the "OP DAP DES". It verifies the integrity of the applet on behalf of the applet provider and it also authenticates the applet provider as the originator of the applet. It is the RSA PKCS#1 Signature of SHA-1 message Digest of the applet.
  The RSA operation uses the applet provider's public key. This RSA DAP key is loaded by the User/Applet Provider in his Security Domain, with the PUT RSA KEY command. This key cannot be updated.

### 6.3.3. Applet Loading with Delegated Management (DM)

In this case, the Applet provider loads his own applet. The cryptographic module provides the Delegated Management (DM) feature as defined in [VOPS]. This feature enables the applet provider to load onto the cryptographic module an applet previously validated by the Issuer (Crypto Officer).

The DM uses two cryptographic mechanisms:

- A Token computation and verification A Token, also called "OP DAP RSA" is an RSA signature computed off-module by the issuer (Crypto Officer) to allow the loading of this applet. The applet provider sends this Token along with the applet. On-module, the Card Manager verifies the token to check the Origin of the applet, (i.e. that the applet has been authorized by the Issuer) and the integrity of the applet. The Token verification operation uses the issuer's RSA DM public key. This key is loaded in the Crypto Officer Security Domain with a PUT RSA KEY command. This key cannot be updated.
- A Receipt computation and verification A Receipt is sent to the Issuer via the applet provider to confirm that the loading operations were done as expected. This Receipt contains data followed by an EDC. This EDC is made of a series of DES, ended by a TDES. All the DES and TDES operations use the issuer 's TDES DM key. This TDES DM key is loaded in the Crypto Officer Security Domain with a PUT DES KEY command. This key cannot be updated.

## *6.4. Physical Security Rules*

The physical security of the base cryptographic module is designed to meet FIPS 140-2 level 3 requirements. A hard opaque epoxy is used to encapsulate the module to meet level 3 requirements. From the time of its manufacture, the cryptographic module is under the control of the cryptographic Officer until it is ultimately issued to the end user.

## *6.5. Key Management Security Rules*

### 6.5.1. Cryptographic key strength

After May 19, 2007, the use of keys of less than 80-bits of security strength shall not be allowed for use in a FIPS Approved mode of operation.

### 6.5.2. Cryptographic key generation

TDES Session keys for Secure Channel Opening, conforming to Open Platform Card Specification v2.0.1' using FIPS140-2 approved ANSI X9.31 DRNG. RSA key pair generation using FIPS140-2 approved ANSI X9.31 DRNG. The keys are generated in CRT format.

### 6.5.3. Cryptographic key establishment, entry and output

Secret and private keys shall be input and output in encrypted format. RSA PKCS#1 key wrapping shall use a key size of 1024 or 2048 bits. This key establishment method provides 80 and 112 bits of strength, respectively.

### 6.5.4. Cryptographic key storage

The Keys are structured to contain the following parameters:

- Key id, which is the Id of the key
- Algo Id, which determines which algorithm to be used
- Integrity Mechanisms (CRC-16).

### 6.5.5. Cryptographic key destruction

The cryptographic module destroys cryptographic keys by reloading another keyset for Crypto Officer keys, Security Domains Applets Keys, or closing of secure channel for session keys**.**

Key Management Details can be found in the CO / User Guidance document.
The keys loaded for DAP and Delegated Management cannot be updated.
To delete DAP keys, the Security Domain must be deleted. This operation deletes all the keys contained in the Security Domain.
To delete DM keys, the Cryptographic Module must be put in the TERMINATED state. This operation deletes the whole EEPROM. It is enabled by the Set Status command.

The applet provides the Put Data service to overwrite key data. The Change PIN service destroys the PINs by overwriting existing PINs.

## *6.6. Mitigation of Attacks Security Policy*

The cryptographic module has been designed to mitigate the following attacks:

- Timing attacks,
- Simple Power Analysis,
- Differential Power Analysis.
- Differential Fault Analysis

# 7. SECURITY POLICY CHECK LIST TABLES

## 7.1. ROLES & REQUIRED AUTHENTICATION

| Role | Type of authentication | Authentication data |
|---|---|---|
| Crypto Officer | TDES authentication | TDES keys (Crypto Officer Security Domain) |
| User/Applet Provider | TDES authentication | TDES keys (Applet Security Domain) |
| Card Holder | PIN | PIN value |
| Card Administrator | PIN | PIN value |

## 7.2. STRENGTH OF AUTHENTICATION MECHANISMS

| Authentication Mechanism | Strength of Mechanism |
|---|---|
| TDES authentication | Probability that a random attempt succeeds is less than 1 in 1,000,000. The probability that random attempts during a 1-minute period succeeds is less than 1 in a 100,000 |
| RSA authentication | Probability that a random attempt succeeds is less than 1 in 1,000,000. The probability that random attempts during a 1-minute period succeeds is less than 1 in a 100,000 |
| PIN (8 Alpha Numeric characters) | Probability that a random attempt succeeds is less than 1 in 1,000,000. The probability that random attempts during a 1-minute period succeeds is less than 1 in a 100,000 |

## 7.3. MITIGATION OF OTHER ATTACKS

| Other Attacks | Mitigation Mechanism | Specific Limitations |
|---|---|---|
| Timing attacks | Counter Measures against Timing attacks | N/A |
| Simple Power Analysis | Counter Measures against SPA | N/A |
| Differential Power Analysis | Counter Measures against DPA | N/A |
| Differential Fault Analysis | Counter Measures against DFA | N/A |

# 8. REFERENCES


| Reference | Title |
|---|---|
| [JVM] | Java Card ™ 2.1.1 Virtual Machine Specification, Sun Microsystems |
| [JCAPI] | Java Card ™ 2.1.1 Application Programming Interface, Sun Microsystems |
| [JCDG] | Java Card ™applet developer's guide |
| [JCRE] | Java Card ™ 2.1.1 Runtime Environment (JCRE) Specification, Sun Microsystems |
| [VOPS] | Open Platform Card Specification, v2.0.1', Visa International |
| [VOPI] | Visa Open Platform Card Implementation Specification - march 1999, Visa International |
| [ISO7816-1] | ISO/IEC JTC 1/SC 17/WG4 Integrated circuits() cards with contacts – Part 1: Physical Characteristics |
| [ISO7816-2] | ISO/IEC JTC 1/SC 17/WG4 Integrated circuits() cards with contacts – Part 2: Dimension and Location of the contacts |
| [ISO7816-3] | ISO/IEC JTC 1/SC 17/WG4 Integrated circuits() cards with contacts – Part 3: Electronic signals and transmission protocol |
| [X9.31] | American Bankers Association, Digital Signatures using Reversible Public Key Cryptography for the Financial Services Industry (rDSA), ANSI X9.31-1998, Washington, D.C., 1998. |
| [FIPS140-2] | National Institute of Standards and Technology, FIPS 140-2 standard. |
| [FIPS140-2A] | National Institute of Standards and Technology, FIPS 140-2 Annex A: Approved Security Functions. |
| [FIPS140-2B] | National Institute of Standards and Technology, FIPS 140-2 Annex B: Approved Protection Profiles, |
| [FIPS140-2C] | National Institute of Standards and Technology, FIPS 140-2 Annex C: Approved Random Number Generators |
| [FIPS140-2D] | National Institute of Standards and Technology, FIPS 140-2 Annex D: Approved Key Establishment Techniques |
| [DES] | National Institute of Standards and Technology, Data Encryption Standard, Federal Information Processing Standards Publication 46-3, October 25, 1999. |
| [DES Modes] | National Institute of Standards and Technology, DES Modes of Operation, Federal Information Processing Standards Publication 81, December 2, 1980. |

# 9. ACRONYMS

| Acronyms | Definitions |
|---|---|
| **AES** | Advanced Encryption Standard |
| **ANSI** | Americain National Standards Institute |
| **AP** | Application Provider |
| **API** | Application Programming Interface |
| **ATR** | Answer To Reset |
| **CAD** | Card Acceptance Device |
| **CBC** | Cipher Block Chaining |
| **CO** | Crypto Officer |
| **CRC** | Cycling Redundancy Check |
| **DAP** | Data Authentication Pattern |
| **DES** | Data Encryption Standard |
| **DFA** | Differential Fault Analysis |
| **DPA** | Differential Power Analysis |
| **DM** | Delegated Management |
| **DRNG** | Deterministic Random Number Generator |
| **ECB** | Electronic Code Book |
| **EEPROM** | Electrically Erasable and Programmable Read Only Memory |
| **EMI** | Electromagnetic Interference |
| **EMC** | Electromagnetic Compatibility |
| **ICC** | Integrated Circuit Card |
| **ISO** | International Organization for Standardization |
| **JC** | Java Card ™ |
| **JCRE** | Java Card ™ Runtime Environment |
| **MAC** | Message Authentication Code |
| **NDRNG** | Non Deterministic Random Number Generator |
| **OP** | Open Platform |
| **PC** | Personnal Computer |
| **PIN** | Personal Identification Number |
| **PKCS** | Public Key Cryptographic Standards |
| **PRNG** | Pseudo Random Number Generator |
| **RAM** | Random Access Memory |
| **RFU** | Reserved for Future USE |
| **RNG** | Random Number Generator |
| **ROM** | Read only Memory |
| **RSA** | Rivest Shamir Adleman |
| **SHA** | Secure Hash Algorithm |
| **SPA** | Simple Power Analysis |
| **TDES** | Triple DES |