RSA Security Inc.

# RSA Applets on the Schlumberger Cyberflex Access 64K Platform

# FIPS 140-2 Validation Security Policy

**Level 2 Validation**

**Document Version 0.7**
**October 23, 2003**

# Table of Contents


**1 INTRODUCTION ..... 4**

1.1 DOCUMENT OVERVIEW ..... 4
1.2 PURPOSE ..... 4
1.3 PRODUCT INFORMATION ..... 4
1.4 DOCUMENT ORGANIZATION ..... 4
1.5 DEPENDENCIES ..... 4
1.6 TERMINOLOGY ..... 5
1.7 DOCUMENT VERSIONS ..... 5

**2 RSA APPLETS ON THE SCHLUMBERGER CYBERFLEX ACCESS 64K PLATFORM .. 6**

**3 SECURITY LEVELS ..... 6**

**4 CRYPTOGRAPHIC MODULE SPECIFICATION ..... 7**

4.1 OPERATIONAL ENVIRONMENT ..... 8
4.2 MODULE INTERFACES ..... 8
*4.2.1 Physical Interface Description ..... 8*
*4.2.2 Electrical Specifications ..... 8*
*4.2.3 Logical Interface Description ..... 9*
4.3 APPLET SECURITY ..... 9
4.4 FIPS-APPROVED MODE OF OPERATION ..... 9

**5 FOR KEY ZEROIZATION PURPOSES, CARD HOLDERS MAY USE A LOAD KEY COMMAND WITH A KEY OF ALL ZEROS TO OVERWRITE THEIR RSA PRIVATE KEY CONTAINED WITHIN THE CRYPTOGRAPHIC MODULE. ROLES AND SERVICES ..... 9**

**5 ROLES AND SERVICES ..... 10**

5.1 ROLES ..... 10
*5.1.1 The Cryptographic Officer/Issuer Role ..... 10*
*5.1.2 The Cryptographic Officer/Administrator Role ..... 10*
*5.1.3 The Card Holder Role ..... 10*
5.2 SERVICES ..... 11
*5.2.1 Crypto Officer/Issuer Services ..... 11*
*5.2.2 Cryptographic Officer/Administrator Services ..... 11*
*5.2.3 Card Holder Services ..... 12*
*5.2.4 Unauthenticated Services ..... 12*
*5.2.5 Relationship Between Roles & Services ..... 13*
5.3 RSA APPLET SERVICES ..... 13
*5.3.1 ID Applet Services ..... 13*
*5.3.2 PKI Applet Services ..... 14*
*5.3.3 GC Applet Services ..... 14*
5.4 PLATFORM CRYPTOGRAPHIC FUNCTIONS ..... 15
*5.4.1 Random Number Generation ..... 16*
*5.4.2 Self Tests ..... 16*
5.5 CRITICAL SECURITY PARAMETERS: ..... 16

*5.5.1 Cryptographic Keys :* ... *16*
*5.5.2 Other CSPs* ... *17*

**6 SECURITY RULES** ... **18**

6.1 IDENTIFICATION & AUTHENTICATION SECURITY RULES ... 18
*6.1.1 Cryptographic Officer/Issuer Identification and Authentication* ... *18*
*6.1.2 Cryptographic Officer/Administrator Identification and Authentication* ... *18*
*6.1.3 Card Holder Identification and Authentication* ... *18*
*6.1.4 Changing Roles* ... *18*
6.2 REAUTHENTICATION AFTER A POWER CYCLE ... 18
6.3 STRENGTH OF AUTHENTICATION ... 18
*6.3.1 Triple DES* ... *18*
*6.3.2 CO/Admin PIN and Card Holder PIN* ... *19*
6.4 APPLET LOADING SECURITY RULES ... 19
6.5 ACCESS CONTROL SECURITY RULES ... 20
6.6 PHYSICAL SECURITY RULES ... 20
6.7 KEY MANAGEMENT SECURITY POLICY ... 20
*6.7.1 Cryptographic Key Generation* ... *20*
*6.7.2 Cryptographic Key Entry/Output* ... *20*
*6.7.3 Cryptographic Key Storage* ... *20*
*6.7.4 Cryptographic Key and CSP Destruction* ... *21*
MITIGATION OF ATTACKS SECURITY POLICY ... 21

**7 SECURITY POLICY CHECK LIST TABLES** ... **22**

**8 REFERENCES** ... **23**

**9 ACRONYMS** ... **24**

# 1 INTRODUCTION

## *1.1 Document Overview*

This document defines the Security Policy for the RSA Applets on the Schlumberger Cyberflex Access 64K Platform. This document includes a description of the basic security requirements for the RSA Applets on the Schlumberger Cyberflex Access 64K Platform and a qualitative description of how each security requirement is achieved.

## *1.2 Purpose*

This is a non-proprietary cryptographic module security policy for RSA Security Inc.'s RSA Applets on the Schlumberger Cyberflex Access 64K Platform cryptographic module. This security policy describes how the RSA Applets on the Schlumberger Cyberflex Access 64K Platform module meets the security requirements of FIPS 140-2, and how to securely operate the module in a FIPS compliant manner. This policy was prepared as part of the level 2 FIPS 140-2 validation of the RSA Applets on the Schlumberger Cyberflex Access 64K Platform module.

FIPS 140-2 (Federal Information Processing Standards Publication 140-2 — Security Requirements for Cryptographic Modules) details the U.S. Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the NIST Web site at http://csrc.nist.gov/cryptval/.

## *1.3 Product Information*

This document deals only with operations and capabilities of the RSA Applets on the Schlumberger Cyberflex Access 64K Platform module in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the RSA Applets on the Schlumberger Cyberflex Access 64K Platform Module and the entire RSA product line from the RSA Security Web site at. http://www.rsasecurity.com/.

## *1.4 Document Organization*

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

- Finite state machine
- Vendor evidence document
- Module software listing
- Crypto Officer's and User's Guides
- Applet Design Specification
- Delivery and Operation document
- Other supporting documentation as additional references

## *1.5 Dependencies*

The RSA Applets on the Schlumberger Cyberflex Access 64K Platform cryptographic module relies on an independent FIPS validation of the underlying cryptographic algorithms and security functions implemented on the Schlumberger Cyberflex Access 64K Platform cryptographic module. This underlying hardware platform provides its own Security Policy (and related documents).

### *1.6 Terminology*

In this document the RSA Applets on the Schlumberger Cyberflex Access 64K Platform Module will sometimes be referred to as the *Module* or *Cryptographic Module*. References to the underlying Schlumberger Cyberflex Access 64K Platform (or its Security Policy or related documents) appear as *base platform* or *base cryptographic module.*

### *1.7 Document Versions*

Table 1 describes the version history of this Security Policy.

| Version - Date | Description |
|---|---|
| 0.1 – 1/20/03 | Initial Draft. William Duane, RSA Security |
| 0.2 – 1/29/03 | Partial Update to incorporate InfoGard comments. Darren Dupre, RSA Security |
| 0.3 – 3/25/03 | Incorporate InfoGard round 2 comments. Ward Rosenberry, RSA Security |
| 0.4 – 4/14/03 | Incorporate InfoGard round 3 comments. Ward Rosenberry, RSA Security |
| 0.5 – 5/2/03 | Incorporate InfoGard round 4 comments. Ward Rosenberry, RSA Security |
| 0.6 – 5/22/03 | Incorporate InfoGard May 20 comments. Ward Rosenberry, RSA Security |
| 0.7 – 10/23/03 | Incorporate comments from NIST. Darren Dupre, RSA Security |

**Table 1. Document Version History:**

# 2 RSA Applets on the Schlumberger Cyberflex Access 64K Platform

The RSA Applets on the Schlumberger Cyberflex Access 64K Platform 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 platforms.

The RSA Applets on the Schlumberger Cyberflex Access 64K Platform supports "post-issuance". To maintain FIPS validation, only FIPS validated applets may be loaded post issuance.

The OP specification defines a life cycle for OP compliant devices. State transitions between states of the life cycle involve well-defined sequences of operations.

Once the platform is initialized, off-platform applications communicate with the RSA Applets on the Schlumberger Cyberflex Access 64K Platform through a secure channel that is established as part of the platform's initialization process when it is inserted into a reader device. The secure channel is established by the Cryptographic Officer with the Card Manager application on the platform. Through the Card Manager, a secure communication pathway can be established with any of the applets on the platform.

Platforms which have been issued to a Cardholder are necessarily in a "SECURE" state. This means that RSA applets have been loaded onto the platform plus a set of keys and PINs through which the roles of the Cryptographic Officer and the Cardholder can be authenticated.

# 3 Security Levels

The RSA Applets on the Schlumberger Cyberflex Access 64K Platform (cryptographic module) meets the overall requirements applicable to Level 2 security of FIPS 140-2. The individual security requirements specified for FIPS 140-2 meet the level specifications indicated in the following table:

| Security Requirements Section | Level |
|---|---|
| Cryptographic Module | 2 |
| Cryptographic Module Ports and Interfaces | 2 |
| Roles, Services, and Authentication | 2 |
| 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 |

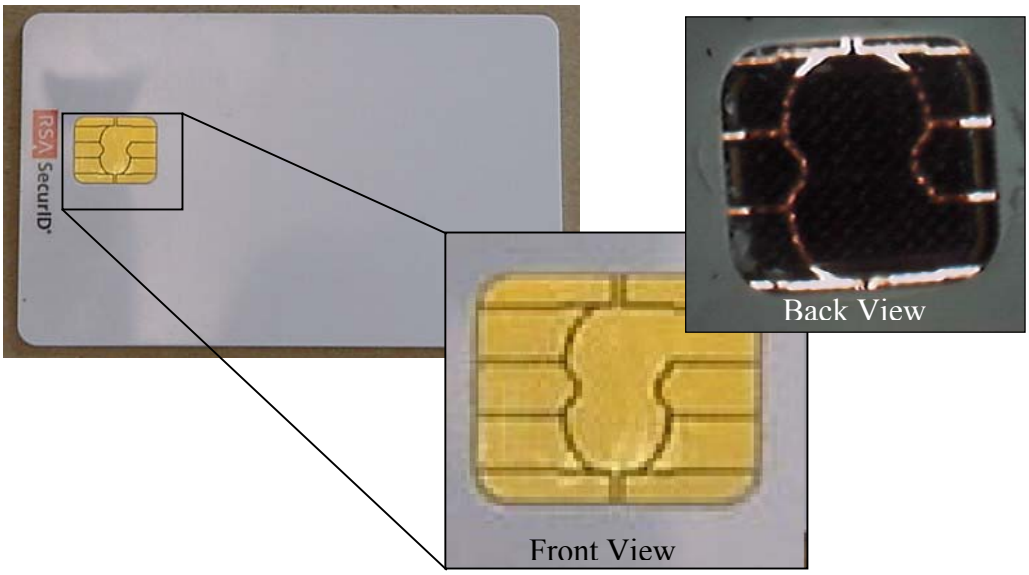
**Table 2. FIPS Security Levels**

# 4 Cryptographic Module Specification

The RSA Applets on the Schlumberger Cyberflex Access 64K Platform supports a command set aimed at allowing the mutual authentication of roles 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 platform and the "card acceptance device" environment for strong authentication of Crypto Officer/Issuer roles. (The Crypto Officer/Administrator and the Card Holder use PINs to authenticate with the card acceptance device.) Establishment of roles using these commands is then used to fulfill "access conditions" that limit the ability of the external world to access information and/or commands on the platform

The RSA Applets on the Schlumberger Cyberflex Access 64K Platform adheres to the various ISO/IEC specifications for Integrated Circuit Chip (ICC) based identification cards. The "cryptographic boundary" for the RSA Applets on the Schlumberger Cyberflex Access 64K Platform vis-à-vis the FIPS 140-2 validation is the "module edge". The module comprises the chip (ICC), the contact faceplate, and the microelectronic connectors between the chip and contact pad. The module is constructed so as to provide the tamper resistance and the tamper evidence required in the FIPS 140-2 physical Level 3 validation. The base module is the Schlumberger Cyberflex Access 64K Platform, Schlumberger HW P/N M512LACC1, HardMask 5 V1, SoftMask 2 V1. Figure 1 shows a physical view of the module configured into a smart card.

**Figure 1. Physical View of the Cryptographic Module**




The RSA Applets on the Schlumberger Cyberflex Access 64K Platform is a single chip implementation of a cryptographic module. The RSA Applets on the Schlumberger Cyberflex Access 64K Platform comprises the following elements:

- Infineon SLE66CX640P, 8 bit micro controller.
- System firmware installed in Read Only Memory (ROM) as part of the chip manufacturing process (known as the Hard Mask) and in Electrically Erasable, Programmable Read Only Memory (EEPROM) for system option and additional customized software (known as the Soft Mask). The firmware is then designated: HardMask 5 V1; SoftMask 2 V1. These HardMask and SoftMask numbers are returned in the Answer To Reset (ATR) character string following the issuing of a RESET signal to the platform (the ATR is: 3B 65 00 00 29 05 01 02 01).
- The RSA applets that are loaded into the EEPROM of the platform.

- Critical Security Parameters stored in the EEPROM as part of the platform personalization operation.

### *4.1 Operational Environment*

The cryptographic module has a non-modifiable operational environment consisting of a Java Virtual Machine operating on a Cyberflex Access 64K chip. The module does not support loading or execution of un-trusted code.

### *4.2 Module Interfaces*

The electrical and physical interface of the cryptographic module is comprised of the 8-electrical contacts from the face of the platform to the chip. These contacts conform to the following specifications:

#### *4.2.1 Physical Interface Description*

The RSA Applets on the Schlumberger Cyberflex Access 64K Platform supports eight contacts that lead to pins on the chip. Only five of these are used.

Minimum contact surface area: 1.7mm * 2.0 mm.

#### *4.2.2 Electrical Specifications*

##### 4.2.2.1 Specific Electrical Functions of the Contacts:

| Contact | Function |
|---|---|
| C1 | Vcc supply voltage 5V +/- 0.5V |
| C2 | RST (Reset) |
| C3 | CLK (Clock) |
| C4 | Reserved for Future Use |
| C5 | GND (Ground) |
| C6 | Not used |
| C7 | I/O bi-directional line |
| C8 | Reserved for Future Use |

**Table 3. Electrical Contact Functions**

##### 4.2.2.2 ICC Supply Current:

- Maximum: 10 mA at 5MHz
- Typical: 3 mA at 5MHz

##### 4.2.2.3 EMI/EMC

The base cryptographic module has been tested to meet the EMI/EMC requirements specified by FCC Part 15, Subpart B, Class B. The cryptographic module is not used for radio communications.

##### 4.2.2.4 Communications

Communications with the RSA Applets on the Schlumberger Cyberflex Access 64K Platforms is based in a standardized, half-duplex transmission protocol. Both T=0 (half-duplex character transmission) and T=1 (half-duplex block transmission) protocols are supported.

#### *4.2.3 Logical Interface Description*

Once electrical (physical) contact and data link layer contact is established between the platform and the reader, the platform functions as a "slave" processor to implement and respond to the reader commands. The platform adheres to a well-defined set of state transitions. Within each state, a specific set of commands is accessible.

(These services are only available to the applets, not the operators of the module.)

### *4.3 Applet Security*

The RSA Applets on the Schlumberger Cyberflex Access 64K Platform includes an on-platform Java Card Virtual Machine. Applets are secure from each other due to the fact that each runs in a "Java Sandbox". The Java Card language does not contain any constructs that allow cross-sandbox communications directly. Any such communication must go through systems software mechanisms which allows for implementation of strict security measures.

### *4.4 FIPS-Approved Mode of Operation*

The following specific actions are required on the part of the Crypto Officer/Issuer and Card Holder along with a restriction within the platform usage environment to ensure the card operates in FIPS-approved mode.

1. The Crypto Officer/Issuer must instantiate all PKI applets to require a PIN for all Generate Key Pair operations and all Sign operations.
2. The Crypto Officer/Issuer must instantiate all container applets to require a PIN for all write operations.
3. End user environments must not allow use of a Load Key command to load externally-generated keys onto the cryptographic module except for RSA Private Key zeroization purposes. Use of the Load Key command for any purpose other than RSA private key zeroization will put the module into a non-FIPS mode of operation.

**5 For key zeroization purposes, Card Holders may use a Load Key command with a key of all zeros to overwrite their RSA private key contained within the cryptographic module.**

## Roles and Services

### *5.1 Roles*

The RSA Applets on the Schlumberger Cyberflex Access 64K Platform defines three distinct roles that are supported by the cryptographic module: the Cryptographic Officer / Issuer, the Cryptographic Officer / Administrator, and the Card Holder. Each of these roles is discussed below.

#### *5.1.1 The Cryptographic Officer/Issuer Role*

An individual takes on the Cryptographic Officer / Issuer (CO/Issuer) role by demonstrating to the Card Manager application that the individual possesses the same set of Triple DES keys that is stored within the Card Manager. By successfully executing a series of commands, the CO/Issuer establishes a secure channel to the Card Manager; establishment of this channel includes mutual authentication of the CO/Issuer role and the Card Manager. Once established, authorization (on the platform) to information and services is granted by the Card Manager. The Card Manager Security Domain corresponds to the Card Issuer Security Domain. Once authenticated, the CO/Issuer can perform various permitted functions, such as executing a series of commands to install FIPS validated applets onto the platform.

The RSA Applets on the Schlumberger Cyberflex Access 64K Platform has a try counter of 15 for each key set contained on the platform. The 15th consecutive failed attempt blocks the key set. The retry counts are per-keyset. If the Card Manager has just one key set, blocking of the key set will block the platform.

The details of the various functions available to the CO/Issuer are enumerated below.

#### *5.1.2 The Cryptographic Officer/Administrator Role*

The Cryptographic Officer / Administrator (CO/Admin) is typically a security expert within the organization which will use the platform. The CO/Admin is a trusted individual, responsible for the management operations associated with the platform, typically including operations such as distributing the platform to the Card Holders, installation of software to support the platform, and so on. An individual takes on the CO/Admin role by demonstrating to the ID applet that the individual possesses the same PIN which is stored within the ID Applet. The CO/Admin PIN is 8 bytes in length. Once authenticated, a CO/Admin can perform various permitted functions, such as executing a series of commands to unlock a platform which was previously locked by the Card Holder (due to a series of consecutive incorrect Card Holder PIN entries). The details of the various functions available to the CO/Admin are enumerated below.

#### *5.1.3 The Card Holder Role*

The Card Holder is the end user of the platform, and is responsible for ownership of the Card Holder's platform. An individual takes on the Card Holder by demonstrating to the ID applet resident on the platform that the individual possesses the same PIN that is stored within the ID applet. Card Holder PINS are strings of characters which can vary in length between 4 and 127 bytes. Once authenticated, a Card Holder can perform various permitted functions such as reading data stored via the General Container Applet. The details of the various functions available to the Card Holder are enumerated below.

## *5.2 Services*

### *5.2.1 Crypto Officer/Issuer Services*

One command set is supported by the Crypto Officer, and is, in fact, used only by the Crypto Officer to allow for the administration of the Security Domains and to load applets onto the platform. This command set includes the following commands:

- **INSTALL:** installing an application or a Security Domain requires the invocation of several different on platform functions. The INSTALL command is used to instruct a Security Domain or the Card Manager as to which installation step it shall perform during an application installation process.
- **LOAD:** this command is used to load the byte-codes of the Load File (package) defined in the previously issued INSTALL command.
- **DELETE:** this command is used to delete a Load File (package) or an Application (applet instance).
- **EXTERNAL AUTHENTICATE**: this command is used by the platform to 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.
- **GET DATA**: 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 AUTHENTICATE.
- **INITIALIZE UPDATE**: this command is used to initiate a Secure Channel with the Card Manager or a Security Domain. Platform and host session data are exchanged, and session keys are generated by the platform upon completion of this command. However, the Secure Channel is considered open upon completion of a successful EXTERNAL AUTHENTICATE command that must immediately follow the INITIALIZE UPDATE command.
- **PUT DATA**: this command is used to store or replace one tagged data object provided in the command data field.
- **PUT KEY**: this command is used to add or replace Security Domain key sets.
- **Deterministic Random Number Generator (DRNG) Statistical Test**: this command is used to execute statistical tests for randomness on the on-platform DRNG.
- **SET STATUS**: this command is used to modify the life cycle state of the platform or the life cycle state of an application.

During the secured channel opening, the command access condition is specified (‘CLEAR’,’MAC’,’MAC+ENC’) and an access control is done on received command.

### *5.2.2 Cryptographic Officer/Administrator Services*

The following commands are available to Crypto Officer/Administrators:

- **CHANGE UNBLOCK PIN:** This command is used by the CO/Admin to change the existing UNBLOCK PIN to a different value. After successful completion of this command, the new PIN value must be used to unblock the Card Holder PIN.
- **UNBLOCK CARD HOLDER PIN**: This command is used by the CO/Admin to unblock a platform which was previously blocked because the Card Holder entered their PIN incorrectly multiple times. After successful completion of this command, the Card Hold is again able to authenticate using the Card Holder PIN. This command also changes the PIN value. The new PIN value may be the same as the previous value.

- **Deterministic Random Number Generator (DRNG) Statistical Test**: this command is used to execute statistical tests for randomness on the on-platform DRNG.

### *5.2.3 Card Holder Services*

The following command is available to Card Holders:

- **Deterministic Random Number Generator (DRNG) Statistical Test**: this command is used to execute statistical tests for randomness on the on-platform DRNG.

### *5.2.4 Unauthenticated Services*

The following commands are available without requiring authentication.

- **SELECT**: this command is used for selecting an application (Card Manager, Security Domain or Applet).
- **GET DATA**: the GET DATA command is used to retrieve a single data object. This command is available in a Secure Channel (see the Note for Table 4.)

  > **Note:** The GET DATA command is available to Crypto Officer/Issuers within a Secure Channel. In this case, GET DATA must follow the same security level as defined in EXTERNAL AUTHENTICATE. A previous and successful execution of the INITIALIZE UPDATE command is required prior to processing this command.

- **GET STATUS**: if the Card Manager is the current application, this command is used to retrieve Card Manager information according to a given search criteria.
- **GET RESPONSE**: this command is restricted to T = 0 ISO protocol for an incoming command which have data to send back. That data is received with the GET RESPONSE command sent immediately after the command it is related to.

### *5.2.5 Relationship Between Roles & Services*

| Roles/Services | No Role | Crypto Officer / Issuer * | Crypto Officer / Administrative | Card Holder |
|---|---|---|---|---|
| INSTALL | | X | | |
| LOAD | | X | | |
| DELETE | | X | | |
| EXTERNAL AUTHENTICATE | | X | | |
| INITIALIZE UPDATE | | X | | |
| PUT DATA | | X | | |
| PUT KEY | | X | | |
| DRNG STATISTICAL TEST | | X | X | X |
| SET STATUS | | X | | |
| SELECT | X | X | X | X |
| GET DATA | X | X | X | X |
| GET STATUS | X | X | X | X |
| GET RESPONSE | X | X | X | X |

* Crypto Officer/Issuers may use the GET DATA command within a secure channel. See the related **Note** in Section 5.2.4, Unauthenticated Services for more information.

**Table 4. Roles and Open Platform Services.**

## *5.3 RSA Applet Services*

There are three RSA applets installed on the base Schlumberger Cyberflex Access 64K Platform:

- The ID applet (version 00 01.00 09)
- The GC Container applet (version 00 01.00 09)
- The PKI applet (version 00 01.00 09)

### *5.3.1 ID Applet Services*

The ID applet provides Platform Holder Verification (CHV) services. Here are the different APDUs/Services that are provided by an ID applet instance:

- **Select:** This service causes the selection of the applet.
- **Install:** This service causes the installation of the applet. This service is called by the OP during the OP Install APDU.
- **Change Unblock Pin:** This APDU is used by the CO/Admin in order to change the existing unblock PIN to a different value. After successful completion of this service, the new PIN value must be used to unblock the Card Holder PIN.
- **Change Card Holder PIN:** This APDU is used by the Card Holder in order to change the existing Card Holder PIN to a different value. After successful completion of this service, the new PIN must be used to authenticate to the platform as the Card Holder role.
- **Unblock Card Holder PIN:** This APDU is used by the CO/Admin in order to unblock a card which was previously blocked by multiple incorrect Card Holder PIN entries. After successful completion of this APDU, the Card Holder is again able to authenticate using the Card Holder PIN. This command also changes the PIN value. The new PIN value may be the same as the previous value.
- **Get Properties**. This APDU is used to obtain information about applet instance configuration.

- **Verify CHV**. This APDU checks the PIN presented by the Card Holder. In addition, this service is available to other applets to verify that the correct PIN has been input by the Card Holder.

| ID Applet Role/Service | No Role | Crypto-graphic Officer / Issuer | Crypto-graphic Officer / Admin | Card Holder |
|---|---|---|---|---|
| Select | X | X | X | X |
| Install | | X | | |
| Change Unblock PIN | | | X | |
| Change Cardholder PIN | | | | X |
| Unblock Cardholder PIN | | | X | |
| Get Properties | X | X | X | X |
| Verify CHV | X | X | X | X |

**Table 5. Roles & Possible ACR Configuration for ID Applet Services. Only FIPS-modes are represented in this chart.**

*5.3.2 PKI Applet Services*

The PKI Applet provides RSA-based cryptographic services. There is one RSA private key for each PKI applet instance. The corresponding certificate is located in the attached GC instance.

Here are the different APDUs / Services that are provided by a PKI applet instance:

- **Select**: This APDU causes the selection of the applet.
- **Install**: This APDU causes the installation of the applet.
- **Get Properties**. This APDU is used to obtain information about applet instance configuration.
- **Generate Key Pair**. This APDU is used to generate an RSA Key Pair in the specified instance of the PKI applet.
- **Get Certificate**. This APDU is used to obtain the certificate corresponding to a Private Key
- **Sign**. This APDU uses a RSA private key to sign data.
- **PIN Verify**. This APDU checks the PIN presented by the Card Holder against the current PIN.
- **Load Key**. This APDU is used to import the Private Key. This APDU exists but is not supported for use in FIPS mode except for Card Holder RSA private key zeroization purposes. Use of the Load Key command for any purpose other than RSA private key zeroization will put the module into a non-FIPS mode of operation.

| PKI Applet Role/Service | No Role | Cryptographic Officer / Issuer | Cryptographic Officer / Admin | Card Holder |
|---|---|---|---|---|
| Install | | X | | |
| Select | X | X | X | X |
| Get Properties | X | X | X | X |
| Generate Key Pair | | | | X |
| Get Certificate | X | X | X | X |
| Sign | | | | X |
| **PIN Verify** | **X** | **X** | **X** | **X** |

**Table 6. Roles & Possible ACR Configuration for PKI Applet Services. Only FIPS-modes are represented in this chart.**

*5.3.3 GC Applet Services*

The Generic Container Applet provides secure storage services. Each GC applet instance corresponds to one storage area. Here are the different APDUs / Services that are provided by a PKI applet instance:

- **Install**: This APDU causes the installation of the applet.
- **Select**: This APDU causes the selection of the applet.
- **Get Properties**. This APDU is used to obtain information about applet instance configuration.
- **Update Buffer**. This APDU is used to write or modify data elements in storage area.
- **Read Buffer**. This APDU is used to read data elements from storage area.
- **PIN Verify**. This APDU checks the PIN presented by the Card Holder against the current PIN.
- **Delete Tag**: This APDU deletes the specified tag value, and associated data, from the GC applet data area.
- **Add Tag**: This APDU creates the specified tag value within the GC applet data area. After creation there is no data associated with the tag value.
- **Write Tag**: This APDU writes data associated with a specific tag into the GC applet data area.
- **Read Tag**: This APDU reads data associated with a specific tag from the GC applet data area.

| GC Applet Role/Service | No Role | Cryptographic Officer / Issuer | Cryptographic Officer / Admin | Card Holder |
|---|---|---|---|---|
| Install | | X | | |
| Select | X | X | X | X |
| Get Properties | X | X | X | X |
| PIN Verify | X | X | X | X |
| Update Buffer | | | | X |
| Delete Tag | | | | X |
| Add Tag | | | | X |
| Write Tag | | | | X |
| Read Buffer | * | * | * | X |
| Read Tag | * | * | * | X |

* True only if install data for GCA specifies public data (see Applet Design Specification section: Install Data for GCA).

**Table 7. Roles & possible ACR configuration for GC applet services. Only FIPS-modes are represented in this chart.**

### *5.4 Platform Cryptographic Functions*

The Schlumberger Cyberflex Access 64K Platform provides a FIPS validated platform for the RSA Applets which in turn provide cryptographic services to end-user applications. The keys represent the roles involved in controlling the platform. A variety of FIPS 140-2 validated algorithms are used in the RSA Applets on the Schlumberger Cyberflex Access 64K Platform to provide cryptographic services; these include:

| Type | Algorithm | FIPS-Approved | Certificate |
|---|---|---|---|
| Public Key | RSA (key sizes: 512, 768, 1024) | Yes (FIPS 186-2) | |
| Symmetric Key | TDES (CBC), 2 keys TDES | Yes (FIPS 46-3) | 125 |
| Digest | SHA-1 | Yes (FIPS 180-1) | 108 |
| Integrity | CRC16 | No | |
| RNG | DRNG (ANSI X9.31) | Yes (FIPS 186-2) | |
| | NDRNG (ANSI X9.31) | No | |

**Table 8. Cryptographic Algorithms.**

The TDES (CBC mode) algorithm is used both for authenticating the Crypto Officer (EXTERNAL AUTH command) and is used for encrypting data flow from the off platform to the on-platform

environment. The reverse direction is not encrypted; i.e. the status words returned in response to an APDU are not encrypted.

#### *5.4.1 Random Number Generation*

The cryptographic module offers the services of a deterministic random number generator and is compliant with the ANSI X9.31 standard.

#### *5.4.2 Self Tests*

##### 5.4.2.1 Power Up Self Tests

The cryptographic module performs the required set of self-tests at power-up time. When the RSA Applets on the Schlumberger Cyberflex Access 64K Platform is inserted into a reader, once power is applied to the platform (contact) interface, a "Reset" signal is sent from the reader to the platform. The platform then performs a series of GO/NO-GO tests before it responds with an Answer To Reset (ATR) packet of information. These tests include:

- RAM functional test & clearing at Reset,
- Non-deterministic random number generator (NDRNG) functional test,
- EEPROM Firmware integrity check (CRC-16),
- Algorithm (known answer) tests for:
    - CRC16,
    - DES (ECB & CBC mode encrypt/decrypt, not available for use),
    - TDES (ECB & CBC mode encrypt/decrypt),
    - SHA-1 Hashing,
    - RSA PKCS1 sign and verify.

If any of these tests fail, the platform will respond with an ATR and a status indication of self-test error. Then, the platform will go mute. No data of any type is transmitted from the platform to the reader while the self-tests are being performed. Cryptographic operations cannot be performed while the module is in an error state. DES is not available through the cryptographic interface.

##### 5.4.2.2 Conditional Tests

- RSA Key generation:
    - A pair wise consistency check is performed during key generation.
- Random Number Generators:
    - NDRNG: A 16 bit continuous test is performed during each use of the hardware non-deterministic random number generator.
        - The NDRNG is used to generate seed values to feed the DRNG.
    - DRNG: A 16 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 each time an applet is loaded onto the platform.

### *5.5 Critical Security Parameters:*

#### *5.5.1 Cryptographic Keys :*

RSA Applets on the Schlumberger Cyberflex Access 64K Platform includes the following keys:

- Crypto Officer/Issuer (CO/Issuer) Security Domain keys,
- TDES Session keys (keys derived from Crypto Officer/Issuer (CO/Issuer) keys set(s)),
- RSA public and private key pair.

A Security Domain key set is structured in such a way as to contain three types of TDES keys:

- Kenc,auth used to derive session keys for Crypto Officer authentication and encrypted mode of the secure channel,
- Kmac, used to derive session key for MAC mode of the secure channel,
- Kkek used to encrypt keys, to be imported into the platform.

Security Domains allow a number of distinct roles to be established on the platform. These are roles that control access to the various applets stored on the platform. A Security Domain represents the role of an application (applet) operator.

The platform has no display or other mechanism which might disclose information during authentication with the Security Domain Keys. The plaintext nonce that is exchanged during the OP secure session process does not disclose any information that could aid an attacker in determining the derived key set.

### *5.5.2 Other CSPs*

The RSA Applets on the Schlumberger Cyberflex Access 64K Platform includes two other types of CSPs:

- CO/Admin PIN
- Card Holder PIN

All PINs are passed to the platform as a binary strings in order to authenticate the Card Holder or CO/Admin to the platform.

By successfully entering the correct PIN sequence, an individual can prove knowledge of the Card Holder PIN stored within the ID applet, and thereby authenticate to the platform as the Card Holder role. Once the correct Card Holder PIN has been entered, the role of Card Holder is established, and the platform is left in an authenticated state until the platform is powered down or an incorrect PIN is entered.

Similarly, by successfully entering the correct PIN sequence, an individual can prove knowledge of the CO/Admin PIN stored within the ID applet, and thereby authenticate to the platform as the CO/Admin role. There is a general-purpose command supported by the Crypto Officer to change and unblock a PIN, but there is no general command to verify a PIN. A “verify PIN” command is provided by the applets through use of APIs.

The CO/Admin PIN authentication happens as part of the “Unblock Card Holder PIN” APDU, and a successful authentication will cause the Card Holder PIN to be unblocked. If the incorrect CO/Admin PIN is passed with the “Unblock Card Holder PIN” APDU, then the Card Holder PIN will not be unblocked. Whether or not the correct CO/Admin PIN is supplied, the card is left in an un-authenticated state after completion of the APDU processing.

The platform has no display or other mechanism that might disclose information during a PIN based authentication. During the PIN verification process the only data that is released is the number of retry attempts remaining.

# 6 SECURITY RULES

## *6.1 Identification & Authentication Security Rules*

The module implements specific methods for identifying and authenticating the different roles. The implementation consists of the binding of a Role-Based Access Control Rule to each service.

### *6.1.1 Cryptographic Officer/Issuer Identification and Authentication*

The Cryptographic Officer/Issuer must prove the possession of the Card 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).

### *6.1.2 Cryptographic Officer/Administrator Identification and Authentication*

The Cryptographic Officer/Administrator must prove possession of the CO/Admin PIN. An individual takes on the CO/Admin role by demonstrating to the ID applet that the individual possesses the same PIN which is stored within the ID Applet. CO/Admin PINS are 8-byte strings of characters. The CO/Admin PIN is passed with the command. A valid PIN causes the module to enter the CO/Admin Role in which the command executes. The module transitions from the CO/Admin role to the unauthenticated state when the command completes.

### *6.1.3 Card Holder Identification and Authentication*

The Card Holder must prove possession of the Card Holder PIN. An individual takes on the Card Holder role by demonstrating to the ID applet resident on the platform that the individual possesses the same PIN that is stored within the ID applet. Card Holder PINS are strings of characters which can vary in length between 4 and 127 bytes.

### *6.1.4 Changing Roles*

If the user of the platform wished to change from one role to another for some reason (for example from CO/Issuer to Card Holder), then the operator must re-authenticate to the platform using the credentials appropriate for the new role the operator was attempting to assume

## *6.2 Reauthentication After a Power Cycle*

If power is removed and re-applied to the platform, the platform will be in an un-authenticated state. Role based authentication must re-occur to gain access to protected services and APDUs offered by the card.

## *6.3 Strength of Authentication*

### *6.3.1 Triple DES*

Each of the Triple DES keys used by the CO/Issuer has an effective key length of 168bits. This results in over 3E50 possible keys for each of the Triple DES keys in the CO/Issuer 3 key set which far exceeds the 1 in a million test requirement.

In order to try a key against the platform, the attacker must send a minimum of an13 byte APDU to the card, and get a resulting 2-byte response. Since there is a single I/O port on the platform, this means that each Triple DES key attempt requires 15 bytes of data to be clocked in or out of the card. The

maximum data rate for the platform is 115Kbps through this single port. If we ignore the processing time required on the platform to process the triple DES key, then we can compute the maximum number of attempts which could occur within a 60 second interval:

- 15 bytes of I/O at 8bits/byte = 120bits/attempt
- 120bits/attempt divided by 115,000bits/second = .001043seconds/attempt
- 60seconds/minute divided by .001043seconds/attempt = 57,526attempts/minute

Since the Triple DES keyspace is over 3E50 possible values, it is clear that 57,526 attempts in a 60 second interval will not significantly traverse the space of possible values. As a result, the platform far exceeds the requirement of 1 in 100,000 for multiple attempts in a 60 second interval.

In reality the situation is even better than this for several reasons. First the attacker would need to compromise all 3 triple DES keys, not just one. In addition to this, the processing time needed for the platform to process each triple DES key is not insignificant, and would substantially reduce the number of attempts possible during the 60 second interval.

#### *6.3.2 CO/Admin PIN and Card Holder PIN*

The length of the CO/Admin PIN is fixed at 8 bytes while the minimum length of the Card Holder PIN is 4 bytes. In both cases, we allow any keyboard characters including Shift-number combinations. That is, each byte of the PIN can be one of the character set (a-z, A-Z, 0-9) yielding a minimum of 62^4 or approximately 14.7 million possible PINs. This far exceeds the 1 in a million test.

In order to try a PIN against the platform, the attacker must send a 9 byte APDU to the card, and get a resulting 2-byte response. Since there is a single I/O port on the platform, this means that each PIN attempt requires 11bytes of data to be clocked in or out of the card. The maximum data rate for the platform is 115Kbps through this single port. If we ignore the processing time required on the platform to check the PIN, then we can compute the maximum number of PIN attempts which could occur within a 60 second interval:

- 11 bytes of I/O at 8bits/byte = 88bits/attempt
- 88bits/attempt divided by 115,000bits/second = .000765seconds/attempt
- 60seconds/minute divided by .000765seconds/attempt = 78,431attempts/minute

Since the minimum length PIN results in over 14.7 million possible values, it is clear that 78,431 attempts in a 60 second interval will not significantly traverse the space of possible PIN values. As a result, the platform far exceeds the requirement of 1 in 100,000 for multiple attempts in a 60 second interval.

In reality, the situation is significantly better than even this. The maximum number of attempts which the attacker could perform is limited by an 8 bit counter internal to the ID applet which will block the card if the number of consecutive failed PIN attempts exceeds the counter value. At a maximum this would limit the number of attempts possible in 60 seconds to 256 attempts. In practice, this counter is set to a value of 15 attempts per key set.

### *6.4 Applet Loading Security Rules*

The cryptographic module allows only loading of FIPS validated applets. Applets can only be loaded through a secure channel; i.e. they pass from the off platform to the on-platform environment in an encrypted and MACed form.

### *6.5 Access Control Security Rules*

Keys must be loaded through a secure channel. Consequently, keys are always loaded in the encrypted form.

### *6.6 Physical Security Rules*

The physical security of the underlying Schlumberger Cyberflex Access 64K Platform 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 platform is in possession of a Cryptographic Officer until it is ultimately issued to the Card Holder. Starting with the time the platform is manufactured it is under the control of the CO/Issuer, who is authenticated as discussed above using the 3DES key set. The platform is then distributed from the CO/Issuer to the CO/Admin. The CO/Admin authenticates using the CO/Admin PIN as described above.

No specific actions are required by users to maintain physical security rules.

### *6.7 Key Management Security Policy*

#### *6.7.1 Cryptographic Key Generation*

- TDES Session key derivation using FIPS140-2 approved ANSI X9.31 DRNG for Secure Channel Opening.
- RSA key pair generation using FIPS140-2 approved ANSI X9.31 DRNG.

No intermediate key generation values are output from the cryptographic module upon completion of the key generation process

#### *6.7.2 Cryptographic Key Entry/Output*

CO/Issuer (asymmetric) keys shall always be input in encrypted format, using the Put Key command within a secure channel. During this process, the keys are double encrypted (using the Session Key Kenc,auth and the Kkek Key).

Card Holder (asymmetric) keys must be created on the card using the Generate Key command. It is possible to write a private key into the platform using a Load Key operation, however this is not supported in FIPS mode except for RSA private key zeroization purposes. Use of the Load Key command for any purpose other than RSA private key zeroization will put the module into a non-FIPS mode of operation. Private keys are never output under any condition.

#### *6.7.3 Cryptographic Key Storage*

The Keys are structured to contain the following parameters:

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

Note that none of the applets store cryptographic keys. Applets access key related functions via the Javacard API.

### *6.7.4 Cryptographic Key and CSP Destruction*

There is no specific command to destroy cryptographic keys, however a Load Key command can be used with a value of zero that overwrites a Card Holder RSA private key with a value of all zeros, effectively zeroizing the selected key.

The Card Holder PIN or CO/Admin PIN can be zeroized by issuing a Change PIN or Change Unblock PIN command with a value of all zeroes for the new PIN. This will overwrite the appropriate PIN.

***Mitigation of attacks Security Policy***

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

- Simple Power Analysis,
- Differential Power Analysis.

# 7 SECURITY POLICY CHECK LIST TABLES

| Role | Type of authentication | Authentication data |
|---|---|---|
| Crypto Officer/Issuer | TDES authentication | TDES keys |
| Crypto Officer/Admin | PIN | Admin PIN |
| User/Card Holder | PIN | User/Card Holder PIN |

**Table 9. Roles and Required Identification and Authentication.**

| Authentication Mechanism | Strength of Mechanism |
|---|---|
| TDES authentication | High (Far exceeds the 1 in a million test.) |
| PIN based authentication | High (Far exceeds the 1 in a million test.) |

**Table 10. Strength of Authentication Mechanisms.**

| Role | Authorized Services |
|---|---|
| Crypto Officer/Issuer | All CO/Issuer Services as listed in sections 5.2 and 5.3 |
| Crypto Officer/Admin | All CO/Admin Services as listed in sections 5.2 and 5.3 |
| Card Holder | All Card Holder Services as listed in sections 5.2 and 5.3 |

**Table 11. Services Authorized for Roles.**

| Service | CSP | Types of Access (eg. Read, Write, Execute) |
|---|---|---|
| External Authenticate | TDES CO Keys | Execute |
| PUT KEY | TDES CO Keys | Write |
| Sign | RSA Private Key | Execute |
| Generate Key Pair | RSA Private Key | Write |
| | | |
| | | |
| | | |
| Change Unblock PIN | CO/Admin PIN | Write |
| Change/Unblock PIN | CO/Admin PIN | Execute |
| Change/Unblock PIN | Card Holder PIN | Write |
| PIN Verify, Verify CHV | Card Holder PIN | Execute |

**Table 12. Access Rights within Services.**

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

**Table 13. Mitigation of Other Attacks.**

# 8 REFERENCES

[JVM] Java Card ™ 2.1 Virtual Machine Specification v1.1 - june 1999, Sun Microsystems
[JCAPI] Java Card ™ 2.1 Application Programming Interface, Sun Microsystems
[JCDG] Java Card ™applet developer's guide
[JCRE] Java Card ™ 2.1 Runtime Environment (JCRE) Specification, Sun Microsystems
[VOPS] Open Platform Card Specification, v2.0 - april 1999, Visa International
[VOPI] Visa Open Platform Card Implementation Specification - march 1999, Visa International
[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.
[DSS] National Institute of Standards and Technology, Digital Signature Standard (DSS), Federal Information
Processing Standards Publication 186-2, January 27, 2000.

# 9 ACRONYMS

**ACR:** Access Control Rule
**AP**: Application Provider
**APDU:** Application Protocol Data Unit
**ATR**: Answer To Reset
**API:** Application Programming Interface
**CBC:** Cipher-Block Chaining
**DES:** Data Encryption Standard
**DRNG:** Deterministic Random Number Generator
**ECB:** Electronic Code Book
**EEPROM:** Electrically Erasable and Programmable Read Only Memory
**GC:** Generic Container
**ID:** Identification
**JC21:** Java Card ™ 2.1
**JCRE:** Java Card ™ Runtime Environment
**MAC:** Message Authentication Code
**NRNG:** Non-deterministic Random Number Generator
**PIN:** Personal Identification Number
**PKI:** Public Key Infrastructure
**RAM**: Random Access Memory
**ROM:** Read Only Memory
**OP:** Open Platform