Security Policy

for

Schlumberger Cyberflex Access 32K

Smart Card Module with Schlumberger PKI Applets

Version 1.07

TABLE OF CONTENTS

1 Scope of Document

This document defines the Security Policy for the Schlumberger Cyberflex Access 32K Smart Card Module with Schlumberger PKI Applets. Included is a description of the basic security requirements for the Schlumberger Cyberflex Access 32K Smart Card Module with Schlumberger PKI Applets card and a qualitative description of how each security requirement is achieved.

2 Introduction

The Schlumberger Cyberflex Access 32K Smart Card Module with Schlumberger PKI Applets contains an implementation of the Open Platform (OP) Version 2.0.1 specification, which defines a secure infrastructure for post-issuance programmable smart cards. The OP specification defines a life cycle for OP compliant cards. State transitions between states of the life cycle involve well defined sequences of operations. Cards which have been issued to a Card Holder are necessarily in a "SECURE" state. This means that a defined set of applications have been loaded onto the card plus a set of keys and PINs through which the rolesof the Cryptographic Officer and the Card Holder can be authenticated.

3 Security Levels

The Schlumberger Cyberflex Access 32K Smart Card Module with Schlumberger PKI Applets (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 Specification	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	2
Self Tests	2
Design Assurance	2
Mitigation of other attacks	2

4 Cryptographic Module Specification

The Schlumberger Cyberflex Access 32K Smart Card Module with Schlumberger PKI Applets is mounted in an ID-1 class smart card body that adheres to the various ISO/IEC specifications for Integrated Circuit Chip (ICC) based identification cards. The "cryptographic boundary" for the Schlumberger Cyberflex Access 32K Smart Card

Module with Schlumberger PKI Applets vis-à-vis the FIPS 140-2 validation is the "module edge". The module is comprised of the chip (ICC), the contact faceplate, and the micro-electronic connectors between the chip and contact pad all contained within an epoxy substrate. 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 Schlumberger Cyberflex Access 32K Smart Card Module with Schlumberger PKI Applets is a single chip implementation of a cryptographic module.

4.1 Module Interfaces

The electrical and physical interface of the Schlumberger Cyberflex Access 32K Smart Card Module with Schlumberger PKI Applets, as a cryptographic module, is comprised of the 8-electrical contacts from the face of the card to the chip. These contacts conform to the following specifications:

4.1.1 Physical Interface Description

The Schlumberger Cyberflex Access 32K Smart Card Module with Schlumberger PKI Applets supports eight contacts that lead to pins on the chip. Only five of these are used. The location of the contacts complies with ISO/IEC 7816-2. Minimum contact surface area: 1.7mm * 2.0 mm

Contact dimensions are standard credit card compliant as per ISO/IEC 7816-1:

Dimension	Value
Length	85.5mm
Width	54.0mm
Thickness	0.80mm

4.1.1.1 Electrical Specifications

Specific electrical functions of the contacts:

Contact	Function
C1	Vcc supply voltage 3V-5V +/- 0.5V
C2	RST (Reset)
C3	CLK (Clock)
C4	RFU
C5	GND (Ground)
C6	Not used
C7	I/O bi-directional line
C8	RFU

ICC supply current:

- MAX: 50 mA at 5MHz
- TYP: 5 mA at 5MHz
- Card structure and ICC electrical contacts defined by ISO/IEC 7816-1&2.
- Electrical signaling between the “card acceptance device” (CAD) and the card defined by ISO/IEC 7816-3.
- Card security and key access command set defined by ISO/IEC 7816-4.
- CAD to card communication protocols defined by ISO/IEC 7816-3 & 4.

4.1.2 Logical Interface Description

Electrical (physical) contact and data link layer contact is established between the card and the CAD by the CAD issuing a RESET signal to the card which then responds with an "Answer To Reset (ATR)” containing the version numbers of the hard and soft masks contained on the card. From this point on, the card functions as a “slave” processor to implement and respond to the CAD’s “master” commands. The card 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 defined in the Schlumberger Cyberflex Access 32K Smart Card Module with Schlumberger PKI Applets Technical Specification Document that is included as a proprietary and private extension to this Schlumberger Cyberflex Access 32K Smart Card Module with Schlumberger PKI Applets Security Policy document.

In addition to the basic card with its resident software platform, three applets are also included within the cryptographic module. These are:

- Gina Applet – Version 1.1
- Smart Login Applet – Version 1.1
- PKI Applet – Version 1.1

Each of these applets provides additional commands that the card will support, in addition to those commands provided by the basic resident (ROM-stored) software on the card. The Gina Applet provides support for several commands which enable the secure storage and retrieval of account and password information for login operations on Windows platforms. The Smart Login Applet provides support for several commands which enable the secure storage and retrieval of account and password information for login operations on arbitrary secure web sites. The PKI Applet provides support for several commands which perform cryptographic operations in support of off-card Public Key Infrastructures.

Both the Gina applet and the Smart Login applet make use of commands provided by the PKI applet; specifically, the commands which provide a PIN to control access to other commands.

5 Roles and Services

5.1.1 Roles

The Schlumberger Cyberflex Access 32K Smart Card Module with Schlumberger PKI Applets defines two distinct roles that are supported by the on-card cryptographic system: the Cryptographic Officer and the User (Card Holder).

- Cryptographic Officer: established by demonstrating knowledge of a key set or a CO PIN.
- Card Holder: a User role as authenticated by knowledge of a PIN

Through on-card applets, services are provided to the Card Holder based on his authenticating to his role. The Card Holder authenticates his role to the applets by proving knowledge of a Personal Identification Number (PIN) stored within the PKI applet. Individual applets can have additional PINs, allowing them to do their own authentication of the Card Holder. All PINs used with the basic card or applets are 7-12 digits in length.

The module insures the authentication of off-card entities (the CO and Card Holder) and provides them with cryptographic services according to their role.

Cryptographic Officer - This role is the on card security controller. The Cryptographic Officer establishes his role on the card by demonstrating to the Card Manager application that he possesses the knowledge of a TDES key set stored within the Card Manager or by knowledge of a CO PIN stored within the PKI applet. The Cryptographic Officer can change the CO PIN by using the CHANGE_CHV command and entering the CO PIN. By successfully executing a series of commands, the Cryptographic Officer establishes a secure channel to the Card Manager; establishment of this channel includes mutual authentication of roles between the Cryptographic Officer and the Card Manager. Once established, authorization (on the card) to information and services is granted by the Card Manager. The Card Manager Security Domain corresponds to the Card Issuer Security Domain.

Card Holder - The Card Holder is responsible for insuring the ownership of his card and for not communicating his PIN. The Card Holder is authenticated by verification of a PIN. The PIN is provided in the PKI applet.

5.1.2 Basic Card Services

5.1.2.1 Crypto Officer Administrative Services

The Crypto Officer can effective changes on the card or within applets on the card through a series of commands accessible (to the CO) after the CO role has been authenticated. The CO authenticates his role in order to reset the PIN in the applets by proving knowledge of the CO PIN. Alternately, the CO authenticates his role in order to issue commands to the basic card by proving knowledge of a key set. These commands include:

EXTERNAL AUTHENTICATE: this command is used by the card 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 AUTH.

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.

INITIALIZE UPDATE: this command is used to initiate a Secure Channel with the Card Manager. Card and host session data are exchanged, and session keys are generated by the card 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. A PUT KEY command with a key-set of all zeros will zeroize the Security Domain key sets.

SELECT: this command is used for selecting an application (Card Manager or Applet).

SET STATUS: this command is used to modify the life cycle state of the card or the life cycle state of an application.

All commands except (Select, Initialize update, External Authentication and Get Status) need a secured channel to be executed. During the secured channel opening, the command access condition is specified ('MAC','MAC+ENC') and an access control is done on received command.

5.1.2.2 Card Cryptographic Functions

The purpose of the Schlumberger Cyberflex Access 32K Smart Card Module with Schlumberger PKI Applets is to provide a FIPS validated platform for applets that may in turn provide cryptographic services to end-user applications. The keys represent the roles involved in controlling the card. A variety of FIPS 140-2 validated algorithms are used in the Schlumberger Cyberflex Access 32K Smart Card Module with Schlumberger PKI Applets to provide cryptographic services; these include:

- TDES, (2 keys TDES): This algorithm is used to encrypt and MAC data sent to the module by the CO during the secure session
- SHA-1: Used during the RSA signature process to hash the data to be signed
- RSA PKCS1 (512, 768, 1024 bit keys): Used to sign data with the imported RSA private key

5.1.2.3 Self Tests

5.1.2.3.1 Power Up Self Tests

The Schlumberger Cyberflex Access 32K Smart Card Module with Schlumberger PKI Applets performs the required set of self-tests at power-up time. When the Schlumberger Cyberflex Access 32K Smart Card Module with Schlumberger PKI Applets is inserted into a smart card reader, once power is applied to the card (contact) interface, a "Reset" signal is sent from the reader to the card. The card 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
- HRNG functional test
- EEPROM Firmware integrity check
- Algorithm (known answer) tests for
  - TDES (encryption and decryption in ECB mode)
  - SHA-1 Hashing
  - RSA signature

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

5.1.2.3.2 Conditional Tests

Random Number Generator:

PRNG: A 16 bits continuous testing is performed during each use of the deterministic RNG.

Software/Firmware integrity tests.

5.1.2.4 Applets

The applet services are invoked by external APDU commands sent to the card. The Access Control Rules(ACRs) are applied on the APDU commands.

5.1.2.4.1 GINA Applet Services

The GINA applet provides support for login operations on a Windows platform. The applet uses a pseudo-file mechanism for storing information which can then be read from the card/applet in order to be used for the login operation. This pseudo-file mechanisms is used in order to maintain the paradigm for storing and retrieving information that has been used historically on smart cards; that is, an on-card file system. For this applet, and the other applets on this card, there is no real file system in the same sense as the file systems historically found on other smart cards. Rather, within this applet information is referenced by a "pseudo-file name" and the storage and retrieval operations are performed through "READ_BINARY" and "WRITE_BINARY" commands, much as they would have been done on cards with "real" file systems. Here are the different APDUs / Services that are provided by a GINA applet instance:

- **GET_VERSION**. This command is used to query the on-card applet for its version number.
- **SELECT_FILE** This command is used to select one of the two on-card "files" supported by this applet; one of the files contains an account name and the other a password used to login the Card Holder to a Windows account.
- **READ_BINARY** This command is used to read the information stored in the selected pseudo-file provided by this applet. There are two pseudo-files used within this applet; File 2000 and File 2001. This command can read information from these two pseudo-files.
  - File 2000 is used to store an account name.
  - File 2001 is used to store a password.
- **WRITE_BINARY** This command is used to write information into the selected pseudo-file provided by this applet for storing an account name and a password for that account. The same two files (that were mentioned in the previous command) can be "written to" using this command.
  - File 2000 is used to store an account name.
  - File 2001 is used to store a password.
- **FILE_SIZE** This command is used to return the size (in bytes) of the selected pseudo-file.

It should be noted that the PIN verification and control commands of the PKI applet are used by this applet to provide PIN controlled access to the file data stored in the pseudo-files of this applet.

Role / Authentication Method vs. Services	No Role	Crypto-graphic Officer	Card Holder PIN
GINA Applet			
GET_VERSION	**X**		
SELECT_FILE	**X**		
READ_BINARY (2000)			**X**
READ_BINARY (2001)			**X**
WRITE_BINARY(2000)			**X**
WRITE_BINARY(2001)			**X**
FILE_SIZE	**X**		

Table 1 - Roles & Possible ACR Configuration for GINA Applet Services

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

- **GET_INSTALL_DATA**. This APDU is used to obtain the certificate corresponding to a Private Key.
- **GET_VERSION** This APDU is used to retrieve the version number of the PKI applet
- **SELECT_FILE** The PKI applet provides several pseudo-files in which key and PIN values can be stored. This APDU is used to indicate which of these pseudo-files will be actually accessed by the next read, write, or file_size command.
- **READ_BINARY** This APDU allows the selected pseudo-file to be read. Five pseudo-files are used in this applet; see the description of the previous applet to better understand why this pseudo-file mechanism is used. Pseudo-file 2000 is used to store descriptor information with various fields protected by different PINs; that is, either the CO PIN or the User PIN. Pseudo-file 3000 is used to store an RSA public-key and a publicly available digital certificate in. Pseudo-file 3100 is used to store an RSA private-key. Pseudo-files 3200 and 3300 are used to store digital certificates in, but distribution of these certificates must be approved by the User; i.e. they're not innately publicly available. A READ_BINARY(3000) command is used to export the public key, stored in a digitally signed certificate form, from the card.

- **WRITE_BINARY** This APDU allows the selected pseudo-file to be written. A WRITE_BINARY(3100) command is used to zeroize the RSA Private-Key file on the card. A WRITE_BINARY (3000) command is used to store a certificate on the card.
- **FILE_SIZE** This APDU returns the size of the selected pseudo-file.
- **GET_CHV_POLICY** This APDU allows the authorization policy to be retrieved.
- **GET_CHV_MAX_LENGTH** This APDU establishes the maximum length of the PIN which can be stored in this applet.
- **SIGN**. This APDU uses an RSA private key to sign data. The RSA private key used in this operation must be generated off-card and loaded onto the card during the personalization operations performed by the CO prior to issuing the card.
- **VERIFY_CHV**. This APDU checks the PIN presented by the Card Holder against the current PIN.
- **CHANGE_CHV**. This APDU is used to change the current PIN value. A CHANGE_CHV command specifying a new PIN or all zeros is used to zeroize both the Card Holder PIN and the CO PIN.
- **GET_PIN_STATE** This APDU determines whether the PIN is in a blocked or an unblocked state.
- **LOGOUT_ALL** This APDU terminates the currently existing access conditions which have been established.
- **ALLOCATE_KEY_PAIR** This APDU allocates file space to hold an RSA public/private key pair.
- **FREE_KEY_PAIR** This APDU deletes an existing RSA public/private key pair.
- **UNWRAP_PRIVATE_KEY_INIT** This APDU initializes the decryption operation of a private key encrypted with the CO KEK for loading into the applet.
- **UNWRAP_PRIVATE_KEY** This APDU completes the transfer and decryption of a private key encrypted with the CO KEK for loading into the applet from off-card.
- **ASK_RANDOM** This APDU returns a nonce to an off-card element to be used in an external authentication operation.
- **UNBLOCK_CHV** This APDU is used by the CO to unblock the user PIN. To execute this command the CO must demonstrate knowledge of the CO PIN.

Role / Authentication Method vs. Services	No Role	Crypto-graphic Officer	Card Holder PIN
PKI Applet			
GET_INSTALL_DATA	X		
SIGN			X
GET_VERSION	X		
SELECT_FILE	X		
READ_BINARY (2000)	X		X
READ_BINARY (3000)	X		
READ_BINARY (3100)			X
READ_BINARY (3200)			X
READ_BINARY (3300)			X
WRITE_BINARY (2000) partial			X
WRITE_BINARY (2000) partial		X	
WRITE_BINARY (3000)		X	X
WRITE_BINARY (3100)		X	
WRITE_BINARY (3200)		X	
WRITE_BINARY (3300)		X	
FILE_SIZE	X		
GET_CHV_POLICY	X		
GET_CHV_MAX_LENGTH	X		
VERIFY_CHV	X		
CHANGE_CHV			X
LOGOUT_ALL	X		
ALLOCATE_KEYPAIR			X
FREE_KEY_PAIR			X
UNWRAP_PRIVATE_KEY_INIT		X	
UNWRAP_PRIVATE_KEY		X	
ASK_RANDOM	X		
UNBLOCK_CHV		X	

Table 2 -Roles & Possible ACR Configuration for PKI Applet Services

5.1.2.4.3 Smart Login Applet Services

The Smart Login Applet provides secure storage services. Each Smart Login applet instance corresponds to one storage area.

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

- **CHOOSE**. This APDU is used to select the specific data area in which account and password information is stored within the applet.
- **READ_BINARY**. This APDU is used to read data elements from the pseudo-file provided by this applet. In general, pseudo-file 2000 is used to store an “account name” and pseudo-file 2001 is used to store a “password”. This is not a password that in any way provides access to information on the card. Rather, it is a password that can be used by an application external to the card. Perhaps the best model is to think

of these two files being used to store the account and password necessary to allow a user's web browser to login to a remote web server account.

- **WRITE_BINARY**. This APDU is used to write information into the pseudo-file provided by this applet. Pseudo-file 2000 is used to store an "account name" and pseudo-file 2001 is used to store a "password".
- **GET_VERSION** This APDU is used to retrieve the version number of this on-card applet.
- **GET_SIZE** This APDU is used to retrieve the size of the file storage area within the applet (of the chosen file).

Role / Authentication Method vs. Services	**No Role**	**Crypto-graphic Officer**	**Card Holder PIN**
Smart Login Applet			
CHOOSE	**X**		
WRITE_BINARY(2000)			**X**
WRITE_BINARY(2001)			**X**
READ_BINARY (2000)	**X**		
READ_BINARY (2001)			**X**
GET_VERSION	**X**		
GET_SIZE	**X**		

Table 3 - Roles & possible ACR configuration for Smart Login applet services

5.1.3 Critical Security Parameters (CSPs)

5.1.3.1 Cryptographic Keys

The Schlumberger Cyberflex Access 32K Smart Card Module with Schlumberger PKI Applets includes one set of the following keys:

- Initialization Key, K_{init} used only for the first Card Manager key-set loading,
- Crypto Officer Security Domain keys as described below
- TDES Session keys (keys derived from Crypto Officer key set)

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

- $K_{enc,auth}$ used to derive session keys for Crypto Officer authentication and encrypted mode of the secure channel,
- K_{mac}, used to derive session key for MAC mode of the secure channel,
- K_{kek} used to encrypt keys, to be imported into the platform.

One to several RSA (public key – private key) pairs used in the PKI applet to perform digital signatures.

5.1.3.2 Other CSPs

The Schlumberger Cyberflex Access 32K Smart Card Module with Schlumberger PKI Applets includes two other types of CSPs:

- Two Personal Identification Numbers (PINs) in the PKI applet:
  - A Card Holder Verification PIN to authenticate the Card Holder
  - A PIN Unblock PIN used by the Crypto-Officer to unblock a blocked Card Holder PIN

The Card Holder PIN is 7-12 character (numeric) string that may be used to authenticate the Card Holder to the card. That is, by successfully entering a PIN sequence, a Card Holder can prove knowledge of a shared secret (the PIN) and thereby authenticate himself to the card. There is a general-purpose command available to the Crypto Officer to change or unblock a PIN. A “verify PIN” command is provided by the PKI applet.

6 Security Rules

6.1.1 Identification & Authentication Security Rules

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

6.1.1.1 User Identification and Authentication

- **User Authentication**: The User role is authenticated by proving knowledge of the Card Holder PIN.

6.1.1.2 Cryptographic Officer Identification &Authentication

- **Crypto Officer Authentication**: The Cryptographic Officer must generally prove the possession of the Card Manager Key Set composed of 3 TDES keys in order to authenticate his role. 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).

  For an unblock PIN operation, the Crypto Officer may communicate with the card through an unsecured channel and demonstrate knowledge of a CO PIN in order to authenticate his role. Thus, if the unblock PIN operation is performed through a secure channel the CO authenticates his role twice; once through knowledge of the key set and once through knowledge of the CO PIN. If performed through an unsecured channel, the CO must only show knowledge of the CO PIN in order to unblock the Card Holder's PIN.

6.1.2 Physical Security Rules

The physical security of the Schlumberger Cyberflex Access 32K Smart Card Module with Schlumberger PKI Applets 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 card is in possession of the Cryptographic Officer until it is ultimately issued to the end user.

6.1.3 Key Management Security Policy

6.1.3.1 Cryptographic key generation

The RSA key pair is generated off-card and imported onto the card to be used in the PKI Applet. The public-key is used externally from the card by being included on a digital certificate establishing the relationship between the public-key and the role of the Card Holder. The private-key, which is retained securely within the PKI Applet, is used to establish the role of the Card Holder by forming a digital signature.

6.1.3.2 Cryptographic key entry/output

Keys are input to the Card Manager in encrypted format, using the Put Key command within a secure channel. During this process, the keys are double encrypted (using the Session Key and the K_{kek} Key).

An RSA private is input to the PKI applet using the UNWRAP_PRIVATE_KEY_INIT and the UNWRAP_PRIVATE_KEY (APDU) commands. These two commands are used in concert to load an RSA private key, generated off-card, into the PKI applet. The private key is encrypted using the K_{kek} key of the Crypto Officer.

6.1.3.3 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.

6.1.3.4 Cryptographic key destruction

The card destroys cryptographic keys by reloading another key-set for Crypto Officer keys or closing of secure channel for session keys. RSA key pairs are zeroized by the Free Key Pair command.

Key Management Details can be found in a specific proprietary document.

6.1.4 Mitigation of attacks Security Policy

The Schlumberger Cyberflex Access 32K Smart Card Module with Schlumberger PKI Applets has been designed to mitigate the following attacks:

- Simple Power Analysis,
- Differential Power Analysis.

6.1.5 Approved Mode of Operation

The Schlumberger Cyberflex Access 32K Smart Card Module with Schlumberger PKI Applets can be configured to operate in the Approved mode of operation if the following rules are followed:

- Applets must be instantiated with their access control rules set per Section 5.1.2 of this document.
- Module services performed must be limited to those listed in Section 5.1.2 of this document.

7 Security Policy Check List tables

7.1 Roles & Required Authentication

Role	Type of authentication	Authentication data
Crypto Officer	TDES authentication PIN authentication	TDES keys (Crypto Officer Security Domain) CO PIN
User	User PIN	User PIN

7.2 Strength of authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
TDES authentication PIN	High 1:10,000,000 (minimum)

7.3 Services authorized for Roles

Role	Services
Crypto Officer	All CO Services as listed in Section 5.1.2.1 and all CO APIs, as listed in Section 5.1.2.4
User	Only Card Holder Services as listed in Section 5.1.2.4

7.4 Access Rights within Services

Service	CSP	Types of Access (eg. Read, Write, Execute)
Crypto Officer (CO)	TDES CO Keys	Execute
	TDES CO Keys	Write (PUT KEY command)
	CO PIN	Write(PIN CHANGE command)
	RSA Private Key(s)	Write (Unwrap Privet Key)
	RSA Private Key(s)	Execute (Sign)
User	User PIN	Read (Verify CHV)
	User PIN	Write (Change CHV)

7.5 Mitigation of Other Attacks

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

8 References

1. Global Platform - Open Platform – Card Specification v2.0.1 – 7 April 2000.