# Security Policy

# For

# ActivCard Applet suite on

# SchlumbergerSema Cyberflex Access 32K

Public Version 1.6

# TABLE OF CONTENTS

# 1 Scope of Document

This document defines the Security Policy for the module: “ActivCard Applet suite on SchlumbergerSema Cyberflex Access 32K”. Included are a description of the basic security requirements for the module and a qualitative description of how each security requirement is achieved.

# 2 Introduction

The ActivCard Applet suite on SchlumbergerSema Cyberflex Access 32K offers JavaCard 2.1 and Open Platform 2.0.1’ services to applets on the card such as ActivCard Applet Suite.

The Open Platform (OP) Version 2.0.1’ specification, combined with JavaCard 2.1 defines a secure infrastructure for post-issuance programmable smart cards. The OP specification defines a life cycle for OP compliant cards. OP State transitions between states of the life cycle involve well-defined sequences of operations. Cards that have been issued to a Cardholder are necessarily in an OP “SECURED” state. This means that a defined set of applications have been loaded onto the card plus a set of keys and a PIN through which the roles of the Cryptographic Officer and the Cardholder can be authenticated.

The SchlumbergerSema Cyberflex Access 32K smart card is referred as the “smart card platform” in this document.

The ActivCard applets submitted for FIPS evaluation are:

- ID applet, v 1.0.0.19
- PKI (Public Key Infrastructure) applet, v 1.0.0.23
- GC (Generic Container) applet, v 1.0.0.18
- Fingerprint Match On Card (MOC) applet, v 1.0.0.10

The ID applet offers Card Holder Verification (CHV) services to off-card entities.
The PKI Applet offers RSA-based cryptographic services to off-card entities.
The GC Applet offers secure storage services to off-card entities.
The Fingerprint MOC Applet offers fingerprint based Cardholder enrollment and verification services to off-card entities. The MOC applet relies on Precise Biometrics JavaCard library for fingerprint verification on card.

# 3 Security Levels

The ActivCard Applet suite on SchlumbergerSema Cyberflex Access 32K (cryptographic module) meets the overall requirements applicable to Level 2 security of FIPS 140-1. The individual security requirements specified for FIPS 140-1 meet the level specifications indicated in the following table.

| Security Requirements Section | Level |
|---|---|
| Cryptographic Module | 2 |

| | |
|---|---|
| Module Interfaces | 2 |
| Roles and Services | 2 |
| Finite State Machine | 2 |
| Physical Security | 3 |
| Software Security | 3 |
| Operating System Security | N/A |
| Key Management | 2 |
| Cryptographic Algorithms | 2 |
| EMI/EMC | 2 |
| Self-Tests | 2 |

## 3.1 Cryptographic Module Specification

ActivCard Applet suite on SchlumbergerSema Cyberflex Access 32K is an ID-1 class smart card that adheres to the various ISO/IEC specifications for Integrated Circuit Chip (ICC) based identification cards. The "cryptographic boundary" for the ActivCard Applet suite on SchlumbergerSema Cyberflex Access 32K vis-à-vis the FIPS 140-1 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. The module is constructed so as to provide the tamper resistance and the tamper evidence required in the FIPS 140-1 physical Level 3 validation.

ActivCard Applet suite on SchlumbergerSema Cyberflex Access 32K is a single chip implementation of a cryptographic module.

## 3.2 Module Interfaces

The electrical and physical interface of the ActivCard Applet suite on SchlumbergerSema Cyberflex Access 32K, 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:

### *3.2.1 Physical Interface Description*

The ActivCard Applet suite on SchlumbergerSema Cyberflex Access 32K 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 |

#### 3.2.1.1 Electrical Specifications

Specific electrical functions of the contacts:

| Contact | Function |
|---|---|
| C1 | Vcc supply voltage 5V +/- 0.5V |
| C2 | RST (Reset) |
| C3 | CLK (Clock) |
| C4 | RFU (Reserved for Future Use) |
| 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.

### *3.2.2 Logical Interface Description*

Once electrical (physical) contact and data link layer contact is established between the card and the CAD, 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 Cyberflex 32K and ActivCard Applet Suite technical specification documents that are included as a proprietary and private extension to this Security Policy.

This card also provides an additional set of on-card services through the Java Card APIs. The API classes and their associated methods are also defined in the technical specification documents mentioned in the previous section..

## 3.3 Roles and Services

The ActivCard Applet suite on SchlumbergerSema Cyberflex Access 32K supports two User roles, a Cardholder and an Application Operator, and one Cryptographic Officer role.  See section 4 for a complete description of Roles and Services.

## 3.4 Finite State Machine Model

The ActivCard Applet suite on SchlumbergerSema Cyberflex Access 32K is compliant with the ISO/IEC 7816-3,4 specifications. This means that the card communicates via Application Protocol Data Unit packets transferred from the CAD to the card, followed by a response APDU from the card back to the CAD. Within this protocol, the card functions as a pure, finite state machine. The card's system software undergoes a set of well-defined state transitions, as keys are stored on the card to establish Security Domains. Applets also progress through a set of well-defined state transitions as they are loaded, installed, and prepared for execution.

The Finite State Model for the ActivCard Applet suite on SchlumbergerSema Cyberflex Access 32K is published as a separate document.

### 3.5 Physical Security

The physical security of the ActivCard Applet suite on SchlumbergerSema Cyberflex Access 32K is designed to meet FIPS 140-1 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 User. From that point, the card is in the physical possession of the User.

To attack the cryptographic information contained in the module, which is to attempt to compromise this information, requires physical access to the card. To eavesdrop on normal activities of the module, while it is still in possession of either the Cryptographic Officer or of the User, will be demonstrated to be difficult or impossible due to the protocols and security mechanisms protecting access to the module's information and services. To eavesdrop on the module through extraordinary means requires physical possession of the card. In this event, the absence of the card is detected by either the Cryptographic Officer or the User and the capabilities of the card within a larger systems context can be disabled.

If the module is attacked through physical means, the chip provides tamper evidence due to the disturbance of the packaging of the module. The ICC is embedded within an epoxy coating that is extremely difficult to penetrate without leaving evidence of the attack. Further, the packaging itself is resistant to penetration.

### 3.6 Software Security

The basic systems software of ActivCard Applet suite on SchlumbergerSema Cyberflex Access 32K is secure from modification due to the fact that it is stored in ROM. This systems software is written primarily in the C programming language that allows for extensive review to confirm security.

- Software security of the ActivCard Applet suite on SchlumbergerSema Cyberflex Access 32K is strictly controlled by the Card Manager application

The card systems software includes an on-card 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 communication directly; any such communication must go by way of systems software mechanisms, which allow for implementation of strict security measures. No applet source code may be loaded onto the card after completion of the manufacturing process.

### 3.7 Operating System Security

This section is not applicable to this certification due to the fact that no applet source code may be loaded onto the card after completion of the manufacturing process.

### 3.8 Key Management

The smart card module includes the following keys:

- Initialization Key, $K_{init}$ used only for the first Card Manager key-set loading,
- Security Domain sets containing three types of keys:
  1. $K_{enc,auth}$ used for Cryptographic Officer authentication per OP Specification
  2. $K_{mac}$, used for Cryptographic Officer authentication per OP Specification
  3. $K_{ek}$ used as Key Wrapping Key for inputting security domain key sets into the module
- Application Operator TDES keys for accessing services provided by ActivCard applet suite.
- Card Holder RSA key pairs.

The module contains an ANSI X9.17 PRNG for generation of RSA key pairs.

### 3.9 Cryptographic Algorithms

The following algorithms are performed by the ActivCard Applet suite on SchlumbergerSema Cyberflex Access 32K.

- TDES CBC, ECB
- SHA-1
- RSA Signature (PKCS #1 compliant)

### 3.10 EMI/EMC

The ActivCard Applet suite on SchlumbergerSema Cyberflex Access 32K has been tested to meet the EMI/EMC requirements specified by FCC Part 15, Subpart J, Class A

### 3.11 Self-tests

The ActivCard Applet suite on SchlumbergerSema Cyberflex Access 32K performs the required set of self-tests at power-up time. When the ActivCard Applet suite on SchlumbergerSema Cyberflex Access 32K is inserted into a CAD, once power is applied to the card (contact) interface, a “Reset” signal is sent from the CAD 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 cleared at Reset
- EEPROM integrity check
- Algorithm (known answer) tests for:
- TDES
- 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 CAD while the self-tests are being performed.

# 4 Roles and Services

The module ActivCard Applet suite on SchlumbergerSema Cyberflex Access 32K insures the authentication of off-card entities and provides them with cryptographic services according to their role.
Three distinct authenticated roles are supported by the on-card cryptographic system: the Cardholder, the Application Operator, and the Cryptographic Officer roles

## 4.1 User Roles

- **Cardholder** - The Card Holder is responsible for insuring the ownership of his card and for not communicating his PIN. The Cardholder is authenticated by verification of a PIN , or by submitting his fingerprint(s).PIN and fingerprint authentication are used interchangeably, i.e. a service requiring Card Holder authentication can be obtained by either entering his PIN/password, or by submitting his fingerprint(s).
- **Application Operator** – The Application Operator represents an off-card entity operating an external application requesting the services offered by the applets. The applet authenticates the Application Operator role by verifying the possession of a 3DES key.

## 4.2 Cryptographic Officer Role

The Cryptographic Officer owns a OP Card Manager or OP Security Domain Key Set. He mutually authenticates to the OP Card Manager and accesses the OP Card Manager services by establishing a secure channel with that key set.The OP Card Manager is the controlling application on the card, and provides services for content, status and key management on the card.. The Cryptographic Officer is also responsible for managing the security configuration of the applets, and in particular executes the necessary PIN, fingerprint(s) management and key management operations for the applet: The Cryptographic Officer has the privilege to unblock the PIN, after successive wrong PIN values have been tried, and to reset the fingerprint matching counter, after successive mismatch of fingerprint(s) have been attempted.

## 4.3 Any Role

This role is allowed to access services that do not require any authentication. This role is needed for example, so that certain card information can be obtained prior to services that require authentication.

## 4.4 Role Authentication

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.

### *4.4.1 User Authentication*

- **PIN**: the Card Holder must send either 1) a Verify PIN command, or 2) a Verify Match command with fingerprint(s) data, to any applet to access any Applet service protected with PIN. The APDU corresponding to the applet service must be sent before the card is removed or a reset order is send to the card.

- **PIN Always**: the Card Holder must send a Verify PIN command to any applet to access any applet service protected with PIN Always
- **External Authentication (XAUT)**: The Application Operator must prove the possession of a particular TDES key to access the GC Applet read or update service protected with External Authentication with this particular key.

### *4.4.2 Cryptographic Officer Authentication*

- **OP Authentication**: The Cryptographic Officer must prove the possession of a 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.
- **External Authentication (XAUT)**: The Cryptographic Officer must prove the possession of a particular TDES key to access the ID Applet PIN unblock service protected with External Authentication with this particular key..

## 4.5 Services

In the following, the applet services are explained in detail. In addition, a table that describes what roles can access what services (or what services are available to what roles) is presented. The first column of the table lists the services (corresponding to APDU name), and the first column corresponds to the roles, followed by the authentication method required for that role. Certain combinations of roles are explicitly defined and access control rules can be set to enforce them.

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

### *4.5.1 ID Applet Services*

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

- **Select**: This APDU causes the selection of the applet.
- **Install**: This APDU causes the installation of the applet.
- **Change PIN/Unblock**.
  - The Change PIN APDU is used by the cryptographic officer to set a new PIN value and recover Card Holder access.
  - the Change PIN APDU is also used by the Card Holder to set a new PIN value upon presentation of the current PIN
- **Get Properties**. This APDU is used to obtain information about applet instance configuration.
- **Initialize update**. This APDU corresponds to the OP secure channel specification.
- **External Authenticate**. This APDU corresponds to the OP secure channel specification.
- **Verify CHV**. This APDU checks the PIN presented by the Card Holder
- **Put Key**. This APDU is used to set the XAUT key used to unblock the PIN, and must be used with the Key Wrapping Key. The APDU format is compliant with OP specification.

- **Get Challenge**. This APDU is used in combination with AC external Authenticate to perform an external authentication of the Cryptographic Officer in order to unblock the PIN.
- **AC External Authenticate**. This APDU is used in combination with a Get Challenge, this APDU is used to unblock the PIN.
- **Change PIN after First Use**. This APDU indicates that the Card Holder must change his PIN before any PIN protected service can be accessed.
- **Set Status**: This APDU is sent when the applet instance life cycle needs to be changed. The applet instance life cycle can be: SELECTABLE, BLOCKED, PERSONALIZED
- **Set Application UID**: This APDU is sent when the UID associated with the applet instance needs to be changed

| **Role / Authentication Method Vs. Services** | Any Role / None | Crypto-graphic Officer SECURE CHANNEL | Crypto-graphic Officer XAUT | Card Holder PIN |
|---|---|---|---|---|
| **ID Applet** | | | | |
| INSTALL | | X | | |
| CHANGE PIN/UNBLOCK | | X | X | X |
| GET PROPERTIES | X | | | |
| INITIALIZE UPDATE | X | | | |
| EXTERNAL AUTHENTICATE | | X | | |
| VERIFY CHV | | | | X |
| PUT KEY | | X | | |
| GET CHALLENGE | X | | | |
| AC EXTERNAL AUTHENTICATE | | | X | |
| CHANGE PIN AFTER FIRST USE | X | | | |
| SET STATUS | | X | | |
| SET APPLICATION UID | | X | | |

Table 1 - Roles & Possible ACR Configuration for ID Applet Services
Only FIPS-modes are represented in this chart.

### *4.5.2 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.
- **Initialize update**. This APDU follows the OP secure channel specification.

- **External Authenticate**. This APDU follows the OP secure channel specification.
- **Generate Key Pair**. This APDU is used to generate a Key Pair in the Smart Card.
- **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.
- **Put Key**. This APDU is used to import/unwrap the Private Key. The APDU format follows OP specification.
- **Set Status**: This APDU is sent when the applet instance life cycle needs to be changed. The applet instance life cycle can be: SELECTABLE, BLOCKED, PERSONALIZED
- **Set Application UID**: This APDU is sent when the UID associated with the applet instance needs to be changed

| **Role / Authentication Method Vs. Services** | Any Role / None | Crypto-graphic Officer SECURE CHANNEL | Card Holder PIN | Card Holder PIN ALWAYS | NEVER |
|---|---|---|---|---|---|
| **PKI Applet** | | | | | |
| INSTALL | | X | | | |
| GET PROPERTIES | X | | | | |
| INITIALIZE UPDATE | X | | | | |
| EXTERNAL AUTHENTICATE | | X | | | |
| GENERATE KEY PAIR | | X | X | X | X |
| GET CERTIFICATE | X | | X | X | X |
| SIGN | | | X | X | X |
| PIN VERIFY | | | X | X | |
| PUT KEY | | X | | | |
| SET STATUS | | X | | | |
| SET APPLICATION UID | | X | | | |

Table 2 -Roles & Possible ACR Configuration for PKI Applet Services
Only FIPS-modes are represented in this chart.

### *4.5.3 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:

- **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.
- **Initialize update**. This APDU follows the OP secure channel specification.
- **External Authenticate**. This APDU follows the OP secure channel specification.

- **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.
- **Get Challenge**. This APDU is used in combination with GC external Authenticate to perform an external authentication.
- **Put Key**. This APDU imports/unwraps the XAUT keys. The APDU format follows OP specification..
- **GC External Authenticate**. This APDU communicates the cryptogram obtained by TDES encryption of a card challenge with the TDES key associated to the service protected by XAUT.
- **PIN Verify**. This APDU checks the PIN presented by the Card Holder against the current PIN.
- **Set Status**: This APDU is sent when the applet instance life cycle needs to be changed. The applet instance life cycle can be: SELECTABLE, BLOCKED, PERSONALIZED
- **Set Application UID**: This APDU is sent when the UID associated with the applet instance needs to be changed

| **Role / Authentication Method Vs. Services** | Any Role / None | Crypto-graphic Officer SECURE CHANNEL | Card Holder PIN | Card Holder PIN ALWAYS | Application Operator XAUT | A.O. or C.H. XAUT or PIN | A.O. and C.H. XAUT then PIN |
|---|---|---|---|---|---|---|---|
| **GC Applet** | | | | | | | |
| INSTALL | | X | | | | | |
| GET PROPERTIES | X | | | | | | |
| INITIALIZE UPDATE | X | | | | | | |
| EXTERNAL AUTHENTICATE | | X | | | | | |
| UPDATE BUFFER | X | X | X | X | X | X | X |
| READ BUFFER | X | X | X | X | X | X | X |
| GET CHALLENGE | X | | | | | | |
| PUT KEY | | X | | | | | |
| GC EXTERNAL AUTHENTICATE | | | | | X | | |
| PIN VERIFY | | | X | X | | | |
| SET STATUS | | X | | | | | |
| SET APPLICATION UID | | X | | | | | |

Table 3 - Roles & possible ACR configuration for GC applet services
Only FIPS-modes are represented in this chart.

### 4.5.4 *Fingerprint Match on Card Applet Services*

The Fingerprint Match on Card (MOC) applet provides an alternative to PIN verification. Multiple fingerprints can be matched. For each fingerprint, a pair of templates, one public, one private, are stored in the card during enrollment. The user live fingerprint, processed with a public template retrieved from the card by middleware, is sent to the card to perform the match with the private template on card securely. If match succeeds, a PIN previously stored in the Fingerprint MOC applet is used to authenticate the user to the card.
The following are the list of APDU/services provided by the Fingerprint MOC applet:

- **Enroll Public Template**: This APDU is used to record the public minutia template in the card;
- **Enroll Private Template**: This APDU is used to record the private minutia template in the card;
- **Delete Finger Template**: This APDU is used to delete the registration of a template in the card;
- **Read Public Template**: This APDU is used to retrieve the public minutia template from the card;
- **Verify Match**: This APDU is used to perform the matching of a live user fingerprint with the one recorded in the card;
- **Get Properties**: This APDU is used to retrieve applet instance properties from the card;
- **Initialize update**. This APDU follows the OP secure channel specification. It is the first message for setting up OP secure channel by mutual authenticating an off-card entity and the card. Secure channel is not set at this point;
- **External Authenticate**. This APDU follows the OP secure channel specification. It is the second message for setting up OP secure channel by mutual authenticating an off-card entity and the card. Secure channel is set at this point.
- **Put Key**. This APDU imports/unwraps the TDES XAUT keys. The APDU format follows OP specification. This XAUT key is used to reset the Fingerprint MOC matching counter when fingerprint matching is blocked due to multiple unsuccessful matching attempts.
- **Get Challenge**. This APDU is used in combination with AC external Authenticate to perform an external authentication.
- **AC External Authenticate**. This APDU communicates the cryptogram obtained by TDES encryption of a card challenge with the TDES key associated to the service – here to reset the Fingerprint MOC counter – protected by XAUT
- **PIN Verify**. This APDU checks the PIN presented by the Card Holder against the current PIN associated with the ID applet instance;
- **Trace PIN**. This APDU is used to copy the PIN value installed in the IP applet to the Fingerprint MOC applet. This APDU is necessary before performing fingerprint authentication.
- **Set Status**: This APDU is sent when the applet instance life cycle needs to be changed. The applet instance life cycle can be: SELECTABLE, BLOCKED, PERSONALIZED.
- **Set Application UID**: This APDU is sent when the UID associated with the applet instance needs to be changed.

| **Role<br>/<br>Authentication Method<br>Vs.<br>Services** | Any Role<br>/<br>None | Crypto-graphic Officer<br>SECURE CHANNEL | Crypto-graphic Officer<br>XAUT | Card Holder<br>PIN |
|---|---|---|---|---|
| **ID Applet** | | | | |
| INSTALL | | X | | |

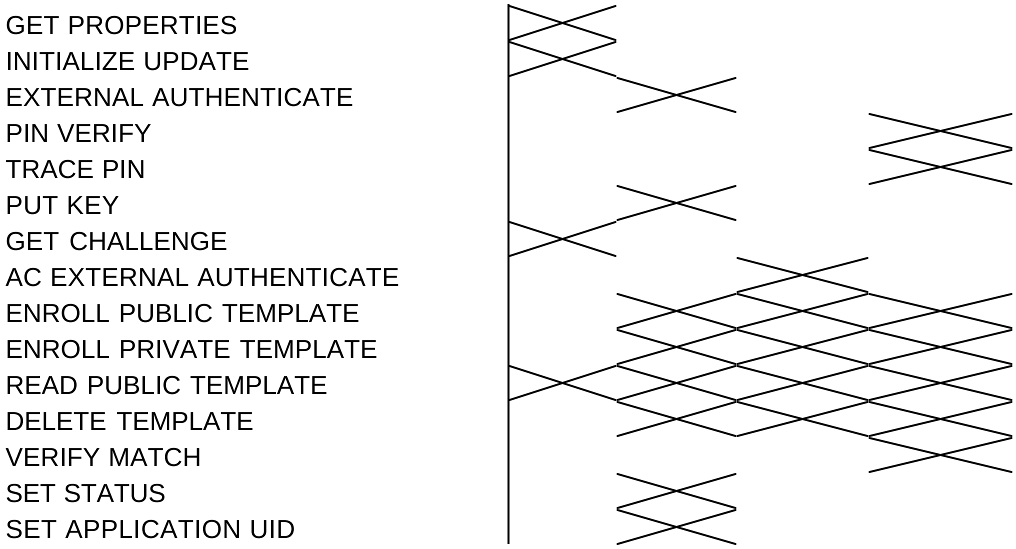

Table 4 - Roles & possible ACR configuration for Fingerprint MOC applet services
Only FIPS-modes are represented in this chart.

# 5 Security Rules

## 5.1 Applet environment

- The applets must be installed within a FIPS 140-1 certified smart card.
- The applets must be installed on a smart card platform offering Java Card and Open Platform (or Global Platform) services.
- The Card Holder must take the necessary measures to insure that the terminal and/or the Card Acceptance Device are controlled by a valid role: Card Holder, Application Operator or Cryptographic Officer.

## 5.2 Content Management

- The management of the life cycle of the applets – load, instantiate, delete, personalize keys, shall follow the Open Platform standard.
- Content management, status management and key management APDU commands (such asinstantiate, delete, put key) are protected by OP authentication.
- The instantiation of applet instances may either occur at pre-issuance, issuance or at post-issuance by any entity owning Open Platform key sets of the Card Manager..
- There may be as many instances of each applet as there are available smart card resources.

## 5.3 Role Authentication

- The applets shall provide the following distinct operator roles: The user role – Application Operator or Card Holder, and Cryptographic officer role.
- The applets shall provide role-based authentication.
- Cryptographic services are restricted to authenticated roles.

- The Role authentication methods (ACRs) for each applet service are set by the Cryptographic officer during Applet instantiation and cannot be modified during the lifetime of the applet instance.
- To ensure that only FIPS certified services are provided, the ACRs must be set according to section 4.5 Tables (Role/Authentication Methods vs. Services).
- When authentication of the role cannot be performed because the related key or password or key attributes are missing, the corresponding service must be disabled.
- The results of authentication must be set in transient memory and therefore cleared when the module is powered down.
- The Applet instance configuration may require the combined authentication of different roles to access a particular service. For instance the Application Operator and then the Card holder must both authenticate themselves to access the UpdateBuffer service.
- The Card  Holder can access services requiring Application Operator authentication after the Application Operator has been authenticated successfully.
- The Application Operator can access services requiring Card Holder authentication by PIN after the Card Holder has been authenticated successfully. This rule is not applicable for services requiring Card Holder authentication with PIN ALWAYS.
- To perform fingerprint authentication with the Fingerprint MOC applet, an ID applet must be instantiated, and not in blocked state.

## 5.4 Key management

- RSA private keys and TDES keys must be transported encrypted to the card.

## 5.5 PIN management

- The password or PIN that is used by the applet to authenticate the Card Holder must not be divulged to other parties than the Card Holder.
- The ID applet must be configured by the cryptographic officer so that:
  - After 1<= M <= 127 consecutive unsuccessful PIN code validation attempts, the Card Holder services must be disabled. (eg. The PIN is blocked)
  - After 1<= N <= 127 consecutive unsuccessful PIN unblocking attempts with incorrect key or parameters, the card Holder services are permanently disabled (eg. The PIN is locked)
  - The PIN length P must be configured as follows:  4 <= P <= 8  binary  bytes.

## 5.6 Fingerprint MOC management

- The public and private templates stored in the card during enrollment are used to authenticate a user during live fingerprint matching, and must be protected accordingly.
- The Fingerprint MOC must be configured by the cryptographic officer so that:
  - After 1 <= M <= 127 consecutive unsuccessful live fingerprint matching attempts, the Card Holder services must be disabled (Applet BLOCKED)
  - The Card Holder services/Applet can only be unblocked by Cryptographic Officer using secure channel or Application Operator using XAUT key.

# 6 Definition of Security Relevant Data Items

## 6.1 List of SRDIs

The following Security Relevant Data Items (SRDIs) are managed from the applets:

- **Authentication Method (or ACR)**: These data elements define the Authentication Method that is permanently set for the service. The ACRs are set by the Cryptographic Officer upon applet instantiation.
- **Open Platform Applet life cycle states**: The applet status information (PERSONALIZED, BLOCKED, SELECTABLE). These states are managed by the Card Manager, but the state transitions are managed from the applets.
- **External Authentication Keys**: These are TDES keys that enable the authentication of Application Operators (GC read / GC Write) or Cryptographic Officers (PIN Unblock).
- **RSA private keys**: are managed (generated, unwrapped) from the PKI applet using the java card cryptographic services. These keys are used to sign data.
- **RSA public keys**: Public keys are generated on card from the RSA key pair generation, and exported off card.
- **X.509 Certificates**: The certificates corresponding to the private keys present in the card are managed by the applets.
- **Personal Identification Numbers or passwords (**PIN): PINs and PIN attributes are managed from the ID applet, which relies on the Java Card PIN management service.
- **Public Fingerprint Template:** The public fingerprint template and associated attributes are used by fingerprint middleware to obtain matching data from a live fingerprint.
- **Private Fingerprint Template:** The private fingerprint template and associated attributes are used inside the card to process the matching data of a live fingerprint. It never leaves the card.
- **Open Platform Key Sets:** are managed by the card manager or security domain. These keys enable the authentication of the Cryptographic Officer, and the encryption of inputted keys.  They are inputted into the module via the Put Key command.

## 6.2 Access to SRDIs vs. Services

The following matrices show for each applet how services access SRDIs.

### *6.2.1 PIN Applet*

| **PIN applet**<br>Columns: Services(roles)<br>Rows: Access to SRDIs | **Card Holder** | **Cryptographic Officer** | INSTALL-instantiate (C.O) | CHANGE PIN/UNBLOCK(C.O) | GET PROPERTIES(any) | INITIALIZE UPDATE(any) | EXTERNAL AUTHENTICATE(C.O) | VERIFY CHV(C.H) | PUT KEY(C.O) | GET CHALLENGE(any) | AC EXTERNAL AUTHENTICATE(C.O) | CHANGE PIN AFTER FIRST USE(any) | Set Status |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Access Control Rules** | | | | | | | | | | | | | |
| Install ACR | | ☒ | ☒ | | | | | | | | | | |
| **PIN or Password** | | | | | | | | | | | | | |
| Install PIN | | ☒ | ☒ | | | | | | | | | | |
| Change/Unblock PIN | ☒ | ☒ | | ☒ | | | | | | | | | |
| Verify PIN | ☒ | | | | | | | ☒ | | | | | |
| **External Authentication Keys** | | | | | | | | | | | | | |
| Delete key | | ☒ | | | | | | | ☒ | | | | |
| Import key | | ☒ | | | | | | | ☒ | | | | |
| Verify cryptogram | | ☒ | | ☒ | | | | | | | ☒ | | |
| **Card Manager Key set** | | | | | | | | | | | | | |
| Verify Cryptogram | | ☒ | | ☒ | | | ☒ | | ☒ | | | | |
| Decrypt APDU payload | | ☒ | | ☒ | | | | | ☒ | | | | |
| **Applet Instance Status** | | | | | | | | | | | | | |
| Change Status | | ☒ | | | | | | | | | | | ☒ |

### *6.2.2 PKI Applet*

**PKI applet services**
Columns: Services(roles)
Rows: Access to SRDIs

| | ***Card Holder*** | ***Cryptographic Officer*** | INSTALL instantiate (C.O) | GET PROPERTIES (any) | INITIALIZE UPDATE(any) | EXTERNAL AUTHENTICATE(C.O) | GENERATE KEY PAIR (C.O or CH) | GET CERTIFICATE(any) | SIGN(C.H) | Set Status | PIN VERIFY(C.H) | | PUT KEY(C.O) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Access Control Rules** | | | | | | | | | | | | | |
| Install ACR | | ☒ | ☒ | | | | | | | | | | |
| **PIN or Password** | | | | | | | | | | | | | |
| Verify PIN | ☒ | | | | | | | | | | ☒ | | |
| **RSA Key Pair** | | | | | | | | | | | | | |
| Generate Key Pair | ☒ | ☒ | | | | | ☒ | | | | | | |
| Import CRT components | | ☒ | | | | | | | | | | ☒ | |
| Delete private key | | ☒ | | | | | | | | | | ☒ | |
| Sign data | ☒ | | | | | | | | ☒ | | | | |
| **Card Manager Key set** | | | | | | | | | | | | | |
| Verify Cryptogram | | ☒ | | | | | | | | | | ☒ | |
| Decrypt Data | | ☒ | | | | ☒ | | | | | | ☒ | |
| **Applet Instance Status** | | | | | | | | | | | | | |
| Change Status | | ☒ | | | | | | | | ☒ | | | |

### 6.2.3 GC Applet

| **GC applet services**<br>Columns: Services(roles)<br>Rows: Access to SRDIs | **Card Holder** | **Cryptographic Officer** | **Application Operator** | INSTALL (Instantiate) | GET PROPERTIES (any) | INITIALIZE UPDATE (any) | EXTERNAL AUTHENTICATE (C.O) | Set Status | UPDATE BUFFER (C.0 or A.O or C.H) | READ BUFFER (C.0 or A.O or C.H) | GET CHALLENGE (any) | PUT KEY (C.O) | GC EXTERNAL AUTHENT(A.0) | PIN VERIFY (C.H) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Access Control Rules** | | | | | | | | | | | | | | |
| Install ACR | | ☒ | | ☒ | | | | | | | | | | |
| **PIN or Password** | | | | | | | | | | | | | | |
| Verify PIN | ☒ | | | | | | | | | | | | | ☒ |
| **External Authentication Keys** | | | | | | | | | | | | | | |
| Delete key | | ☒ | | | | | | | | | | ☒ | | |
| Import key | | ☒ | | | | | | | | | | ☒ | | |
| Verify cryptogram | | | ☒ | | | | | | | | | | ☒ | |
| **Card Manager Key set** | | | | | | | | | | | | | | |
| Verify Cryptogram | | ☒ | | | | | | | ☒ | ☒ | | ☒ | | |
| Decrypt Data | | ☒ | | | | | ☒ | | ☒ | ☒ | | ☒ | | |
| **Applet Instance Status** | | | | | | | | | | | | | | |
| Change Status | | ☒ | | | | | | ☒ | | | | | | |

### 6.2.4 Fingerprint MOC Applet

| **Fingerprint MOC applet**<br>Columns: Services(roles)<br>Rows: Access to SRDIs | **Card Holder** | **Cryptographic Officer** | INSTALL-instantiate (C.O) | GET PROPERTIES(any) | ENROLL PUBLIC TEMPLATE | ENROLL PRIVATE TEMPLATE | DELETE FINGER TEMPLATE | READ PUBLIC TEMPLATE | VERIFY MATCH | INITIALIZE UPDATE(any) | EXTERNAL AUTHENTICATE(C.O) | VERIFY CHV(C.H) | TRACE PIN | PUT KEY(C.O) | GET CHALLENGE(any) | AC EXTERNAL AUTHENTICATE(C.O) | Set Status |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Access Control Rules** | | | | | | | | | | | | | | | | | |
| Install ACR | | ☒ | ☒ | | | | | | | | | | | | | | |
| **PIN or Password** | | | | | | | | | | | | | | | | | |
| Verify PIN | ☒ | | | | | | | | | | | ☒ | | | | | |
| Trace PIN | ☒ | | | | | | | | | | | | ☒ | | | | |
| **Finger print template** | | | | | | | | | | | | | | | | | |
| Enroll public template | ☒ | ☒ | | | ☒ | | | | | | | | | | | | |
| Enroll private template | ☒ | ☒ | | | | ☒ | | | | | | | | | | | |
| Delete template | ☒ | ☒ | | | | | ☒ | | | | | | | | | | |
| Read public template | ☒ | ☒ | | | | | | ☒ | | | | | | | | | |
| Verify Match | ☒ | ☒ | | | | | | | ☒ | | | | | | | | |
| **External Authentication Keys** | | | | | | | | | | | | | | | | | |
| Delete key | | ☒ | | | | | | | | | | | | ☒ | | | |
| Import key | | ☒ | | | | | | | | | | | | ☒ | | | |
| Verify cryptogram | | ☒ | | | | | | | | | | | | | | ☒ | |
| **Card Manager Key set** | | | | | | | | | | | | | | | | | |
| Verify Cryptogram | | ☒ | | | | | | | | | ☒ | | | ☒ | | | |
| Decrypt APDU payload | | ☒ | | | | | | | | | | | | ☒ | | | |
| **Applet Instance Status** | | | | | | | | | | | | | | | | | |
| Change Status | | ☒ | | | | | | | | | | | | | | | ☒ |

## 7 References

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