ActivCard

axalto

ActivCard Digital Identity Applet Suite v 1.1.5 on Cyberflex Access 64k v2

FIPS140-2 Level 2

Cryptographic Module Security Policy

Version 1.3

ActivCard

axalto

Table of Contents

1. INTRODUCTION

This document defines the Security Policy for the "ActivCard Digital Identity Applet Suite v1.1.5 on Cyberflex Access 64k v2" cryptographic module, submitted for validation, in accordance with FIPS140-2 Level 2 standard. Included is a description of the security requirements for the module and a qualitative description of how each security requirement is achieved. In particular, this security policy specifies the security rules under which the cryptographic module must operate.

2. OVERVIEW

2.1 AXALTO CYBERFLEX ACCESS 64K V2 CRYPTOGRAPHIC MODULE

The Axalto Cyberflex Access 64k v2 cryptographic module loads and runs applets written in the Java programming language. The Cyberflex Access 64K v2 cryptographic module contains a microprocessor and EEPROM to provide processing capability and memory for storing instructions and data. The module can be used to store and update account information, personal data, and even monetary value. The module, when placed in a plastic smart card housing, is ideal for secure Internet access, purchases, portable digital telephones, and for benefit programs and health care applications. Cyberflex Access 64k v2 cryptographic module, when housed in smart card housing, brings new services, as well as increased security, portability, and convenience, to computer applications.

The Cyberflex Access 64k v2 cryptographic module combines the advantages of the Java programming language and cryptographic services with those of the cryptographic module. The security of Cyberflex Access 64k v2 cryptographic module comes from both software and hardware. Data integrity and security are provided through cryptographic services, Java features, and the Systems Software. In addition, the cryptographic module hardware provides a tamper-resistance and tamper-evidence features, that meets FIPS140-2 Level 3 physical security requirements.

The Cyberflex Access 64k v2 cryptographic module contains an implementation of the Java Card ™ specification (JC) Version 2.1.1 and of the Open Platform (OP) Version 2.0.1 specification, which defines a secure infrastructure for post-issuance programmable cryptographic module housed in a smart card housing. The JC specification defines Java Card ™ Application Programming Interface (API) that can be used by applets developers to take advantage of the various on-board cryptographic services. The Cyberflex Access 64k v2 cryptographic module is a "post-issuance programmable" cryptographic module. It includes an on-module virtual machine interpreter that allows programs (applets) written in Java to be loaded onto the cryptographic module and placed into execution. The module is considered operating in FIPS mode if (1) only FIPS validated applets are loaded and instantiated, (2) the applets are instantiated according to the security policy described in this document. Under these conditions, the module always operates in FIPS approved mode. The module checks all validated applets and will not load any applets that do not have the correct MAC. The OP specification defines a life cycle for OP compliant cryptographic modules. State transitions between states of the life cycle involve well-defined sequences of operations. Once applets loaded and the cryptographic module is initialized, external applications communicate with Cyberflex Access 64k v2 cryptographic module through a secure channel that is put into place as part of the cryptographic module's initialization process when it is inserted into a card reader. The secure channel is established by the Cryptographic Officer with the Card Manager application on the cryptographic module. Through the Card Manager, a secure communication pathway can be established with any of the applets on the cryptographic module. Each applet can provide additional "command services" which can be accessed by external applications.

2.2 ACTIVCARD DIGITAL IDENTITY APPLET SUITE V1.1.5

The ActivCard Digital Identity Applet Suite v1.1.5 consists of the following:

- ID applet package
- PKI applet package
- GC applet package
- SKI applet package

The ID applet offers Card Holder Verification (CHV) services to external application.
The PKI Applet offers PKI cryptographic services to external application.
The GC Applet offers secure storage services to external application.
The SKI Applet offers DES or TDES based one-time password service.

There may be as many instances of each applet as there are available cryptographic module resources. There are dependencies between applet instances PKI ➔ GC ➔ ID, and SKI ➔ ID. This means that a PKI instance requires a GC instance and an ID instance to operate. On the other hand, an ID instance can be present alone on the cryptographic module.
Those applets are included within the cryptographic boundary of the module, and enable cryptographic services. They are therefore subject to validation.
The document further refers to any of these three applets by 'the applet'(s).

3. SECURITY LEVEL

The ActivCard Digital Identity Applet Suite v1.1.5 on Cyberflex Access 64k v2 is designed and implemented to meet the Level 2 requirements of FIPS140-2. The cryptographic module enforces FIPS mode of operation at any time. 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	3
Self Tests	2
Design Assurance	2
Mitigation of other attacks	2

4. CRYPTOGRAPHIC MODULE SPECIFICATION

The ActivCard Digital Identity Applet Suite v1.1.5 on Cyberflex Access 64k v2 support role based authentication of card holder, application operators and cryptographic officers using PIN or TDES keys. All services provided by the cryptographic module are protected by role based access control policy following the result of the authentication.

This validation effort will be aimed at the Systems software, virtual machine, Card Manager application, and ActivCard applets. If additional applets are loaded to this cryptographic module, then these additional applets will need to go through a separate validation and will need to be FIPS 140-2 validated. The module checks all validated applets and will not load any applets that do not have the correct MAC.

The Cyberflex Access 64K V2 cryptographic module supports a command set aimed at allowing the mutual authentication of identities using strong cryptography with "card acceptance devices" in ISO mode (and PCs or other terminals that they might be connected to). Specifically, the TDES algorithm is used within authentication commands between the cryptographic module and the "card acceptance device" environment to authenticate identities. Establishment of identities using these commands is then used to fulfill "access conditions" which limit the ability of the external world to access information and/or commands on the Cyberflex Access 64K V2 cryptographic module.

The Cyberflex Access 64K V2 cryptographic module adheres to the various ISO/IEC specifications for Integrated Circuit Chip (ICC) based identification cards. The "cryptographic boundary" for the Cyberflex Access 64K V2 cryptographic module 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.

Cyberflex Access 64K V2 cryptographic module is a single chip implementation of a cryptographic module. The product is designated M512LACC2. The Cyberflex Access 64K V2 cryptographic module chip is comprised of the following elements:

- Philips P16WX064, 16 bit micro controller,
- System software is installed in Read Only Memory (ROM) as part of the chip manufacturing process (known as Hard mask) and in Electrically Erasable, Programmable Read Only Memory (EEPROM) for system options and additional customized software (known as soft mask). The software is then designated: Hard Mask n°01 Version 01 (ie. 1v1); Soft Mask n°02 Version 03 (ie. 2v3). Note that in the smart card world, Hard Mask refers to software stored in ROM; in other guises, this might be referred to as "firmware". These hard mask and soft mask identification numbers are returned in the response to the MaskTrack command (01 01 02 03).
- Critical Security Parameters stored in EEPROM as part of the Cyberflex Access 64K V2 cryptographic module personalization operation.

The ActivCard Digital Identity Applet Suite v1.1.5 are composed of the following elements:

- ID applet package version 1.0.0.23
- PKI applet package version 1.0.0.29
- GC applet package version 1.0.0.27
- SKI applet package version 1.0.0.16

The applet package byte code is loaded in the cryptographic module memory.

The applets offer services to external applications, and rely on key management, secure memory management and cryptographic services provided by the cryptographic module.
The services are activated with “APDU commands” sent to the cryptographic module.

Applets depend on a unique security domain for the security configuration. This SD can either be the Card Manager or a separate domain.
The Card Manager is itself a Security Domain with additional services to load, install applets and to control the global cryptographic module status.

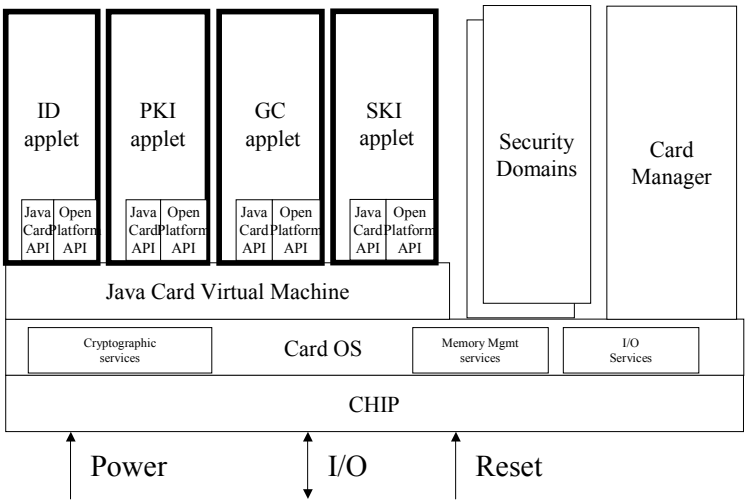

Figure 1: Functional block diagram

Every security domain holds one or more security domain Key Sets composed of TDES keys.
The ownership of a key set allows for establishing a secure channel (SC) between the host and either the security domain or the security domain applets. The SC is generally used for administrative operations such as entering the application keys in the applets instances belonging to the security domain, or entering new key sets in the security domain itself. Note that a security domain key set can be used to enter a replacement key set in the same security domain – the replacement involves the deletion of the original key set. This is how an Applet Security Controller role (ASC), which solely owns the replacement key set, can take control of the personalization of all applet instances belonging to a security domain.

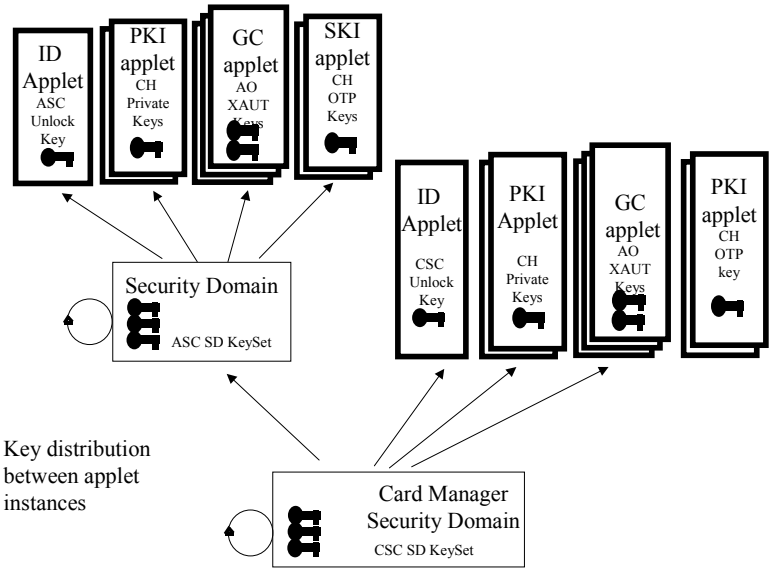

Figure 2: Key Distribution – Role separation

Also note that the Card Security Controller (CSC) role, which owns keys sets of the Card Manager, is also an Applet Security Controller role for all applet instances depending on the Card Manager security domain

4.1 MODULE INTERFACES

The electrical and physical interface of the ActivCard Digital Identity Applet Suite v1.1.5 on Cyberflex Access 64k v2, as a cryptographic module, is comprised of the 8-electrical contacts from the face of the cryptographic module to the chip. These contacts conform to the following specifications.

4.1.1 Physical Interface description

The ActivCard Digital Identity Applet Suite v1.1.5 on Cyberflex Access 64k v2 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 standard. Minimum contact surface area is 1.7mm * 2.0 mm.
Contact dimensions are standard credit card compliant as per ISO/IEC 7816-1 standard:

Dimension	Value
Length	85.5mm
Width	54.0mm
Thickness	0.80mm

4.1.2 Electrical specifications

4.1.2.1 Specific electrical functions of the contacts:

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

4.1.2.2 ICC supply current:

Maximum value: 10 mA at 5MHz (3mA type), short time peak value according to ISO 7816-3.

The communication between the card reader and the ActivCard Digital Identity Applet Suite v1.1.5 on Cyberflex Access 64k v2 is based on a standardized, half-duplex character transmission, ISO 7816 protocol.

Both protocols T=0 and T=1 are supported.

4.1.3 Logical Interface Description

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

5. ROLES & SERVICES

5.1 DEFINITION OF ROLES AND SERVICES

5.1.1 Roles

The ActivCard Digital Identity Applet Suite v1.1.5 on Cyberflex Access 64k v2 defines four distinct roles that are supported by the on-module cryptographic system: Card Security Controller (CSC) role, Applet Security Controller (ASC) role, Application Operator role, and Card Holder role.

5.1.1.1 User Roles:

- **Card Holder Role** - The Card Holder role is responsible for insuring the ownership of his cryptographic module and for not communicating his PIN. An applet authenticates the Card Holder by verifying his PIN.
- **Application Operator Role** – The Application Operator role represents an external application requesting the services offered by the applets. An applet authenticates the Application Operator role by verifying the possession of a TDES key.

5.1.1.2 Cryptographic Officers roles:

- **Card Security Controller (CSC) Role:** This role is responsible for managing the security configuration of the card manager and security domains. The CSC role authenticates to the cryptographic module by demonstrating to the Card Manager application that he possesses the knowledge of a TDES key set stored within the Card Manager. By successfully executing a series of commands, the CSC role establishes a secure channel to the Card Manager; establishment of this channel includes mutual authentication of roles between the CSC role and the Card Manager. Once established, the Card Manager grants authorization on the cryptographic module to information and services.
- **Applet Security Controller (ASC) Role:** This role is responsible for managing the security configuration of the applets. The ASC role authenticates to the cryptographic module by demonstrating to the Applet Security Domain that he possesses the knowledge of a TDES key set stored within the Security Domain. The ASC role has the privilege to unblock the PIN, after successive wrong PIN values have been tried. This is done by externally authenticating himself by proving the possession of a TDES key, in order to access the PIN unblock service of an ID applet instance. Note that the protection of the PIN unblock service by external authentication is optional, as the PIN unblock service is always accessible with the ID applet Security Domain Key Set.

5.1.2 Role Authentication

The ActivCard Digital Identity Applet Suite v1.1.5 on Cyberflex Access 64k v2 supports role authentication.

5.1.2.1 User Role Authentication

- The card holder role is authenticated with PIN or PIN Always
  - **PIN**: this Card Holder role must send a Verify CHV command to any ActivCard applet to access any applet service protected with PIN. The APDU corresponding to the applet service protected by PIN can access the service before the cryptographic module is removed or a reset order is send to the cryptographic module.
  - **PIN Always**: this Card Holder role must send a Verify CHV command to any ActivCard applet to access any applet service protected with PIN Always. The APDU

corresponding to the applet service must be sent immediately after the PIN has been verified.

- The Application Operator role is authenticated by the possession of a TDES key.
  - **Application External Authentication (XAUT) key**: The Application Operator role 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: A 8-byte challenge is first obtained from the applet. The Application controlled by the operator encrypts the challenge with a 112-bit TDES key, and submits the resulting cryptogram for verification. The APDU corresponding to the particular applet service must be sent before the cryptographic module is removed or a reset order is send to the cryptographic module.

5.1.2.2 Cryptographic Officer Role Authentication

- The Cryptographic Officer role is authenticated by a TDES key or a TDES key set.
  - **Secure Channel key set:** The Cryptographic Officer (CSC or ASC) role must prove the possession of a key set composed of 3 TDES keys. Two keys (K_{MAC}, K_{ENC}) are used to derive session keys according to Global Platform specification described in [VOPS]. The session keys ensure the confidentiality of the command payload, allow the mutual authentication of the parties and protect the APDU command integrity. A third key (K_{KEK}) is used to encrypt keys transported within the APDU command.
  - **Unblock PIN External Authentication (XAUT) key**: The Cryptographic Officer (ASC) role 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 (K_{XAUT}). The host application controlled by the Cryptographic Officer role encrypts an 8 byte Card challenge with K_{XAUT}, and submits a PIN Unblock APDU including the resulting cryptogram for verification to the cryptographic module.

5.1.3 Services

5.1.3.1 Crypto Officer Role Administrative Services

5.1.3.1.1 Card platform administrative services available to the CSC role

The following card platform services are used for the administration of the security domains, and to load applets onto the cryptographic module. This command set includes the following commands:

- **INSTALL:** this APDU is used to instruct a security domain, or the Card Manager as to which installation/instantiation step it shall perform during an applet installation process.
- **LOAD:** this APDU is used to load the byte-codes of the Load File (package) defined in the previously issued INSTALL command.
- **DELETE:** this APDU is used by the CSC role to delete a Load File (package) or an applet (applet instance).
- **PUT KEY:** this APDU is used to add or replace security domain key sets.
- **SET STATUS:** this APDU is used to modify the life cycle state of the cryptographic module or the life cycle state of an application.
- **INITIALIZE UPDATE:** this APDU is used to initiate an OP Secure Channel with the Card Manager or a security domain. Cryptographic module and host session data are exchanged, and the cryptographic module and host upon completion of this APDU derive session keys. However, the Secure Channel is considered open upon completion of a successful EXTERNAL AUTHENTICATE command that must immediately follow the INITIALIZE UPDATE command.
- **EXTERNAL AUTHENTICATE:** this APDU is used by the cryptographic module 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.
- **PUT DATA:** this APDU is used to store or replace one tagged data object provided in the command data field.

During the secured channel opening, the command access condition is specified ('CLEAR', 'MAC', 'MAC+ENC') and an access control decision is performed on the received command.

5.1.3.1.2 Applet administrative services available to the ASC role

The following applet administrative services are used for configuring applet specific properties and keys.

Common Administrative Services

The following services are provided by all instances of ID, GC and PKI applets.
- **INITIALIZE UPDATE:** This APDU corresponds to the OP secure channel specification. It is used to mutually authenticate with the Cryptographic Officer and derive the session keys.
- **EXTERNAL AUTHENTICATE:** This APDU corresponds to the OP secure channel specification. It is used to mutually authenticate with the Cryptographic Officer and derive the session keys for the secure channel.
- **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, and PERSONALIZED.
- **SET APPLICATION UID:** This APDU is sent when the UID associated with the applet instance needs to be changed.
- **CHANGE SECURITY PROPERTY:** Change Applet ACRs

ID Applet Administrative Services

The ID applet provides Card Holder Verification (CHV) services. Here are the different APDUs / Services that are provided by an ID applet instance:
- **UNBLOCK:** All PIN-protected services of all applet instances that are attached to a particular ID instance are not accessible to the Card Holder when successive PIN verifications for that ID instance fail. These applets are then in "PIN blocked" state.
    - The Change PIN APDU is used to set a new PIN value and recover Card Holder access when used within a secure channel of the Cryptographic Officer.
    - The Get Challenge / AC External Authenticate may also be used to recover Card Holder access from the Cryptographic Officer when the PIN is blocked.
- **PUT KEY:** This APDU is used to enter the XAUT key used to unblock the PIN, and must be used with a secure channel. The APDU format is compliant with OP specification.
- **AC EXTERNAL AUTHENTICATE:** This APDU is used in combination with a Get Challenge; this APDU is used to unblock the PIN by presenting a cryptogram produced by TDES encryption of the challenge with the XAUT key (see put key). It also provides the ID applet instance with the new PIN value.
- **UPDATE PROPERTIES:** Update install parameters of ID applet
- **RESET PIN:** Clear PIN and PIN unblock key

PKI Applet Administrative 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:
- **GENERATE KEY PAIR**. This APDU is used to generate a RSA Key Pair in the cryptographic module. The Private Key is associated to a PKI applet instance.

- **PUT KEY**. This APDU is used to import/unwrap the private key (Chinese Remainder Theorem) components. The APDU format follows OP specification. There is a unique private key for each PKI applet instance.

GC Applet Administrative Services

The Generic Container Applet provides secure storage services. Each GC applet instance corresponds to one storage area consisting of two buffers: one buffer contains the TAGs and Lengths of stored data elements, and the other buffer contains the values of each data element.
Here are the different APDUs / Services that are provided by a GC applet instance:

- **PUT KEY**. This APDU imports/unwraps the TDES XAUT keys. The APDU format follows OP specification. There are three XAUT keys for each GC Applet instances. Read Tag+Length Buffer key, Read Value Buffer key, and Update any buffer key.

SKI Applet Administrative Services

The SKI applet provide DES and TDES based One-Time Password (OTP) generation. The DES based OTP generation is only used for legacy applications. The OTP generation algorithm is described in the SKI applet specification. The following are the APDU / Services that are provided by a SKI applet instance:

- **PUT KEY**. This APDU imports/unwraps a DES or TDES SKI key used for One-Time Password generation. The APDU format follows OP specification.

5.1.3.2 Usage services

5.1.3.2.1 Usage services available to No role (unauthenticated)

Commands that are available for both the Crypto Officer & the User are the following commands:

- **SELECT**: this command is used for selecting an application (Card Manager, Security Domain or Applet). The Card Manager may be selected either for the loading of a Load File or for installing a previously loaded application (or Security Domain).
- **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.
- **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.
- **GET CHALLENGE:** This APDU is used in combination with AC external Authenticate to perform an external authentication of the Application Operator in order to unblock the PIN.
- **INITIALIZE UPDATE**: this command is used to initiate a Secure Channel with the Card Manager or a Security Domain. Cryptographic module and host session data are exchanged, and the cryptographic module upon completion of this command derives session keys. However, the Secure Channel is considered open upon completion of a successful EXTERNAL AUTHENTICATE command that must immediately follow the INITIALIZE UPDATE command.
- **CHANGE PIN AFTER FIRST USE:** This APDU indicates that the Card Holder must change his PIN before any PIN protected service can be accessed.
- **GET PROPERTIES:** This APDU is used to obtain information about applet instance configuration.

- **GET CERTIFICATE:** This APDU is used to obtain the certificate corresponding to the PKI applet instance private key. The certificate is located in the GC instance that is attached to the PKI applet instance.

5.1.3.2.2 Applet usage services available to Application Operator role

The following services are available to the Application Operator role

- **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 read or update buffer – protected by XAUT.
- **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.

5.1.3.2.3 Applet usage services available to Card Holder role

ID Applet Usage Services

The ID applet provides Card Holder Verification (CHV) services. All ID applet usage services are described in the Common Usage Services section above.

- **VERIFY CHV:** This APDU checks the PIN presented by the Card Holder against the current PIN associated with the ID applet instance.
- **CHANGE PIN:** If the applets are not blocked, the Change PIN APDU is used to set a new PIN value if the current PIN can be presented by the card holder.

PKI Applet Usage 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:

- **PRIVATE SIGN/DECRYPT:** This APDU uses the RSA private key in the applet instance to sign data.
- **GENERATE KEY:** This APDU is used to generate an RSA key pair.

GC Applet Usage Services

The GC Applet provides secure storage services. Each GC applet instance corresponds to one storage area consisting of two buffers: one buffer contains the TAGs and Lengths of stored data elements, and the other buffer contains the values of each data element.

- **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.

SKI Applet Usage Services

The SKI Applet provides DES or TDES based One-Time Password generation service. The DES based OTP generation is used only for legacy applications. The following are the APDU / Services provided by the SKI applet instance.

- **GET CODE:** This APDU is to obtain the One-Time Password derived from the DES or TDES SKI key.

5.1.3.3 Relationship between Roles & Services: Card Platform

Roles/Services	CSC role (Card Manager Security Domain)	No Role (Unauthenticated)
INSTALL	X	
LOAD	X	
DELETE	X	
EXTERNAL AUTHENTICATE	X	
GET DATA		X
GET STATUS		X
GET RESPONSE		X
INITIALISE UPDATE	X	
PUT DATA	X	
PUT KEY	X	
SELECT		X
SET STATUS	X	

Table 1: Role and possible ACR configuration for Card Manager

5.1.3.4 Relationship between Roles & Services: Applets

5.1.3.4.1 Access Control Rules

Each applet service is associated with a role-based Access Control Rule that also indicates the allowed role for that service, as detailed in the previous section. The Access Control Rule may be configurable or fixed depending on the Applet service. Each applet instance may be configured independently. The applet services are invoked by external APDU commands sent to the cryptographic module. The ACRs are applied on the APDU commands. All services are specified in the respective Applet Specification documents.

5.1.3.4.2 Roles vs. Services: ID Applet

Services with configurable ACR are in italic.

Role / Authentication Method Vs. Services	No Role / None	Cryptographic Officer (CSC/ASC) / SECURE CHANNEL	Application Operator / XAUT	Card Holder / PIN
ID Applet				
INSTALL		X		
CHANGE PIN				X
UNBLOCK		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		
CHANGE SECURITY PROPERTIES		X		
UPDATE PROPERTIES		X		
RESET PIN		X		

Table 2. Roles & possible ACR configuration for ID applet services

5.1.3.4.3 Roles vs. Services: GC Applet

Role / Authentication Method Vs. Services	No Role / None	Cryptographic Officer (CSC/ASC) / 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					
AC EXTERNAL AUTHENTICATE					X	X	X
VERIFY CHV			X	X			
SET STATUS		X					
SET APPLICATION UID		X					
CHANGE SECURITY PROPERTIES		X					

Table 3. Roles & possible ACR configuration for GC applet services

5.1.3.4.4 Roles vs. Services: PKI Applet

Role / Authentication Method Vs. Services	No Role / None	Cryptographic Officer (CSC/ASC) / SECURE CHANNEL	Card Holder / PIN	Card holder / PIN ALWAYS
PKI Applet				
INSTALL		X		
GET PROPERTIES	X			
INITIALIZE UPDATE	X			
EXTERNAL AUTHENTICATE		X		
GENERATE KEY PAIR		X	X	
GET CERTIFICATE	X		X	X
PRIVATE SIGN/DECRYPT		X	X	X
PIN VERIFY			X	X
PUT KEY		X		
SET STATUS		X		
SET APPLICATION UID		X		
CHANGE SECURITY PROPERTIES		X		

Table 4. Roles & possible ACR configuration for PKI applet services

5.1.3.4.5 Roles vs. Services: PKI Applet

Role / Authentication Method Vs. Services	No Role / None	Cryptographic Officer (CSC/ASC) / SECURE CHANNEL	Card Holder / PIN	Card holder / PIN ALWAYS
SKI Applet				
INSTALL		X		
GET PROPERTIES	X			
INITIALIZE UPDATE	X			
EXTERNAL AUTHENTICATE		X		
GET CODE			X	X
PIN VERIFY			X	X
UPDATE PROPERTIES		X	X	X
PUT KEY		X		
SET STATUS		X		
SET APPLICATION UID		X		
CHANGE SECURITY PROPERTIES		X		

Table 4. Roles & possible ACR configuration for SKI applet services

5.1.3.5 Module Cryptographic Functions

The purpose of the ActivCard Digital Identity Applet Suite v1.1.5 on Cyberflex Access 64k v2 is to provide a FIPS approved platform for applets that may in turn provide cryptographic services to end-user applications. The keys represent the roles involved in controlling the cryptographic module. A variety of validated FIPS 140-2 Approved cryptographic algorithms are used in the ActivCard Digital Identity Applet Suite v1.1.5 on Cyberflex Access 64k v2 to provide cryptographic services; these include:

- DES/ECB (use for legacy systems only)

- TDES/ECB/CBC, (2 keys TDES)
- SHA-1,
- RSA PKCS1 (512, 768, 1024, 2048 bit keys)

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 external application to the cryptographic module environment. The reverse direction is not encrypted; i.e. the status words returned in response to an APDU are not encrypted. TDES, RSA and SHA-1 algorithms are provided as services through Java APIs to applets that may be loaded onto the cryptographic module.

5.1.3.6 RNG

The ActivCard Digital Identity Applet Suite v1.1.5 on Cyberflex Access 64k v2 offers the services of a FIPS approved DRNG using ANSI X9.31 standard.

5.1.3.7 Self Tests

5.1.3.7.1 Power Up Self Tests

The ActivCard Digital Identity Applet Suite v1.1.5 on Cyberflex Access 64k v2 performs the required set of self-tests at power-up time. When the ActivCard Digital Identity Applet Suite v1.1.5 on Cyberflex Access 64k v2 is inserted into a smart card reader, once power is applied to the cryptographic module (contact) interface, a “Reset” signal is sent from the reader to the cryptographic module. The cryptographic module then performs a series of GO/NO-GO tests before it responds (as specified by ISO/IEC 7816) with an Answer To Reset (ATR) packet of information. These tests include:

- RAM functional test & clearing at Reset,
- HRNG functional test,
- EEPROM Firmware integrity check,
- Algorithm (known answer) tests for:
  - CRC16,
  - DES (ECB & CBC mode encrypt/decrypt),
  - TDES (ECB & CBC mode encrypt/decrypt),
  - SHA-1 Hashing,
  - RSA PKCS1 sign and verify.

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

5.1.3.7.2 Conditional Tests

RSA Key generation:

A pair wise consistency check is performed during key generation.

Random Number Generator:

HRNG: A 16 bits continuous testing is performed during each use of the Hardware non-deterministic RNG. The HRNG 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 cryptographic module.

5.1.4 Critical Security Parameters

- **Initialization key K_{init}**: used to secure the card during its transportation from the manufacturer site to the issuance site. This is a TDES key and is replaced with the card manager OP key set as the first step of issuance.
- **Card Security Controller (CSC) OP Key Set:**
  - This is the card manager OP secure channel key set consists of the following three keys:

  - K_{enc}: used to derive session keys for the encrypted mode of the secure channel
  - K_{mac}: used to derive session keys for crypto officer authentication and MAC mode of the secure channel. This key is used to authenticate the CSC role to the card
  - K_{kek}: used to encrypt keys to be loaded onto the cryptographic module
- **Applet Security Controller (ASC) OP Key Set:**
  - This is the security domain OP secure channel key set consists of the following three keys:
    - K'_{enc}: used to derive session keys for the encrypted mode of the secure channel
    - K'_{mac}: used to derive session keys for crypto officer authentication and MAC mode of the secure channel. This key is used to authenticate the ASC role to the card
    - K'_{kek}: used to encrypt keys to be loaded onto the cryptographic module
- **Application External Authentication (XAUT) Key**: TDES key that enables the authentication of Application Operators (PKI/GC read or PKI/GC Update)
- **Unblock PIN External Authentication (XAUT) key:** TDES key that enables the ASC role to perform the Reset Retry Counter operation.
- **RSA private keys**: managed (generated, unwrapped) from the PKI/GC applet using the Java Card cryptographic services. These keys are used to sign data.
- **SKI TDES keys**: managed (unwrapped) from the SKI applet using the Java Card cryptographic services. These keys are used to generate One Time Passwords.
- **Personal Identification Numbers (PIN):** PINs and PIN attributes are managed from the ACA Applet, which relies on Java Card PIN management service.
- **Authentication Method (or ACR)**: These data elements define the Authentication Method that is permanently set for the service. Several services offer a configurable Authentication Method. For such services, the authentication method should be set according to the tables in section 5.1.3.

5.2 ACCESS TO CSPS VS SERVICES

The following Matrix shows for each applet how services access CSPs.

5.2.1 ID Applet

ID applet Columns: Services(roles) Rows: Access to CSPs	**Card Holder**	**Application Operator**	**Cryptographic Officer**	INSTALL-instantiate (CSC)	CHANGE PIN/UNBLOCK(ASC)	GET PROPERTIES(any)	INITIALIZE UPDATE(any)	EXTERNAL AUTHENTICATE(ASC)	VERIFY CHV(C.H)	PUT KEY(ASC)	GET CHALLENGE(any)	AC EXTERNAL AUTHENTICATE(ASC)	CHANGE PIN AFTER FIRST USE(any)	UPDATE PROPERTIES (ASC)	CHANGE SECURITY PRPERTIES (ASC)	RESET PIN (ASC)	Set Status (ASC)
Access Control Rules																	
Set ACR			X	X											X		
PIN or Password																	
Set PIN controls			X	X										X			
Set PIN			X	X												X	
Change/Unblock PIN	X	X	X		X												
Verify CHV	X								X								
External Authentication Keys																	
Delete key			X							X							
Enter key			X							X							
Verify cryptogram		X			X							X					
Card Manager Key set																	
Verify Cryptogram			X		X			X		X							
Decrypt APDU payload			X		X					X							
Applet Instance Status																	
Change Status			X													X	X

5.2.2 PKI Applet

PKI applet services Columns: Services (roles) Rows: Access to CSPs	***Card Holder***	***Cryptographic Officer***	INSTALL instantiate (CSC)	GET PROPERTIES (any)	INITIALIZE UPDATE(any)	EXTERNAL AUTHENTICATE(ASC)	GENERATE KEY PAIR (ASCor CH)	GET CERTIFICATE(any)	SIGN(C.H)	Set Status(ASC)	CHANGE SECURITY PROPERTIES(ASC)	PIN VERIFY(C.H)	PUT KEY(ASC)
Access Control Rules													
Set ACR		X	X								X		
PIN or Password													
Verify CHV	X											X	
RSA Key Pair													
Generate Key Pair	X	X					X						
Enter CRT components		X											X
Delete private key		X											X
Sign data	X	X							X				
Card Manager Key set													
Verify Cryptogram		X				X							
Decrypt Data		X				X							X
Applet Instance Status													
Change Status		X								X			

5.2.3 GC Applet

GC applet services Columns: Services (roles) Rows: Access to CSPs	**Card Holder**	**Cryptographic Officer**	**Application Operator**	INSTALL (Instantiate) (CSC)	GET PROPERTIES (any)	INITIALIZE UPDATE (any)	EXTERNAL AUTHENTICATE (ASC)	Set Status	UPDATE BUFFER (ASC or A.O or C.H)	READ BUFFER (ASC or A.O or C.H)	GET CHALLENGE (any)	PUT KEY (ASC)	CHANGE SECURITY PROPERTIES (ASC)	GC EXTERNAL AUTHENT(A.0)	PIN VERIFY (C.H)
Access Control Rules															
Set ACR		X		X									X		
PIN or Password															
Verify CHV	X														X
External Authentication Keys															
Delete key		X										X			
Enter key		X										X			
Verify cryptogram			X											X	
Card Manager Key set															
Verify Cryptogram		X					X					X			
Decrypt Data		X							X	X		X			
Applet Instance Status															
Change Status		X						X							

5.2.4 SKI Applet

GC applet services Columns: Services (roles) Rows: Access to CSPs	**Card Holder**	**Cryptographic Officer**	**Application Operator**	INSTALL (Instantiate) (CSC)	GET PROPERTIES (any)	INITIALIZE UPDATE (any)	EXTERNAL AUTHENTICATE (ASC)	Set Status	GET Code (CH)	PUT KEY (ASC)	CHANGE SECURITY PROPERTIES (ASC)	UPDATE PROPERTY (SC or CH)	PIN VERIFY (C.H)
Access Control Rules													
Set ACR		X		X							X		
PIN or Password													
Verify CHV	X												X
SKI Key													
Delete key		X								X			
Enter key		X								X			
Card Manager Key set													
Verify Cryptogram		X					X			X			
Decrypt Data		X								X			
Applet Instance Status													
Change Status		X						X					

6. SECURITY RULES

6.1.1 Approved mode of Operation

To maintain the module in an approved mode of Operation, the operator must restrict the usage of the module as follows:

- Module service access control rules must be configured per tables 1, 2, 3, and 4 in section 5.1.3.
- follow all security rules below.

6.1.2 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.

- The module shall provide the following distinct operator roles: The Card Holder role, Application Operator role, Applet Security Controller role and Card Security Controller role.
- The applets shall provide role-based authentication: the card holder is authenticated by the card unique identifier, and the application operator and crypto officers are authenticated by the specific key set version and key index associated with their respective role.
- 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 (Initialize Update & External Authenticate commands).
- 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 ID applet instance.
- 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 Update Buffer 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.
- The DES based One-Time Password generation service provided by SKI applet should only be used with legacy applications.

6.1.3 Applet Life Cycle Security Rules

The ActivCard Digital Identity Applet Suite v1.1.5 on Cyberflex Access 64k v2 allows only loading of FIPS approved applets. Applets can only be loaded through a secure channel; i.e. they pass from the external application to the cryptographic module in an encrypted and MACed form.

- 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 / crypto-officer.
- The management of the life cycle of the applets – load, install, delete, personalize keys, shall follow the Open Platform standard.
- Applets management and key management APDU commands (such as download, install, delete, put key) are protected by secure channel MAC (TDES-CBC). They have their origin authenticated and their integrity verified. In particular this protects the applet byte code against tampering when downloaded at post issuance.
- The download of validated applets packages and the installation of applet instances may either occur at pre-issuance, issuance or post-issuance.
- There may be as many instances of each applet as there are available cryptographic module resources.

6.1.4 Access Control Security Rules

- Keys must be loaded through a secure channel. Consequently, keys are always loaded in the encrypted form.
  - 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 <= N <= 255 consecutive unsuccessful PIN code validation attempts, the Card Holder services must be disabled. (eg. The PIN is blocked)
    - The PIN length L verifies the following rules:
      - 6 <= L <= 255 for PIN composed with random numeric (0-9) or
      - 4 <= L <= 255 for PIN composed with random alpha-numeric (0-9, a - z, A – Z) characters
  - If separation of roles between the Card Holder and Cryptographic officer is required for a particular service, such as the RSA Signature service the PIN always ACR must be selected.

6.1.5 Physical Security Rules

The physical security of the ActivCard Digital Identity Applet Suite v1.1.5 on Cyberflex Access 64k v2 is designed to meet FIPS 140-2 level 3 requirements. A hard opaque epoxy is used to encapsulate the module to meet level 3 requirements. From the time of its manufacture, the cryptographic module is in possession of the Cryptographic Officer until it is ultimately issued to the end user.

6.1.6 Key Management Security Policy

6.1.6.1 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.

6.1.6.2 Cryptographic key entry

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 and the K_{kek} Key).

6.1.6.3 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.

6.1.6.4 *Cryptographic key zerorization*

The cryptographic module zerorizess cryptographic keys by reloading another zero-valued key-set for Crypto Officer keys, Security Domains Applets Keys, or Application Operator XAUT key, or closing of secure channel for session keys**.** The card-holder PIN is zerorized by setting it to zero value. The RSA private key is zerorized by loading a zero-valued key. The SKI key is zerorized by loading a zero-valued key.

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

6.1.7 Mitigation of attacks Security Policy

ActivCard Digital Identity Applet Suite v1.1.5 on Cyberflex Access 64k v2 has been designed to mitigate the following attacks:

- Simple Power Analysis,
- Differential Power Analysis.

7. SECURITY POLICY CHECK LIST TABLES

7.1 ROLES & REQUIRED AUTHENTICATION

Role	Type of authentication	Authentication data
Card Security Controller	TDES challenge response authentication	TDES keys (Secure Channel)
Applet Security Controller	TDES challenge response authentication	TDES key (Secure Channel and XAUT)

Application Operator	TDES challenge response authentication	TDES keys (XAUT)
Card Holder	Verify CHV	PIN

7.2 STRENGTH OF AUTHENTICATION MECHANISMS

Authentication Mechanism	Strength of Mechanism
TDES authentication	> 1:1,000,000
PIN	> 1:1,000,000

7.3 SERVICES AUTHORIZED FOR ROLES

Role	Authorized Services
Card Security Controller	The Card Security Controller services are listed in Section 5.1.3.1.1
Applet Security Controller	The Applet Security Controller services are listed in Section 5.1.3.1.2
Application Operator	The Application Operator Services are listed in Section 5.1.3.2.2
Card Holder	The card holder services are listed in Section 5.1.3.2.3
No role (unauthenticated)	The no role services are listed in Section 5.1.3.2.1

7.4 ACCESS RIGHTS WITHIN SERVICES

Service	CSP	Types of Access (eg. Read, Write, Execute)
Crypto Officer (CSC/ASC) Service	TDES Crypto Officer Keys	Execute (encrypt, decrypt), write (put key)
Application Operator Service	TDES Application Operator Keys	Execute (encrypt, decrypt)
Card Holder Service	PIN	Execute (Verify CHV), write (Change PIN),
Card Holder Service	RSA private key	Execute (Sign/Verify)
Crypto Officer or Card Holder Service	RSA private key	Create (Generate Key)
Crypto Officer Service	RSA private key	Write (Put key)

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

[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]	Global Platform - Open Platform Card Specification, v2.0.1' – April 2000
[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

Acronyms	Definitions
ACR	Access Control Rule
AO	Application Operator
AP	Application Provider
APDU	Application Protocol Data Unit
API	Application Programming Interface
ASC	Applet Security Controller
ATR	Answer To Reset
CBC	Cipher Block Chaining
CO	Cryptographic Officer
CH	Card Holder
CSP	Critical Security Parameter
CSC	Card Security Controller
DES	Data Encryption Standard
ECB	Electronic Code Book
EEPROM	Electrically Erasable and Programmable Read Only Memory
GC	Generic Container
JCRE	Java Card ™ Runtime Environment
MAC	Message Authentication Code
PKI	Public Key Infrastructure
OP	Open Platform
PIN	Personal Identification Number
RAM	Random Access Memory
ROM	Read only Memory
SD	Security Domain
SC	Secure Channel
TDES	Triple DES (112-bit length keys)
XAUT	External Authentication