ActivCard

axalto

ActivCard Applet v2 on Cyberflex Access 64k v1

FIPS140-2 Level 2

Cryptographic Module Security Policy

Version 1.7

ActivCard

axalto

Table of Contents

1. INTRODUCTION

This document defines the Security Policy for the "ActivCard Applet v2 on Cyberflex Access 64K v1" cryptographic module, submitted for validation, in accordance with FIPS140-2 Level 2 requirements. Included are 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 V1

Cyberflex Access 64K v1 is a module from Axalto, that loads and runs applets written in the Java programming language. The Cyberflex Access 64K v1 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. The Cyberflex Access 64K v1 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 v1 module combines the advantages of the Java programming language and cryptographic services with those of the module. Security of the Cyberflex Access 64K v1 module is derived from both the software and hardware. Data integrity and security are provided through cryptographic services, Java features, and the Systems software. In addition, the module hardware provides tamper-resistance, and tamper-evidence features that meet FIPS140-2 Level 3 physical security requirements.

The Cyberflex Access 64K v1 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 a post-issuance programmable cryptographic module housed in a smart card. The JC specification defines Java Card ™ Application Programming Interface (API) that can be used by applet developers to take advantage of the various on-board cryptographic services. The Cyberflex Access 64K v1 module is a "post-issuance programmable" module. It includes an on-module virtual machine interpreter that allows programs (applets) written in Java to be loaded onto the module and placed into execution. The module is considered operating in FIPS mode if the following are true; (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 does not load any applets that do not have the correct MAC. The OP specification defines a life cycle for OP compliant modules. State transitions between states of the life cycle involve well-defined sequences of operations. Once applets are loaded and the module is initialized, external applications communicate with the Cyberflex Access 64K v1 module through a secure channel that is put into place as part of the module's initialization process when it is inserted into a card reader. The Cryptographic Officer establishes the secure channel with the Card Manager application on the module. Through the Card Manager, a secure communication pathway can be established with any of the applets on the module. Each applet can provide additional "command services" which can be accessed by external applications.

2.2 ACTIVCARD APPLET V2

ActivCard Applet v2 provides significant enhancements over the ActivCard v1 Applet in service, security, and flexibility. The ActivCard Applet v2 framework is backward compatible with earlier versions of ActivCard Applets and offers a more open, stable, and flexible platform for developers to build and deploy smart card applications. ActivCard Applet v2 also complies with GSC-IS 2.1 standard.

ActivCard Applets are a modular suite of Java applets that run on a Java card. Version 2 of this suite is distinctive from Version 1 in the following ways:

- It decouples on-card application services from security management such as authentication and secure messaging, providing a more flexible, secure, and open platform for applet developers.
- It provides a flexible architecture to allow future authentication and biometric services to be added to the module without modifying existing applications.

The two applets included in the cryptographic module are:

- **Access Control Applet (ACA)** – this applet is responsible for Access Control Rules (ACR) definition, access control rules enforcement and secure-messaging processing for all card services. Three off-card entity authentication methods – OP secure messaging, PIN, and ActivCard External Authentication are included by default in the ACA applet.
- **PKI/Generic Container (PKI/GC) Applet** – The PKI/GC Applet can be used to provide secure storage for both PKI credentials, and other data, required for implementation of card services including single sign-on applications, identity, and benefits information. This applet is responsible for RSA-based cryptographic operations using the RSA private key stored in the PKI buffer. Up to 8 buffers can be configured for each applet instance.

3. SECURITY LEVEL

The ActivCard Applet v2 on Cyberflex Access 64k v1 is designed and implemented to meet the Level 2 requirements of FIPS140-2. The cryptographic module enforces FIPS mode of operation at all times. 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 Applet v2 on Cyberflex Access 64k v1 supports role-based authentication of the Card Holder, Application Operators, and Cryptographic Officers, using PIN or TDES keys. All services provided by the cryptographic module are protected by a role based access control policy following the result of the authentication.

This validation effort is aimed at the systems software, virtual machines, Card Manager applications, and ActivCard applets. If additional applets are loaded into this cryptographic module, then these additional applets require a separate validation, and must be FIPS 140-2 validated. The module checks all validated applets, and does not load any applets that do not have the correct MAC.

Cyberflex Access 64K v1, housed in the smart card, 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 v2 on Cyberflex Access 64k v1 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 v1 is a single chip implementation of a cryptographic module. The Cyberflex Access 64K v1 chip is comprised of the following elements:

- Infineon SLE66CX640P, 8 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).

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

The Cyberflex Access 64K v1 module firmware versions are as follows:

- OS Hard Mask no5 v01
- OS Soft Mask no4 v01
- OS Soft Mask no4 v02

The ActivCard Applet v2 is composed of the following elements:

- ACA applet package v 2.3.0.1, 2.3.0.4, and 2.3.0.5
- PKI/GC applet package v 2.3.0.1, v2.3.1.1, and 2.3.1.2
- ASC library package v 2.3.0.1 and v2.3.0.3

The applet and library package byte code is loaded in the cryptographic module memory. Note that the ASC library package consists of static utility classes only accessed by the applet and can not be accessed directly by off-card entity.

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 (SD) for the security configuration. This SD can either be the Card Manager or a separate security domain. The Card Manager is itself a security domain with additional services, and applets. The Card Manager controls the global cryptographic module status.

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 applet 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.

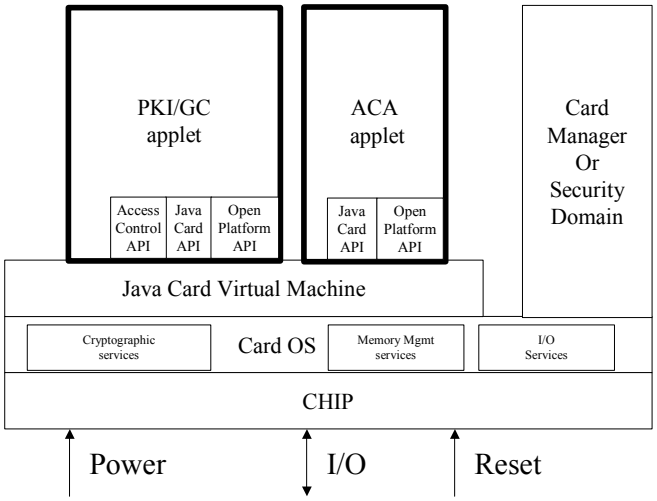

Figure 1: Functional block diagram

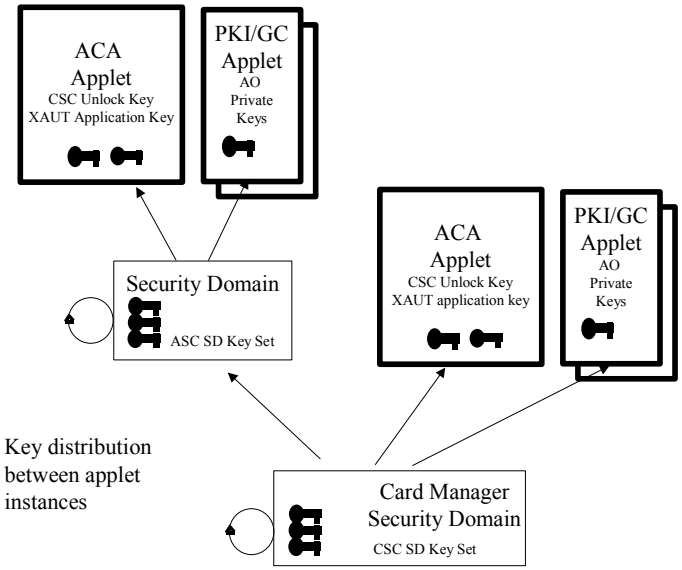

Figure 2: Key Distribution – Role separation

The Card Security Controller (CSC) role, which owns keys sets of the Card Manager, also plays 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 Applet v2 on Cyberflex Access 64K v1, as a cryptographic module, is comprised of 8-electrical contacts from the face of the cryptographic module to the chip. These contacts conform to the specifications listed in the following sub-sections.

4.1.1 Physical Interface description

The ActivCard Applet v2 on Cyberflex Access 64K v1 cryptographic module supports 8 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 Applet v2 on Cyberflex Access 64K v1 cryptographic module is based on a standardized, half-duplex character transmission, ISO 7816 protocol.
Both T=0, and T=1 protocols are supported.

4.1.3 Logical Interface Description

Once electrical (physical) contact, and data link layer contact are 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.
Details of these commands are discussed in the following sections.

4.2 Roles & Services

4.2.1 Roles

The ActivCard Applet v2 on Cyberflex Access 64k v1, 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.

4.2.1.1 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 to other parties. 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 possession of the Application External Authenticate (XAUT) TDES key.

4.2.1.2 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 an OP secure channel TDES key set stored within the Card Manager. By successfully executing the OP secure channel mutual authentication protocol, the CSC role establishes a secure channel to the Card Manager and execute services allowed to the CSC role in a secure manner.
- **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 an OP secure channel TDES key set stored within the security domain. The ASC role also has the privilege of resetting the PIN try counter. This is performed either by authenticating himself using the OP secure channel key set, or an Unblock PIN XAUT TDES key. Note that the protection of the reset PIN retry counter service by XAUT external authentication is optional, as the reset PIN retry counter service is always accessible with the security domain OP key set.

4.2.2 Role Authentication

The ActivCard Applet v2 on Cyberflex Access 64k v1 cryptographic module supports role authentication.

4.2.2.1 User Role Authentication

- The Card Holder role is authenticated with a PIN
  - **PIN**: this Card Holder role must send a Verify CHV APDU to any ActivCard applet or ACA applet to access services protected with PIN access control rules. The APDU corresponding to the applet service protected by the PIN, can access the service before the cryptographic module is removed or a reset order is sent to the cryptographic module.
- 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 PKI/GC buffer read, or update service protected with the External Authentication protocol using this particular key. An 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 to the module for verification. The APDU corresponding to the particular applet service must be sent before the cryptographic module is removed or a reset order is sent to the cryptographic module.

4.2.2.2 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 ACA Applet RESET RETRY COUNTER service protected by 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 RESET RETRY COUNTER APDU that includes the resulting cryptogram for verification to the cryptographic module.

4.2.3 Services

4.2.3.1 Administrative Services

4.2.3.1.1 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 session keys are derived by the cryptographic module and host upon completion of this APDU. 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.

4.2.3.1.2 Applet Administrative Services available to the ASC role

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

ACA Administrative Services

The following services are provided by the ACA 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.
- ***REGISTER APPLET:*** This APDU registers applet instances to the ACA instance so that the access control and secure message service can be provided.
- ***REGISTER ACR:*** This APDU manages the mapping between ACRID and actual APDU instruction.
- ***RESET RETRY COUNTER:*** All PIN-protected services of all applet instances that are registered to the particular ACA instance are not accessible to the Card Holder when successive PIN verifications for that ID instance fail. These applets are then in a “PIN blocked” state.
    - If this APDU is protected in secure channel using Cryptographic Officer OP SC key set, it is used to set a new PIN value and recover card holder access.
    - If this APDU is protected by AC External Authenticate protocol using the Unblock External Authentication (XAUT) key, it also can be used to set a new PIN value and recover Card Holder access.
- ***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 specifications.
- ***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.
- ***AC EXTERNAL AUTHENTICATE***: This APDU is used in combination with a Get Challenge to authenticate the Application Operator using the AC external authenticate protocol.
- ***UPDATE PROPERTIES***. This APDU sets 1) a flag that indicates that the card holder must change his PIN before any PIN protected service can be accessed; 2) return either CAC v1 status word, or GSC-IS v 2.1 status word, when the Card Holder enters the wrong PIN.

PKI/GC Applet Administrative Services

The PKI/GC Applet provides RSA-based cryptographic services. Each PKI/GC applet instance can store up to eight objects, either an RSA key pair / certificate object or T-V buffer object
.
The following services are provided by a PKI/GC applet instance:

- ***GENERATE KEY PAIR:*** This APDU is used to generate an RSA Key Pair in the cryptographic module. The Private Key is associated with 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. A unique private key exists for each RSA key pair object.
- ***SET PROPERTIES:*** This APDU is used to set the object ID of the different PKI/GC objects in the PKI/GC applet instance. Note that the access control rule is enforced at object level rather than the instance level.
- ***READ CERTIFICATE / STATIC BUFFER:*** This APDU is used to read the data from the selected buffer.
- ***UPDATE CERTIFICATE / STATIC BUFFER:*** This APDU is used to update the data stored in the selected buffer.

4.2.3.2 Usage services

4.2.3.2.1 Card Platform and Applet Services Available to No Role (unauthenticated)

- ***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.
- ***PRNG STATISTICAL TEST*****:** this command is used to execute the statistical tests for randomness on the on-card DRNG
- ***GET PROPERTIES***: This APDU is used to obtain information about applet instance configuration.
- ***GET ACR:*** This APDU is used to retrieve the ACR definition for the services.
- ***GET CERTIFICATE***. This APDU is used to obtain the certificate corresponding to RSA private key stored in the corresponding object.
- ***READ CERTIFICATE / STATIC BUFFER:*** This APDU is used to read the data from the selected buffer.

4.2.3.2.2 Applet Usage Services Available to Application Operator

The following services are available to the Application Operator role:

- ***GET CHALLENGE***. This APDU is the first step of the AC External Authenticate protocol and it returns the card random challenge to the host.
- ***AC EXTERNAL AUTHENTICATE***. This APDU is the second step of the AC External Authenticate protocol and it sends the cryptogram to the card for verification of the Application Operator role on the host..
- ***READ CERTIFICATE / STATIC BUFFER:*** This APDU is used to read the data from the selected buffer.
- ***UPDATE CERTIFICATE / STATIC BUFFER:*** This APDU is used to update the data stored in the selected buffer.

4.2.3.2.3 Applet Usage Services Available to Card Holder

Common Usage Services

The following services (APDUs) are common to all instances of applets:

- ***VERIFY CHV***: This APDU checks the PIN presented by the Card Holder against the current PIN associated with the ACA applet instance.

ACA Applet Usage Services

The ACA applet provides Card Holder Verification (CHV) services, access control enforcement, and secure messaging.

- ***CHANGE REFERENCE DATA:*** This APDU is used to change the Card Holder PIN if the Card Holder is correctly authenticated.

PKI/GC Applet Usage Services

The PKI/GC Applet provides RSA-based cryptographic services and secure storage. One RSA private key exists for each PKI buffer. The corresponding certificate is located in this PKI buffer.

The following APDUs / services are provided by a PKI/GC applet instance:

- ***READ CERTIFICATE / STATIC BUFFER:*** This APDU is used to read the data from the selected buffer.
- ***UPDATE CERTIFICATE / STATIC BUFFER:*** This APDU is used to update the data stored in the selected buffer.
- ***PRIVATE SIGN / DECRYPT***. This APDU uses the RSA private key in the PKI buffer to sign data.

4.2.3.3 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
INITIALIZE UPDATE		X
PUT DATA	X	
PUT KEY	X	
SELECT		X
PRNG STATISTICAL TEST		X
SET STATUS	X	

Table 1: Role and possible ACR configuration for Card Manager

4.2.3.4 Relationship Between Roles & Services: Applets

4.2.3.4.1 Access Control Rules

Each applet service is associated with a role-based Access Control Rule (ACR) that also indicates the allowed role for that service, as detailed in the previous section.
The ACR may be configurable or fixed depending on the applet service. The ACA applet is responsible for the configuration, management, and enforcement of the ACRs for each service provided by the applet instances.

The applet services are invoked by external APDU commands sent to the cryptographic module. The ACRs are applied on the APDU commands by the ACA Applet. All services are specified in the respective Applet Specification documents.

4.2.3.4.2 Roles vs. Services: ACA Applet

Services with configurable ACRs are in italic.

Role / Authentication Method Vs. Services	No Role / None	Cryptographic Officer (CSC/ASC) / SECURE CHANNEL	Application Operator or ASC / XAUT	Card Holder / PIN
ACA Applet				
INSTALL		X		
CHANGE REFERENCE DATA				X
GET PROPERTIES	X			
GET ACR	X			
INITIALIZE UPDATE	X			
EXTERNAL AUTHENTICATE		X		
VERIFY CHV	X			
PUT KEY		X		
GET CHALLENGE	X			
AC EXTERNAL AUTHENTICATE			X	
SET STATUS		X		
UPDATE PROPERTIES		X		
RESET RETRY COUNTER		X	X	
REGISTER APPLET		X		
REGISTER ACR		X		

Table 2. Roles & possible ACR configurations for ACA applet services

4.2.3.4.3 Roles vs. Services: PKI/GC Applet

Role / Authentication Method Vs. Services	No Role / None	Cryptographic Officer (CSC/ASC) / SECURE CHANNEL	Card Holder / PIN	Application Operator / XAUT	Application Operator or ASC role XAUT or SECURE CHANNEL
PKI/GC Applet					
INSTALL		X			
GET PROPERTIES	X				
INITIALIZE UPDATE	X				
EXTERNAL AUTHENTICATE		X			
UPDATE CERTIFICATE / STATIC BUFFER		X	X	X	X
READ CERTIFICATE / STATIC BUFFER	X	X	X	X	X
GET CHALLENGE	X				
GENERATE KEY PAIR		X	X		
PRIVATE SIGN / DECRYPT			X		
GET CERTIFICATE	X				
PUT KEY		X			
AC EXTERNAL AUTHENTICATE				X	X
VERIFY CHV	X				
SET STATUS		X			
SET PROPERTIES		X			

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

4.3 MODULE CRYPTOGRAPHIC FUNCTIONS

The purpose of the ActivCard Applet v2 on Cyberflex Access 64k v1 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 algorithms are used in the ActivCard Applet v2 on Cyberflex Access 64k v1 to provide cryptographic services. These include:

- TDES, (2 keys EDE TDES)
- TDES MAC
- SHA-1,
- RSA Sign (PKCS1 512, 768, 1024 bit keys)

The TDES (CBC mode) algorithm is used both for authenticating the Crypto Officer (EXTERNAL AUTH APDU) and 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.

4.3.1 RNG

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

4.3.2 Self Tests

4.3.3 Power-Up Self Tests

The ActivCard Applet v2 on Cyberflex Access 64K v1 cryptographic module performs the required set of self-tests at power-up time. When the ActivCard Applet v2 on Cyberflex Access 64K v1 cryptographic module is inserted into a smart card reader and 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
- RNG functional test
- EEPROM Firmware integrity check
- Algorithm (known answer) tests for:
  - CRC16
  - DES (ECB & CBC mode encrypt/decrypt, not available for use)
  - TDES (ECB & CBC mode encrypt/decrypt)
  - SHA-1 Hashing
  - RSA PKCS1 sign and verify

If any of these tests fail, the cryptographic module respond with an ATR, and a status indication of a self-test error, and the cryptographic module goes 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.

4.3.4 Conditional Tests

RSA Key generation:

A pair-wise consistency check is performed during key generation.

Random Number Generator:

NDRNG: A 16 bit continuous test is performed during each use of the hardware non-deterministic RNG. The NDRNG is used to generate seed values to feed the DRNG.

DRNG: A 16 bit continuous test 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.

4.4 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.
- **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 4.2.3.

4.5 ACCESS TO CSPS VS SERVICES

The following matrix identifies how different services access CSPs for each applet.

4.5.1 ACA Applet

ACA applet Columns: Services(roles) Rows: Access to CSPs	**Card Holder**	**Application Operator**	**Cryptographic Officer**	INSTALL/INSTANTIATE(CSC)	CHANGE REFERENCE DATA	GET PROPERTIES (NO ROLE)	GET ACR (NO ROLE)	INITIALIZE UPDATE (NO ROLE)	EXTERNAL AUTHENTICATE(ASC)	VERIFY CHV (C.H)	PUT KEY (ASC)	GET CHALLENGE (NO ROLE)	AC EXTERNAL AUTHENTICATE (ASC)	SET STATUS (CSC)	UPDATE PROPERTIES (ASC)	RESET RETRY COUNTER (ASC)	REGISTER APPLET (ASC)	REGISTER ACR (ASC)
ACR																		
Install			X	X														
Register ACR			X															X
PIN																		
Reset Retry Counter			X													X		
Change Reference Data	X				X													
Verify CHV	X									X								
XAUT Key																		
Enter/Delete Key			X								X							
Verify Cryptogram		X											X					
OP key set																		
Enter/DKelete Key			X								X							
Verify Cryptogram			X						X		X					X		
Decrypt APDU Payload			X								X					X		
Applet Instance Status																		
Set Status			X											X				
Register Applet			X														X	
Update Property			X												X			

4.5.2 PKI/GC Applet

PKI/GC applet services Columns: Services (roles) Rows: Access to CSPs	***Card Holder***	***Application Operator***	***Cryptographic Officer***	INSTALL/INSTATIATE (CSC)	GET PROPERTIES (any)	INITIALIZE UPDATE(any)	EXTERNAL AUTHENTICATE(ASC)	UPDATE CERT / STATIC BUFFER (A. O)	READ CERT / STATIC BUFFER (A.O)	GET CHALLENGE (No Role)	AC EXTERNAL AUTHENTICATE (A.O)	GENERATE KEY (ASCor CH)	GET CERTIFICATE (any)	PRIVATE SIGN / DECRYPT (C.H)	SET STATUS (ASC)	SET PROPERTIES (ASC)	VERIFY CHV (C.H)	PUT KEY (ASC)
PIN																		
Verify CHV	X																X	
RSA Key Pair																		
Generate Key	X		X									X						
Enter CRT Components			X															X
Delete Private Key			X															X
Sign Data	X													X				
OP key set																		
Verify Cryptogram			X				X											
Decrypt Data			X				X											X
Applet Instance Status																		
Install			X	X														
Set Status			X												X			
Set Properties			X													X		

5. SECURITY RULES

5.1 APPROVED MODE OF OPERATION

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

- module service access control rules must be configured per tables 1, 2, and 3 in section 4.2.3.
- follow all security rules outlined in section 5.2.

5.2 AUTHENTICATION SECURITY RULES

The module implements specific methods for identifying and authenticating the different roles. The implementation consists of binding a role-based ACR 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.
- Applets shall provide role-based authentication:
  - The Card Holder is authenticated by the knowledge of a unique PIN.
  - The Crypto Officer is authenticated via OP secure channel mutual authentication protocol using the card manager/security domain key set that composed of 3 TDES double length keys. Two keys are used to authenticate and MAC the command payload. A third key is used to encrypt keys transported within the APDU command (Initialize Update & External Authenticate commands). For Crypto Officer is also authenticated via AC external authenticate protocol using the Unblock PIN XAUT TDES key.
  - The Application Operator role is authenticated via AC external authenticate protocol using the application XAUT TDES key.
- Cryptographic services are restricted to authenticated roles.
- The role authentication methods (ACRs) for each applet service are set by the Crypto Officer during applet instantiation and can only be modified by the Crypto Officer.
- When authentication of the role cannot be performed because the related key or PIN 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.
- Applet instance configuration may require the combined authentication of different roles to access a particular service. For instance the Application Operator, or the Cryptographic Officer, must both authenticate to access the Update Certificate / Static Buffer service.

5.3 APPLET LIFE CYCLE SECURITY RULES

The ActivCard Applet v2 on Cyberflex Access 64K v1 only permits loading of FIPS approved applets. Applets can only be loaded through an OP 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 Card Acceptance Device are controlled by a valid role; Card Holder, Application Operator or Cryptographic Officer / crypto-officer.
- Management of applet life cycles (load, install, delete, personalize keys), shall follow the Open Platform standard [VOP].
- Applet and key APDU command management (i.e. download, install, delete, put key) are protected by secure channel MAC (TDES-CBC). Their origin is authenticated, and their integrity verified. In particular this protects the applet byte code against tampering when downloaded at post-issuance.
- The download of validated applet packages, and the installation of applet instances, may occur either at pre-issuance, issuance or post-issuance.
- There may be as many instances of each applet as there are cryptographic module resources available.

5.4 ACCESS CONTROL SECURITY RULES

- Keys must be loaded through an OP 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 ACA 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 alpha-numeric (0-9, a - z, A – Z) characters

5.5 PHYSICAL SECURITY RULES

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

5.6 KEY MANAGEMENT SECURITY POLICY

5.6.1 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.

5.6.2 Cryptographic key entry

Keys shall always be input in encrypted format, using the Put Key command within an OP secure channel. During this process, the keys are double encrypted (using the Session Key and the K_{kek} Key).

5.6.3 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.

5.6.4 Cryptographic key zerorization

The cryptographic module zerorizes cryptographic keys by reloading a zero-valued key set for Crypto Officer OP secure channel key set, or Application Operator XAUT key, or closing of secure channel for session keys. The cardholder PIN is zerorized by setting it to zero value. The RSA private key is zerorized by reloading a zero-valued key.

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

5.7 MITIGATION OF ATTACKS

ActivCard Applet v2 on Cyberflex Access 64K v1 cryptographic module has been designed to mitigate the following attacks:

- Simple Power Analysis
- Differential Power Analysis

6. SECURITY POLICY CHECK LIST TABLES

6.1 ROLES & REQUIRED AUTHENTICATION

Role	Type of authentication	Authentication data
Card Security Controller	OP secure channel mutual authentication protocol	OP secure channel TDES key set of three
Applet Security Controller	OP secure channel mutual authentication protocol or TDES	OP secure channel TDES key set of three or Unblock PIN XAUT TDES key
Application Operator	AC External Authenticate protocol	Application XAUT TDES key
Card Holder	Verify CHV service	PIN

6.2 Strength of authentication Mechanisms

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

6.3 Services authorized for Roles

Role	Authorized Services
Card Security Controller	The Card Security Controller role services are listed in Section 4.2.3.1.1
Applet Security Controller	The Applet Security Controller role services are listed in Section 4.2.3.1.2
Application Operator	The Application Operator role services are listed in Section 4.2.3.2.2
Card Holder	The Card Holder role services are listed in Section 4.2.3.2.3

6.4 Access Rights within Services

Service	CSP	Types of Access (i.e. Read, Write, Execute)
Crypto Officer (CSC/ASC) Service	OP secure channel TDES key set of three or Unblock PIN XAUT TDES key	Execute (encrypt, decrypt), write (put key)
Application Operator Service	Application XAUT TDES key	Execute (encrypt, decrypt)
Card Holder Service	PIN	Execute (Verify CHV), write (Change Reference Data)

6.5 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

7. 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.

8. 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
GSC-IS	Government Smart Card Interoperability Standard
JCRE	Java Card ™ Runtime Environment
PKI	Public Key Infrastructure
MAC	Message Authentication Code
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