# ActivIdentity Digital Identity Applet Suite v2 on Axalto Cyberflex Access 64K V2

# FIPS140-2

# Cryptographic Module Security Policy

# Version 1.9

**ActivIdentity, Inc**
**6623 Dumbarton Circle**
**Fremont, CA 94555**
**(510)-574-0100**

 

## Table of Contents

# 1. INTRODUCTION

This document defines the Security Policy for "ActivIdentity Digital Identity Applet Suite V2 on Axalto Cyberflex Access 64K V2" 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 THE AXALTO CYBERFLEX ACCESS 64K V2

The Cyberflex Access 64K V2 cryptographic module from Axalto contains a microprocessor and EEPROM to provide processing capability and memory for storing instructions and data. The cryptographic module loads and runs applets written in the Java programming language.

The product can be used to store and update account information, personal data, and even monetary value. The cards are ideal for secure Internet access, purchases, portable digital telephones, and for benefit programs and health care applications. Cyberflex Access 64K V2 cryptographic module 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 micro module. Security comes from both software and hardware. Data integrity and security are provided through cryptographic services, Java Card ™ features, and the Systems Software. In addition, the Cyberflex Access 64K V2 cryptographic module hardware provides tamper-resistance and tamper-evidence features, that meet FIPS140-2 Level 3 physical 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 smart cards. 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 a virtual machine interpreter that allows programs (applets) written in Java to be loaded onto the Cyberflex Access 64K V2 cryptographic module and placed into execution. The OP specification defines a life cycle for OP compliant smart cards. State transitions between states of the life cycle involve well-defined sequences of operations. Once applets are loaded and the Cyberflex Access 64K V2 cryptographic module is initialized, external applications communicate with Cyberflex Access 64K V2 cryptographic module through a secure channel that is established as part of the Cyberflex Access 64K V2 cryptographic module's initialization process when it is inserted into a Card Acceptance Device (CAD), or card reader. The Secure channel is established by the Cryptographic Officer with the Open Platform Card Manager application on the Cyberflex Access 64K V2 cryptographic module. Through the Card Manager, a secure communication pathway can be established with any of the applets on the Cyberflex Access 64K V2 cryptographic module. Each applet can provide additional "command services" which can be accessed by external applications.

## 2.2 ACTIVIDENTITY DIGITAL IDENTITY APPLET SUITE V2 ON AXALTO CYBERFLEX ACCESS 64K V2

The ActivIdentity Digital Identity Applet Suite v2 on Axalto Cyberflex Access 64K V2

- Allows the configuration of ActivIdentity Digital Identity Applet Suite v2.3.0c,
- Or the configuration of ActivIdentity Digital Identity Applet Suite v2.6.1 (or v2.6.2), but not both.

The applet suites consist of three applets:

- **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 – GP secure messaging, PIN, and ActivIdentity 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 PKI credentials, and other data that are 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 and Internal Authentication using TDES challenge response.
- **ASC Library package** – this is the library package that implements functions required by other applets. The library functions are not directly accessible via the cryptographic module command interface.

The exact versions of each applet packages are described in section 4. Only one version of the applet suite can be instantiated at a time.

## 3. SECURITY LEVEL

The ActivIdentity Digital Identity Applet Suite v2 on Axalto Cyberflex Access 64K V2 is designed and implemented to meet the overall Level 2 requirements of FIPS140-2. This document describes the module FIPS 140-2 Level 2 security policy. The Card Security Controller (CSC) should obtain the hardmask and softmask version via the Answer-To-Reset (ATR) command and, the applet version via the GET PROPERTIES command. The CSC should set the Access Control Rule (ACR) according to table 2 to put the module into the Approved mode of operation.

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 | 3 |
| 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 ActivIdentity Digital Identity Applet Suite v2 on Axalto Cyberflex Access 64K V2 supports identity-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 an identity 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 ActivIdentity applet suites. If additional applets are loaded into this cryptographic module, then these additional applets require a separate validation, and they must be FIPS 140-2 validated. The

cryptographic 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 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 hard opaque epoxy, 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 Cyberflex Access 64K V2 cryptographic module chip is comprised of the following elements:

- Hardware, an IC referenced A1002057 or A1002631
  The IC referenced A1002057 delivers an answer to the MaskTrack command containing 00 00 or 00 02.
  The IC referenced A1002631 delivers an answer to the MaskTrack command containing 00 0A .
- 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 designated by two version numbers: one for the Hard Mask (HM) and one for the Soft Mask (SM). 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”. When all the software is put in ROM, there is no SM. These hard mask and soft mask identification numbers are returned in the response to the MaskTrack command. Currently, one version is available:
  - HM1v3, no SM, delivering an answer to the MaskTrack command containing 01 03 00 00
- Critical Security Parameters stored in EEPROM as part of the Cyberflex Access 64K V2 cryptographic module personalization operation.

The ActivIdentity Digital Identity Applet Suite v2 on Axalto Cyberflex Access 64K V2 is composed of the following elements:

V2.3.0 (patch C) suite
- ACA applet package version 2.3.0c
- PKI/GC applet package version 2.3.0c
- ASC library package version 2.3.0c

V2.6.1 suite
- ACA applet package version 2.6.1
- PKI/GC applet package version 2.6.1
- ASC library package version 2.6.1

V2.6.2 suite
- ACA applet package version 2.6.2
- PKI/GC applet package version 2.6.2
- ASC library package version 2.6.2

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 the library cannot be accessed directly by off-card entity.

The applets offer services to external applications, relying 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 be either the Card Manager or a separate security domain. The Card Manager is itself a security domain with additional services, and applets.

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. Generally, the SC is 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 a Card Security Controller role (CSC), which solely owns the replacement key set, can take control of the personalization of all applet instances belonging to a security domain.

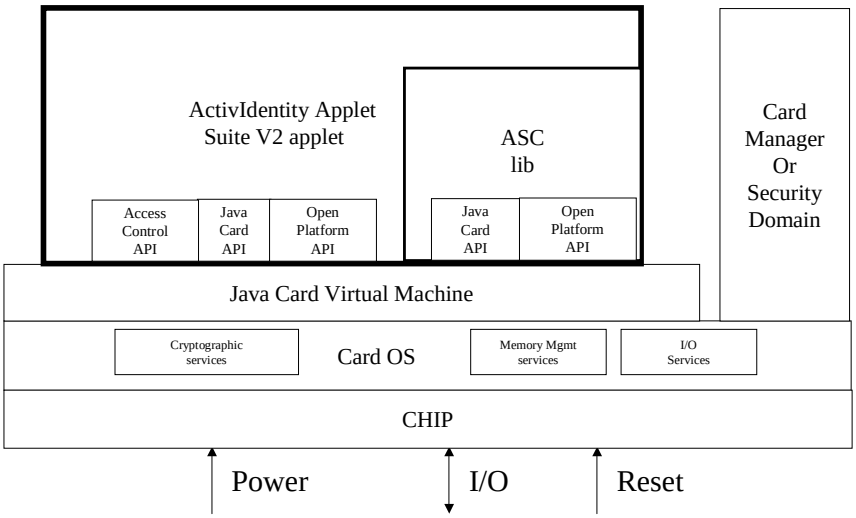


**Figure 3: Functional block diagram**

## 4.1 MODULE INTERFACES

The electrical and physical interface of the Cyberflex Access 64K V2 cryptographic module is comprised of the 5-electrical contacts from the surface of the module to the chip. These contacts conform to the following specifications.

### 4.1.1 Physical Interface description

The Cyberflex Access 64K V2 cryptographic module supports eight contacts that lead to pins on the chip. Only five of these are connected. The location of the contacts complies with [ISO7816-2] 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 +/- 10% |
| 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) |

C4, C6 and C8 are disconnected.

#### *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 reader and the Cyberflex Access 64K V2 cryptographic module is based on a standardized, half-duplex character transmission, ISO 7816 protocol, T=0 or T=1.

### 4.1.3 Logical Interface Description

Once electrical (physical) contact and data link layer contact is established between the module and the reader, the module functions as a “slave” processor to implement and respond to the card reader commands. The Cyberflex Access 64K V2 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. This module also provides an additional set of internal services through the Java Card ™ APIs.

The logical interfaces are connected to the physical interfaces as follows:

| Logical interface | Physical interface |
|---|---|
| Data input | C7 |
| Data output | C7 |
| Status output | C7 |
| Control input | C2, C3, and C7 |
| Power input | C1 and C5 |

# 5. ROLES & SERVICES

## 5.1 IDENTIFICATION

The ActivIdentity Digital Identity Applet Suite v2 on Axalto Cyberflex Access 64K V2 performs identity-based authentication using PIN and cryptographic keys. A unique index value is associated with the PIN or the cryptographic key to uniquely identify the off-card entity performing the authentication.

## 5.2 ROLES

The ActivIdentity Digital Identity Applet Suite v2 on Axalto Cyberflex Access 64K V2 defines three distinct roles that are supported by the on-module cryptographic system; the Card Security Controller (CSC) role, the Application Operator role, and the Card Holder role.

### 5.2.1 User Roles:

- **Card Holder Role (CH)** - The Card Holder role is responsible for ensuring 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 (AO)** – 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.

### 5.2.2 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 GP 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. The CSC role is also responsible for unblocking the PIN using a specific unblock PIN XAUT key with ActivIdentity external authentication protocol.

## 5.3 ROLE AUTHENTICATION

The ActivIdentity Digital Identity Applet Suite v2 on Axalto Cyberflex Access 64K V2 cryptographic module supports identity based role authentication using the following scheme.

### 5.3.1 User Role Authentication

- The Card Holder role is authenticated with a PIN
  - **PIN**: The Card Holder role must send a Verify CHV APDU to the module 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 command 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 protected by the XAUT key, can access the service before the cryptographic module is removed or a reset command is sent to the cryptographic module.

### 5.3.2 Cryptographic Officer Role Authentication

- The Cryptographic Officer role is authenticated by a TDES key set in the case of secure channel key set, or a TDES key in the case of XAUT key.
  - **Secure Channel key set:** The Cryptographic Officer (CSC) role must prove the possession of a key set composed of three TDES keys. Two keys ($K_{MAC}$, $K_{ENC}$) are used to generate session keys according to Global Platform specification. 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 wrap keys transported within the APDU command.
  - **Unblock PIN XAUT key:** The Cryptographic Officer (CSC) role performs the ActivIdentity external authentication protocol using the XAUT TDES key. The PIN is unblocked if the CSC role is successfully authenticated.

## 5.4 SERVICES

This section describes the services each role can perform. When the APDU only applies to v2.3.0c, v2.6.1 or v2.6.2 applet suite, it is explicitly stated within the APDU description. Otherwise, the APDU applies to both applet suites.

### 5.4.1 CSC (Card Manager and Security Domain) Role Services

The following APDUs are sent to card manager:

- ***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).
- ***INITIALIZE UPDATE***: this command is used to initiate a Secure Channel with the Card Manager or a Security Domain. Cyberflex Access 64K V2 cryptographic module and host session data are exchanged, and session keys are generated in the Cyberflex Access 64K V2 cryptographic module upon completion of this command. However, the Secure Channel is not considered open until completion of a successful EXTERNAL AUTHENTICATE command that must immediately follow the INITIALIZE UPDATE command.
- ***EXTERNAL AUTHENTICATE***: this command is used by the Cyberflex Access 64K V2 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 3DES KEY***: this command is used to add or replace Security Domain key sets, except for the RSA DAP public key.
- ***PUT RSA PUBLIC KEY***: this command is used to add a key set containing only the RSA DAP or DM public key.
- ***INSTALL:*** this command is used to instruct the Card Manager (or a Security Domain with Delegated Management privilege) as to which installation step it shall perform during an application installation process.
- ***LOAD:*** this command is used to load the byte-codes of the Load File (package) defined in the previously issued INSTALL command.
- ***DELETE:*** this command is used by the Crypto Officer (or the owner of a Security Domain with Delegated Management privilege) to delete a Load File (package), an Application (applet instance) or a Security Domain.
- ***SET STATUS***: this command is used to modify the life cycle state of the Cyberflex Access 64K V2 cryptographic module or the life cycle state of an application.
- ***GET STATUS***: this command is used to retrieve Card Manager or Applications information according to a given search criteria.
- ***PUT DATA***: this command is used to store or replace one tagged data object provided in the command data field.
- ***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.
- ***MASK TRACK***: This command allows the reading of up to 10 traceability data bytes. This command is used to determine that the module is under FIPS approved mode of operation.
- ***GET SIZE***: This command is provided to retrieve the available EEPROM memory size.
- ***CHANGE ATR***: This command allows modifying the ATR.
- ***READ SERIAL NUMBER***: This command is provided to retrieve the chip Serial Number, which identifies the chip and therefore the cryptographic module as unique.

The following APDUs are sent to ActivIdentity applets:

- ***RESET RETRY COUNTER:*** This APDU is used to unblock the cardholder PIN and restore the VERIFY PIN service with a new counter value if the CSC role is authenticated successfully.

- ***PUT KEY***: This APDU is used to enter various keys: (1) the XAUT key used to authenticate the Application Operator role; (2) the CSC unblock PIN XAUT key; (3); and RSA private key. This command must be used with a secure channel established by CSC role. The APDU format is compliant with GP specifications.
- ***CHANGE REFERENCE DATA(Initial PIN):*** This APDU is used to set the initial cardholder PIN.
- ***REGISTER APPLET:*** This APDU is used to register applet instances to the ACA instance so that the access control and secure message service can be provided.
- ***REGISTER ACR:*** This APDU is used to manage the mapping between ACRID and actual APDU instruction.
- ***SET APPLICATION UID***: This APDU is sent when the UID associated with the applet instance needs to be changed.
- ***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.
- ***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. The public key is output as the response of this command and not stored on the card.
- ***PRIVATE SIGN / DECRYPT***. This APDU uses the RSA private key in the PKI buffer to sign data.
- ***GET CERTIFICATE:*** This APDU is used to obtain the certificate corresponding to RSA private key stored in the corresponding object.
- ***READ BINARY:*** This APDU is used by applet suite v2.6.1 and v2.6.2 to read binary data stored on the card.

### 5.4.2 Application Operator Role

- ***AC EXTERNAL AUTHENTICATE***: This APDU is used in combination with a Get Challenge to authenticate the Application Operator using the AC external authenticate protocol
- ***READ CERTIFICATE / STATIC BUFFER:*** This APDU is used to read the data from the selected buffer.
- ***READ BINARY:*** This APDU is used by applet suite v2.6.1 and v2.6.2 to read the data from selected buffer.
- ***UPDATE CERTIFICATE / STATIC BUFFER:*** This APDU is used to update the data stored in the selected buffer.
- ***GET CERTIFICATE:*** This APDU is used to obtain the certificate corresponding to RSA private key stored in the corresponding object.

### 5.4.3 Card Holder Role

- ***VERIFY PIN***: This APDU checks the PIN presented by the cardholder against the current PIN.
- ***CHANGE REFERENCE DATA:*** This APDU is used to change the cardholder PIN if the Card Holder is correctly authenticated.
- ***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. The public key is output as the response of this command and not stored on the card.
- ***PRIVATE SIGN / DECRYPT***. This APDU uses the RSA private key in the PKI buffer to sign data.
- ***READ CERTIFICATE / STATIC BUFFER:*** This APDU is used to read the data from the selected buffer.
- ***READ BINARY:*** This APDU is used by applet suite 2.6.1 and v2.6.2 to read the data from selected buffer.

- ***UPDATE CERTIFICATE / STATIC BUFFER:*** This APDU is used to update the data stored in the selected buffer.
- ***GET CERTIFICATE:*** This APDU is used to obtain the certificate corresponding to RSA private key stored in the corresponding object.

### 5.4.4 No Role

- ***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).
- ***INITIALIZE UPDATE***: this command is used to initiate a Secure Channel with the Card Manager or a Security Domain. Cyberflex Access 64K V2 cryptographic module and host session data are exchanged, and session keys are generated in the Cyberflex Access 64K V2 cryptographic module upon completion of this command. However, the Secure Channel is not considered open until completion of a successful EXTERNAL AUTHENTICATE command that must immediately follow the INITIALIZE UPDATE command.
- ***GET DATA***: this command is used to retrieve a single data object, such as the Card Identification data.
- ***MASK TRACK:*** This command allows the reading of up to 10 traceability data bytes. This command is used to determine that the module is under FIPS approved mode of operation.
- ***READ SERIAL NUMBER:*** This command is provided to retrieve the chip Serial Number, which identifies the chip and therefore the cryptographic module as unique.
- ***GET RESPONSE***: this command is restricted to T=0 ISO protocol for an incoming command which has data to send back. That data is received with the GET RESPONSE command sent immediately after the command to which it is related.
- ***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.
- ***READ CERTIFICATE / STATIC BUFFER:*** This APDU is used to read the data from the selected buffer.
- ***READ BINARY:*** This APDU is used by applet suite v2.6.1 and v2.6.2 to read binary data stored on the card.
- ***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.
- ***GET CERTIFICATE***: This APDU is used to obtain the certificate corresponding to RSA private key stored in the corresponding object.
- ***LOGOUT:*** This APDU is used to logout all authenticated roles.

## 5.5 Relationship Between Roles and Services

For the Card Manager services, the access rules are listed in Table 1.

| Roles/Services | CSC Role (Card Manager) | CSC Role (Security Domain) | No Role (Unauthenticated) |
|---|---|---|---|
| SELECT | X | X | X |
| INITIALIZE UPDATE | | | X |
| EXTERNAL AUTHENTICATE | X | X | |
| PUT 3DES KEY | X | X | |
| PUT RSA PUBLIC KEY(1) | X | | |
| INSTALL | X | X(2) | |
| LOAD | X | X(2) | |

| | | | |
|---|---|---|---|
| DELETE | X | X(2) | |
| SET STATUS | X | X | |
| GET STATUS | X | X | |
| PUT DATA | X | X | |
| GET DATA | X | X | X |
| MASK TRACK | X | X | X |
| GET SIZE | X | X | |
| CHANGE ATR | X | X | |
| READ SERIAL NUMBER | X | X | X |

**Table 1: Role and possible ACR configuration for Card Manager**

Note (1) The PUT RSA PUBLIC KEY command is only used to import the RSA Public Key used for DAP or Delegated Management.

Note (2) INSTALL, LOAD and DELETE command are available to security Domains having the Delegated Management privilege.

.

For applets suite v2.3.0c, v2.6.1 and v2.6.2, the access rules are listed in Table 2.

| Role / Authentication Method Vs. Services | No Role / None | Cryptographic Officer (CSC) / SECURE CHANNEL | Application Operator / XAUT | Card Holder / PIN | V2.3.0C | V2.6.1 V2.6.2 |
|---|---|---|---|---|---|---|
| RESET RETRY COUNTER | | X | | | X | X |
| CHANGE REFERENCE DATA (Initial PIN) | | X | | | X | X |
| PUT KEY | | X | | | X | X |
| REGISTER APPLET | | X | | | X | X |
| REGISTER ACR | | X | | | X | X |
| SET APPLICATION UID | | X | | | X | X |
| AC EXTERNAL AUTHENTICATE | | | X | | X | X |
| VERIFY PIN | | | | X | X | X |
| CHANGE REFERENCE DATA | | | | X | X | |
| SELECT | X | | | | X | X |
| GET RESPONSE | X | | | | X | X |
| GET PROPERTIES | X | | | | X | X |
| GET ACR | X | | | | X | X |
| GET CHALLENGE | X | | | | X | X |
| LOGOUT | X | | | | X | X |
| GENERATE KEY PAIR | | X | | X | X | X |
| PRIVATE SIGN / DECRYPT | | X | | X | X | X |
| UPDATE | | X | X | X | X | X |

| | | | | | | |
|---|---|---|---|---|---|---|
| CERTIFICATE / STATIC BUFFER | | | | | | |
| READ CERTIFICATE / STATIC BUFFER | X | X | X | X | X | X |
| GET CERTIFICATE | X | X | X | X | X | X |
| READ BINARY | X | X | X | X | | X |

**Table 2: Role and possible ACR configuration for Applet**

# 6. MODULE CRYPTOGRAPHIC FUNCTIONS

The purpose of the ActivIdentity Digital Identity Applet Suite v2 on Axalto Cyberflex Access 64K V2 is to provide a FIPS approved platform that in turn provides cryptographic services to end-user applications. The keys represent the roles involved in controlling the cryptographic module. A variety of FIPS 140-2 validated algorithms are used in the ActivIdentity Digital Identity Applet Suite v2 on Axalto Cyberflex Access 64K V2 to provide cryptographic services.

## 6.1 CRYPTOGRAPHIC ALGORITHMS, MODE AND KEY LENGTH

- **DES [Cert.#293] – ECB and CBC modes:**
  - Transitional phase only - valid until May 19, 2007
  - DES is used together with TDES as an EDC for the “OP DES DAP” and for the DM Receipt as described in section 9.2.3.
  - DES functions are also provided as services to applets, through Java APIs. They shall be used only for legacy systems.
- **DES MAC [Cert. #293, vendor affirmed]**
  - Transitional phase only – valid until May 19, 2007, for legacy systems
- **TDES, (2 keys TDES) [Cert.#312]:**
  - The TDES (CBC and ECB modes) algorithm is used
    - for authenticating the Crypto Officer (EXTERNAL AUTH command)
    - for encrypting data flow from the off module to the on-module environment. The reverse direction is not encrypted; i.e. the status words returned in response to an APDU are not encrypted.
    - As a TDESMAC to authenticate the originator and to the verification the integrity of the message
  - TDES is also used together with DES as an EDC (cf. DES).
  - TDES functions are also provided as services to applets, through Java APIs.
- **TDES MAC [Cert. #312, vendor affirmed]**
- **AES 128 [Cert.#220] – ECB and CBC modes:**
  - The AES functions are only provided as services through Java APIs to applets.
- **SHA-1 [Cert.#301]:**
  - The SHA-1 function is used in the RSA signature.
  - It is used in the DAP and the DM.
  - It is also provided as a service through Java APIs to applets.
- **RSA PKCS1 (1024, 2048 bit keys) [Cert.#51]:**
  - RSA is used for the “OP RSA DAP” as described in section section 9.2.2.
  - RSA is used for the DM as described in section section 9.2.3

- **DRNG ANSI X9.31 [Cert.#64]:**
  - The DRNG function is used to generate a nonce during the INITIALIZE UPDATE command.
  - It is also provided as a service through Java APIs to applets.

# 7. SELF TESTS

## 7.1 POWER-UP SELF TESTS

The Cyberflex Access 64K V2 cryptographic module performs the required set of self-tests at power-up time. When the Cyberflex Access 64K V2 cryptographic module is inserted into a reader, once power is applied to the module' electrical (contact) interface, a "Reset" signal is sent from the reader to the module. The Cyberflex Access 64K V2 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,
- EEPROM Firmware integrity check with a 39/32 Systematic ECC (7 additional bits for every 32 bits). This ECC check is activated by the reading of the whole firmware.
- Algorithm (known answer) tests for:
  - CRC16,
  - DES (ECB & CBC mode encrypt/decrypt),
  - TDES (ECB & CBC mode encrypt/decrypt),
  - AES (ECB & CBC mode encrypt/decrypt),
  - SHA-1 Hashing,
  - RSA PKCS1 sign and verify.
  - DRNG
  - TDES MAC

If any of these tests fail, the Cyberflex Access 64K V2 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.

## 7.2 CONDITIONAL TESTS

RSA Key generation:

A pair wise consistency check is performed during key generation. It is done in both directions: sign then verify for signature usage; encrypt then decrypt for possible key wrapping usage.

Random Number Generator:

NDRNG: A 16 bits continuous testing 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 64 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 whenever an applet is loaded onto the Cyberflex Access 64K V2 cryptographic module. This MAC is linked to the secure messaging
An optional DAP verification is made. The algorithm used is an RSA signature or an algorithm using DES for the first n-1 blocks and a TDES for the last block.

## 7.3 CRITICAL SECURITY PARAMETERS:

- **TDES Initialization key set $K_{int}$**: used to secure the card during its transportation from the manufacturer site to the issuance site. This key set is generated out side of the cryptographic module and then loaded into the card manager security domain during the card manufacturing and initialization process.
- **TDES CSC Card Manager / Security Domain key set:**
  - $K_{enc}$: used to generate session keys for the encrypted mode of the secure channel
  - $K_{mac}$: used to generate session keys for CSC authentication and MAC mode of the secure channel. This key is used to authenticate the CSC to the card
  - $K_{kek}$: used to wrap keys to be loaded onto the cryptographic module

This key set is generated out side of the cryptographic module in an HSM, and the loaded protected with a Global Platform secure channel using the key set that already exists in the card manager security domain (for example, Kinit)

- **External Authentication Keys (XAUT)**: TDES keys that enable the authentication of either Application Operators (PKI/GC read or PKI/GC Update) or Cryptographic Officers (Reset Retry Counter and Unblock PIN). These keys are generated out side of the cryptographic module in an HSM, and then are loaded protected with a Global Platform secure channel using the CSC Card Manager / Security Domain key set.
- **RSA private keys**: managed (generated or unwrapped) from the PKI/GC applet using the Java Card cryptographic services. These keys are used to generate signatures. They are either generated on the card or outside of the cryptographic module in an HSM, and then loaded protected with a Global Platform secure channel using the CSC Card Manager / Security Domain key set.
- **Personal Identification Numbers (PIN):** PINs and PIN attributes are managed from the ACA Applet, which relies on Java Card PIN management service. The initial PIN is loaded protected with Global Platform secure channel using the CSC Card Manager / Security Domain key set, and can be changed later by the user after a successful user authentication event.
- **Access Control Rule**: 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 table 2. The Access Control Rule are set by the Card Security Controller via a Global Platform secure channel using the CSC Card Manager / Security Domain key set.

# 8. ACCESS TO CSPS VS SERVICES

The following matrix identifies how different services access CSPs defined above.

| CSP | Service | Role | Type of Access |
|---|---|---|---|
| ACR | INSTALL/INSTANTIATE | CSC | Write |
| | REGISTER ACR | CSC | Execute |
| PIN | RESET RETRY COUNTER | CSC | Write |
| | CHANGE REFERENCE DATA | Card Holder | Write |
| | VERIFY CHV | Card Holder | Execute |
| XAUT Key | PUT KEY | CSC | Write |
| | GET CHALLENGE & AC EXT AUTH | AO | Execute |
| CSC GP key set | PUT 3DES KEY | CSC | Write |
| | INIT UPDATE & EXT AUTH | CSC | Execute |
| RSA private key | PUT KEY | CSC | Write |
| | GENERATE KEY | Card Holder/ CSC | Create |
| | PRIVATE SIGN/DECRYPT | Card Holder | Execute |

**Table 3: Access to CSPs and the Services**

# 9. SECURITY RULES

## 9.1 APPROVED MODE OF OPERATION

The cryptographic module enforces FIPS mode of operation at all times. This is asserted when the MASK TRACK command delivers an answer containing:
"01 01 02 01", "01 01 02 03", "01 02 01 01", or "01 03 00 00"

In addition to above, the operator of the cryptographic module

- Sends ATR, GET PROPERTIES to the module to validate that the hardware and software version are the same as those listed in table 2.

- Sends GET ACR to the module to validate that module service Access Control Rules are configured per table 2.
- Ensures that the module follows all security rules outlined in section 10 to maintain in FIPS mode.

## 9.2 APPLET LOADING SECURITY RULES

### 9.2.1 Integrity and Confidentiality of the loading

Only applets validated to FIPS 140-1 or 140-2 shall be loaded onto the Axalto Cyberflex Access 64K V2 cryptographic module.
Applets can only be loaded through a secure channel; i.e. they pass from the off module to the on-module environment in an encrypted and MACed form.
This is a mandatory rule. It guarantees the integrity and the confidentiality of the applet during its loading.
The DAP and Delegated Management features described below are considered optional but complimentary for use by the Cryptographic Officer/User and are consistent with operation of the module in FIPS mode.

### 9.2.2 Applet Loading with "OP DAP"

In this case, the Issuer (Crypto Officer) loads the applet owned by the Applet provider. The Issuer knows that the applet is correct because he loads it inside a secure channel with his own keys, thereby ensuring the applet Origin and Integrity. The Cyberflex Access 64K V2 cryptographic module provides a mechanism designated as "DAP" in OP 2.0.1' to give the same confidence to the Applet provider.

This mechanism uses a DAP, computed off-module by the Applet provider and loaded by the Issuer along with the applet. This DAP is then verified on-module with the Applet Provider 's keys, thereby ensuring that the applet loaded onto the module is the one given by the Applet Provider. The DAP verification is done systematically at the end of the loading, without any additional command.

The Cyberflex Access 64K V2 cryptographic module provides two methods of DAP implementation, "OP DAP DES" and "OP DAP RSA". Only one of them is used when loading an applet.

- The "OP DAP DES" works as an EDC that verifies the integrity of the applet on behalf of the applet provider. It is made of a series of DES computations, ended by a TDES computation.
  All the DES and TDES operations use the TDES DAP secret key. This TDES DAP key is loaded by the User/Applet Provider in his Security Domain, with the PUT KEY command. This TDES DAP key cannot be updated.
- The "OP DAP RSA" is a signature verification, which is a stronger mechanism than the "OP DAP DES". It verifies the integrity of the applet on behalf of the applet provider and it also authenticates the applet provider as the originator of the applet. It is the RSA PKCS#1 Signature of SHA-1 message Digest of the applet.
  The RSA operation uses the applet provider's public key. This RSA DAP key is loaded by the User/Applet Provider in his Security Domain, with the PUT RSA KEY command. This key cannot be updated.

### 9.2.3 Applet Loading with Delegated Management (DM)

In this case, the Applet provider loads his own applet. The Cyberflex Access 64K V2 cryptographic module provides the Delegated Management (DM) feature as defined in [VOPS]. This feature enables the applet provider to load onto the cryptographic module an applet previously validated by the Issuer (Crypto Officer).

The DM uses two cryptographic mechanisms:

- A Token computation and verification
  A Token, also called “OP DAP RSA” is an RSA signature computed off-module by the issuer (Crypto Officer) to allow the loading of this applet. The applet provider sends this Token along with the applet. On-module, the Card Manager verifies the token to check the Origin of the applet, (i.e. that the applet has been authorized by the Issuer) and the integrity of the applet.
  The Token verification operation uses the issuer‘s RSA DM public key. This key is loaded in the Crypto Officer Security Domain with a PUT RSA KEY command. This key cannot be updated.
- A Receipt computation and verification
  A Receipt is sent to the Issuer via the applet provider to confirm that the loading operations were done as expected. This Receipt contains data followed by an EDC. This EDC is made of a series of DES, ended by a TDES. All the DES and TDES operations use the issuer ‘s TDES DM key. This TDES DM key is loaded in the Crypto Officer Security Domain with a PUT KEY command. This key cannot be updated.

### 9.3 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.

- All CSPs are entered into the cryptographic module encrypted except the card holder PIN.
- A PIN ID represents the identity of the Card Holder.
- The key ID of the XAUT key represents the identity of the Application Operator.
- The key ID of the OP secure channel key represents the identity of the CSC.
- The module provides the following distinct operator roles: Card Holder role, Application Operator role, and Card Security Controller role.
- The applets provides role-based authentication:
  - The Card Holder is identified by a PIN ID and authenticated by the knowledge of a PIN
  - The CSC is identified by a key ID and authenticated via a GP secure channel mutual authentication protocol using the card manager/security domain key set that is composed of three TDES double length keys. Two keys are used to authenticate and MAC the command payload. A third key is used to wrap keys transported within the APDU command (Initialize Update and External Authenticate commands).
  - The Application Operator role is identified by a key ID and 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 service are set by the CSC during applet instantiation and can only be modified by the CSC.
- When authentication of the role cannot be performed because the related key or PIN attributes are missing, the corresponding service must not be available.
- 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.

### 9.4 ACCESS CONTROL SECURITY RULES

- Keys must be loaded through a GP 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 parties other 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) and 4<= L <= 255 for PIN composed with alpha-numeric (0-9, a - z, A – Z) characters

## 9.5 KEY MANAGEMENT SECURITY POLICY

### 9.5.1 Cryptographic Key Generation

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

### 9.5.2 Cryptographic Key Entry

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

### 9.5.3 Cryptographic Key Storage

The Keys are structured to contain the following parameters:

- Key set version
- Key index, which is the ID of the key,
- Algo ID, which determines which algorithm to be used,
- Integrity Mechanisms (CRC-16)

### 9.5.4 Cryptographic Key Zerorization

The cryptographic module zerorizes cryptographic keys by reloading either a zero-valued key set for a CSC GP secure channel key set via PUT TDES KEY, or an Application Operator XAUT key with PUT KEY command, or closing of secure channel for secure channel session keys**.** The Card Holder PIN is zerorized by setting it to zero value via the CHANGE REFERENCE DATA command. The RSA private key is zerorized by reloading a zero-valued key using PUT KEY.

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

## 9.6 MITIGATION OF ATTACKS

The Cyberflex Access 64K V2 cryptographic module has been designed to mitigate the following attacks:

- Timing attacks,
- Simple Power Analysis,
- Differential Power Analysis.
- Differential Fault Analysis
- Flash Gun

# 10. SECURITY POLICY CHECK LIST TABLES

## 10.1 ROLES AND REQUIRED AUTHENTICATION

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

### 10.2 STRENGTH OF AUTHENTICATION MECHANISMS

| Authentication Mechanism | Strength of Mechanism |
|---|---|
| TDES authentication | > 1:2 [112] |
| PIN | > 1:1,000,000 for decimal PIN |

### 10.3 SERVICES AUTHORIZED FOR ROLES

| Role | Authorized Services |
|---|---|
| Card Security Controller | The Card Security Controller role services are listed in Section 5.2 |
| Application Operator | The Application Operator role services are listed in Section 5.2 |
| Card Holder | The Card Holder role services are listed in Section 5.2 |

### 10.4 ACCESS RIGHTS WITHIN SERVICES

| Service | CSP | Types of Access (i.e. Read, Write, Execute) |
|---|---|---|
| CSC (CSC) Service | GP 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) |

### 10.5 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 |
| Timing Analysis | Counter Measures against TA | N/A |
| Differential Fault Induction | Counter Measures against FI | N/A |
| Flash Gun | Counter Measures against FG | N/A |

## 11. REFERENCES


- Java Card ™ 2.2 Virtual Machine Specification, June 2002, Sun Microsystems
- Java Card ™ 2.2 Application Programming Interface, revision 1.1, September 2002, Sun Microsystems
- Java Card ™applet developer's guide
- Java Card ™ 2.2 Runtime Environment (JCRE) Specification, June 2002, Sun Microsystems
- Global platform Card Specification, v2.1.1, March 2003, Global Platform
- Global platform Card Specification, v2.1.1, Amendment A, February 2004, Global Platform
- "Integrated circuit(s) cards with contacts – Part 2 Dimension and Location of the contacts." ISO/IEC 7816-2 (1999)

- "Integrated circuit(s) cards with contacts – Part 3 Electronic signal and transmission protocols." ISO/IEC 7816-3, AMD1 (2002)
- "Integrated circuit(s) cards with contacts – Part 4 Inter industry commands for interchange." ISO/IEC 7816-4, AMD1 (1997)
- American Bankers Association, Digital Signatures using Reversible Public Key Cryptography for the Financial Services Industry (rDSA), ANSI X9.31-1998, Washington, D.C., 1998.
- "Security Requirements for Cryptographic Modules", FIPS PUB140-2, May 2001, National Institute of Standards and Technology
- "FIPS 140-2 Annex A: Approved Security Functions", May 2001,National Institute of Standards and Technology
- "FIPS 140-2 Annex C: Approved Random Number Generators", May 2001, National Institute of Standards and Technology
- "FIPS 140-2 Annex D: Approved Key Establishment Techniques", May 2001, National Institute of Standards and Technology
- "FIPS PUB 46-3: Data Encryption Standard", October 25, 1999, National Institute of Standards and Technology
- "FIPS PUB 81: DES Modes of Operation", December 2, 1980, National Institute of Standards and Technology


## 12. ACRONYMS

| Acronyms | Definitions |
|---|---|
| **ACR** | Access Control Rule |
| **AO** | Application Operator |
| **AP** | Application Provider |
| **APDU** | Application Protocol Data Unit |
| **API** | Application Programming Interface |
| **ASC** | ActivIdentity Smart Card |
| **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 |
| **GP** | Global 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 |