ActivIdentity Digital Identity Applet Suite V2 for Extended PIV

FIPS140-2

Cryptographic Module Security Policy

Version 1.5

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 for Extended PIV" 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 OCS ID-ONE COSMO 64 V5

The Oberthur Card Systems ID-One Cosmo 64 v5 Chip Platform is a single chip multiple-application cryptographic JavaCard module with dual interface (contact and contactless) specifically designed for identity and government market needs.

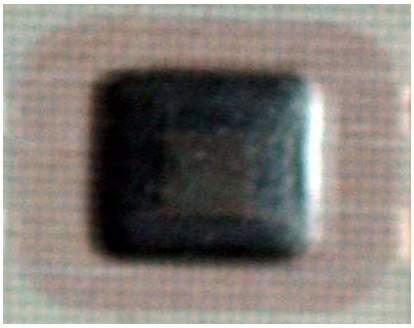
The cryptographic module loads and runs applets written in the Java programming language. It includes a native implementation of the latest Java Card ™ (version 2.2) and Global platform (version 2.1.1A) specifications, with full support for Delegated Management and DAP/mandated DAP (Data Authentication Pattern) that define a secure infrastructure for post-issuance programmable platforms.

DAP consists in a signature of the load data block (application binary file loaded to the card). The binary can be signed and checked by the card before the application is installed. The DAP is a Global Platform features intended for a Controlling Authority to sign the data block before the application is registered in the card.

Additional features include biometric extensions as defined by the JavaCard Forum and Logical Channels.

The Oberthur Card Systems ID-One Cosmo 64 v5 combines the advantages of the Java™ programming language and cryptographic services with those of a dual interface micro module. The same security level is achieved with both contact and contactless interfaces due to carefully designed hardware and software features. In addition, whether embedded into a plastic card or into an electronic passport, the Oberthur Card Systems ID-One Cosmo 64 v5 cryptographic module hardware provides tamper-resistance and tamper evidence features that meet FIPS 140-2 Level 3 Physical Security requirements.

Either the contact or contactless interface can be disabled during manufacturing depending on market specific requirements. The photo, Figure 1, shows an example of the target of validation.



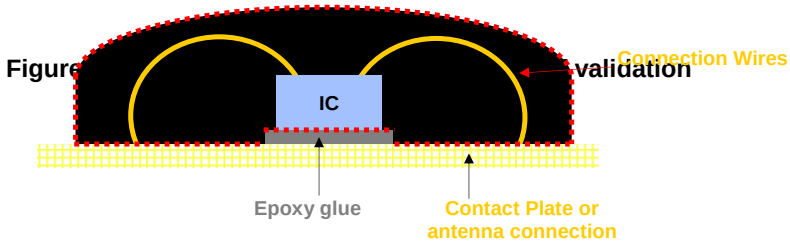


Figure 2: Example of the micro-controller and the golden wires underneath the epoxy resin

The diagram, Figure 2, shows an example the integrated Circuit (micro-controller) and the golden wires underneath the epoxy resin.

The red dotted line shows the module cryptographic boundary. The epoxy glue and the support on which the crypto module is glued (contact plate or antenna) are not part of the crypto module boundary.

The module contains a microprocessor and EEPROM to provide processing capabilities and data storage and offers Java Card™ Technology and Global platform services to applets on the chip.

This document addresses the submission for validation of the module in accordance with FIPS 140-2 Level 2 standard.

Included are a description of the basic 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.

The Chip platform directly provides all the low-level services such as memory management, I/O control, cryptographic algorithms and physical security. It also contains a native implementation of the Java Card ™ specification (JC) version 2.2 and of the Global platform (GP) version 2.1.1A specification, which define a secure infrastructure for post-issuance programmable platforms. These services can be accessed by the applets instantiated from code loaded onto the chip EEPROM or ROM using the Java Card™ Application Programming Interface (API).

The Card Manager provides the Global Platform services that are both internal (accessible by applets) and external services (accessible by either external or non-chip applications).

2.2 ACTIVIDENTITY DIGITAL IDENTITY APPLET SUITE V2 FOR EXTENDED PIV

The ActivIdentity Digital Identity Applet Suite V2 for Extended PIV supports execution of services via contact and contacless interfaces. Only a few services are contactless enabled, while all applet commands can execute with a contact reader.

The v2 applet suite consists of five 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 PUK 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 buffers.
- **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.
- **PIV EP Applet package** – This Applet implements the Personal Identity Verification services from NIST SP800-73-1. It exposes the End Point (EP) APDU commands from this specification. The Applet is a wrapper on top of v2.6.2a applets (ASC Lib, ACA and GC/PKI above). Its purpose is to access PIV Card-Edge and objects although objects are stored in v2.6.2a applet instances. This PIV Applet cannot operate in a standalone mode; it must link with ACA and GC/PKI(s) applet to operate properly.
- **SKI Applet package** – This Applet exposes services for one-time password operations (synchronous mode)

3. SECURITY LEVEL

The ActivIdentity Digital Identity Applet Suite V2 for Extended PIV 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) and GET DATA (with Tag 'DF52') command and, the applet version via the GET PROPERTIES command (or GET DATA from PIV EP Applet). 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 for Extended PIV supports identity-based authentication of the Card Holder, Application Operators, and Cryptographic Officers, using PIN/ PUK 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 application, and ActivIdentity applets. 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 ID-One Cosmo 64 V5 Module submitted for this validation includes the following commercial configurations:

1. ID-One Cosmo 64 D v5.2 FIPS with Optional Code R3 Generic
    - Hardware Platform # "77" with Firmware "E303-063683" and dual (or contact only, contactless only) interface.
    - Hardware Platform # "77" with Firmware "E303-063684" and dual (or contact only, contactless only) interface.

The ActivIdentity Digital Identity Applet Suite V2 for Extended PIV is composed of the following elements:

- **Applet V2.6.2a**:

Configuration 1

- ACA applet package version 2.6.2.A3
- PKI/GC applet package version 2.6.2.A1
- ASC library package version 2.6.2.A1
- PIV End Point package 2.6.2.A1
- SKI applet package 2.6.2.A2

Configuration 2

- ACA applet package version 2.6.2.A3
- PKI/GC applet package version 2.6.2.A1
- ASC library package version 2.6.2.A1
- PIV End Point package 2.6.2.A2
- SKI applet package 2.6.2.A2

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.

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.

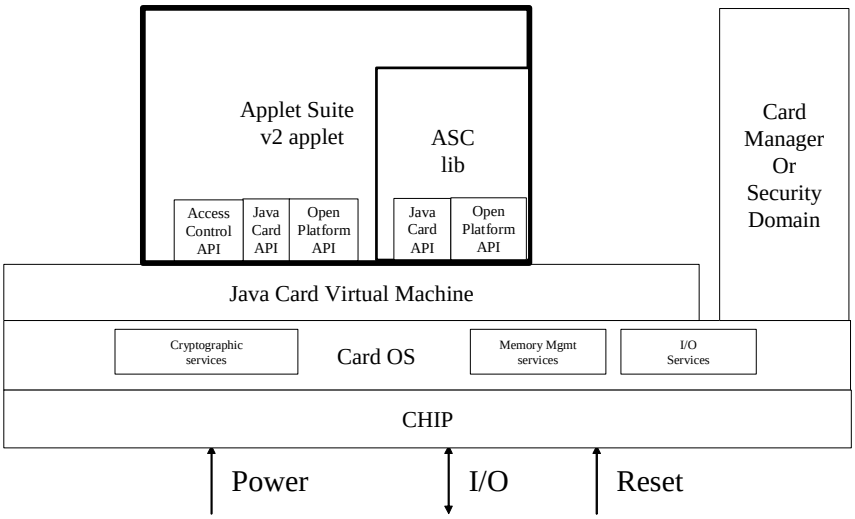


Figure 3: Functional block diagram

4.1 MODULE INTERFACES

The integrated circuit used in the ID-One Cosmo 64 v5 can support the following interfaces:

- ISO/IEC 7816: Identification Cards – Integrated Circuit Cards with Contacts
- ISO/IEC 14443: Identification Cards – Contactless Integrated Circuit Cards – Proximity cards

The ActivIdentity Digital Identity Applet Suite V2 for Extended PIV is validated both on the ISO/IEC 7816 and ISO/IEC 14443 interfaces.

4.1.1 ISO/IEC 7816 Physical Interface (contact mode)

4.1.1.1 Interface Physical Specifications

In this contact mode, communication to and from the cryptographic module is done through a printed circuit (contact plate) that provides the electrical connection required. Five electric wires connect the module to the printed circuit, and from there, to the outside world. The printed circuit itself is outside of the module cryptographic boundaries and is mentioned only for illustration purposes.

The ID-One Cosmo 64 v5 operates in both ISO 7816-3 class A and class B. Class A requires a power supply voltage between 4.5 Volt and 5.5 Volt. Class B requires a power supply voltage between 2.7 Volt and 3.3 Volt. This provides the opportunity for a new range of applications using lower voltage portable readers.

4.1.1.2 Interface Electrical Specifications

The following picture shows an example of the printed circuit and the location where the five electrical connections from the module are wire bonded to the contact plate.

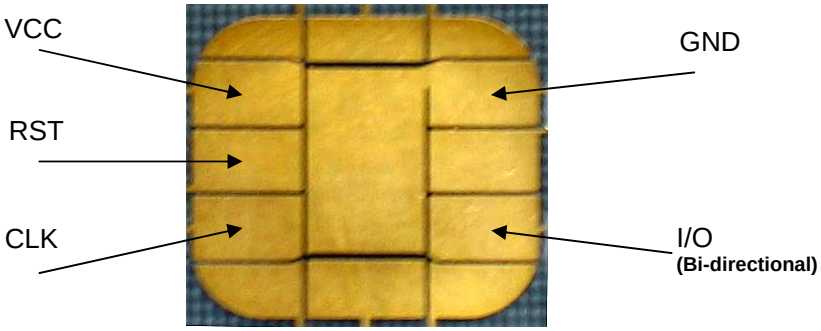


Figure 4: Contact plate used to provide electrical communication with the cryptographic module

The five electrical signals transmitted to the module through the contact mode wires coming from the contact plate are as follows:

- **VCC**: Supply Voltage Power supply input. (1.62V to 5.5V)
- **GND**: Ground (reference voltage)
- **RST**: External reset signal from the interface device (card read / write device)
- **CLK**: External clock (1MHz to 10MHz). This clock is just for data transmission as both processor and coprocessors are driven independently by an internal oscillator at a much higher frequency.
- **I/O**: Input or output for serial data to / from the processor

These five electronic signals are in full compliance with the ISO/IEC 7816-3 standard.

4.1.2 Transmission Protocol and Speed

The transmission protocols with the ID-One Cosmo 64 v5 comply with ISO/IEC 7816-3 (half duplex character oriented transmission protocols ISO T=0 and T=1).

Characters can be exchanged in either direct convention (Z level corresponds to a logical 1 and LSB is sent first) or in inverse convention (Z level corresponds to a logical 0 and LSB is sent first).
The Oberthur ID-One Cosmo 64 v5 supports the Protocol and Parameter Selection to select a new protocol type or change the transmission baud rate.

Up to 256 data bytes can be exchanged within one command.
The maximum communication speed in contact mode is 614,400 bauds (with a clock of 4.9Mhz).

4.2 Logical Interface Description

Once communication is established between the reader and the platform. The platform functions as a “slave” processor to implement and respond to the reader commands. The platform adheres to a well-defined set of state transitions. Within each state, a specific set of commands is accessible. The I/O ports of the platform (either physical in contact mode or virtual in the case of RF transmission) provide the following logical interfaces:

	ISO 7816	ISO 14443
Data In:	I/O Pin	I/O Pins
Data Out:	I/O Pin	I/O Pins
Status Out:	I/O Pin	I/O Pins
Control In:	I/O, Clk and Reset Pins	I/O Pins

4.3 ISO/IEC 14443 RF INTERFACE (CONTACTLESS MODE)

4.3.1 Interface Physical Specifications

In the contactless mode, the cryptographic module uses only two electrical connections, LA and LB, to close the loop of an external antenna, as illustrated in the following picture. The two electrical connections LA and LB, used in contactless mode are physically different from the electrical connections used in contact mode.

The antenna is not within the cryptographic boundaries of the module.

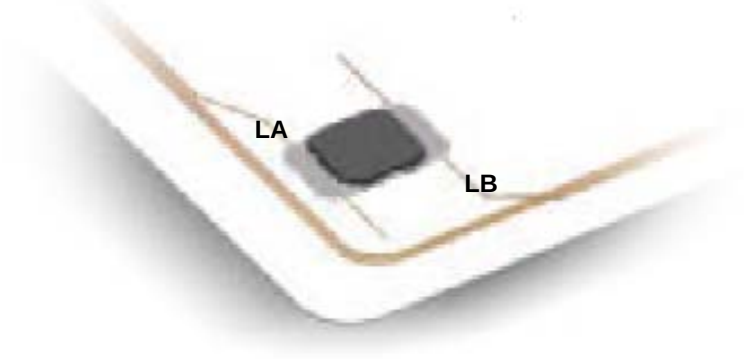


Figure 5: Example of connection of the cryptographic module to the antenna for the contactless mode

4.3.2 Interface Electrical Specifications

Power and data are transmitted to the module from the antenna using a modulation signal at 13.56 MHz.

The proximity coupling device (reader) produces an energizing RF field that couples to the Proximity Mounted Chip Assembly (ID-One Cosmo 64 v5 module) to transfer power.

Data communication is achieved through a modulation of the energizing RF field, using amplitude shift keying (ASK) type of modulation.

The module operates independently of the external clock applied on the interfaces. The main processor and cryptographic co-processors (TDES, RSA) are driven independently of the external clock by an uninterrupted internal oscillator.

During contactless communication, an on-chip capacitor provides all power to the internal oscillator.

A low frequency sensor monitors the external frequency applied to the interfaces. If the frequency is out of the specified range, the chip is reset.

RF signal and power interface are fully compliant with ISO/IEC 14443 part 2: radio frequency power and signal interface for contactless integrated circuit cards – proximity cards.

Initialization and anti-collision that define start of communication and card select are fully compliant with ISO/IED 14443 part 3.

A transmission protocol that defines data exchange between reader and cards are fully compliant with ISO/IEC 14443 part 4.

An anti-collision mechanism compliant with ISO/IEC 14443 is provided by the interface to ensure trouble free communication with the cryptographic module, and to protect from interferences due to the presence of multiple modules or readers within the communication range.

The contactless communication range of the ID-One Cosmo 64 v5 dual interface module is about 10 cm.

More information on this interface can be found in the above-mentioned ISO/IEC standard.

4.3.3 Transmission protocol

Communications with the ID-One Cosmo 64 v5 in contactless mode is based on a fully standardized (ISO/IEC 14443), half-duplex transmission protocol, called T=CL.

5. ROLES & SERVICES

5.1 IDENTIFICATION

The ActivIdentity Digital Identity Applet Suite V2 for Extended PIV 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 for Extended PIV 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 providing the PUK credential to unblock the PIN (SP800-73-1).

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 GP 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.

5.3 ROLE AUTHENTICATION

The ActivIdentity Digital Identity Applet Suite V2 for Extended PIV 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 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 8 bytes-string for PIN Unblocking Key (PUK):
  - **Unblock with PUK:** The AO can also complete the PIN unblock operation with the PUK (which is loaded under the CSC role).

5.3.2 Cryptographic Officer Role Authentication

- The Cryptographic Officer role is authenticated by a TDES key set for secure channel key set
  - **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.

5.4 SERVICES

This section describes the services each role can perform.

5.4.1 CSC (Card Manager and Security Domain) Role Services

The following APDUs are sent to card manager:

- ***INSTALL:*** This APDU is used to instruct either 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).
- ***GET STATUS:*** This APDU is used to get the life cycle state of the cryptographic module or the life cycle state of an application
- ***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.
- ***INITIALIZE UPDATE***: This APDU is used to initiate an GP Secure Channel with the Card Manager or a security domain. Cryptographic module and host session data are exchanged, and the cryptographic module and host upon completion of this APDU generates session keys. However, the Secure Channel is considered open upon completion of a successful EXTERNAL AUTHENTICATE command that must immediately follow the INITIALIZE UPDATE command.
- ***EXTERNAL AUTHENTICATE***: This APDU is used by the cryptographic module to authenticate the host, to establish the Secure Channel, and to determine the level of security required for all subsequent commands within the Secure Channel. A previous and successful execution of the INITIALIZE UPDATE command is required prior to processing this command.
- ***STORE DATA***: This APDU is used to store or replace one tagged data object provided in the command data field.
- ***PUT 3DES KEY:*** This APDU is used to add or replace security domain key sets.
- ***PUT PUBLIC KEY***: This APDU is used to load RSA public keys such as the Token Verification Key or the DAP Verification Key. These keys are used for Delegated Management and DAP verification as specified by Global Platform.

- ***DELEGATE MANAGEMENT***: Delegated Management gives the Card Issuer (CSC) the possibility of empowering partnered Application Provider (Users) the ability to initiate approved and pre-authorized Card Content changes (loading, installation, extradition or deletion).

The following APDUs are sent to ActivIdentity applets:

- ***RESET RETRY COUNTER:*** This APDU is used to unblock the cardholder PIN and restore the VERIFY service with a new counter value if the CSC role is authenticated successfully. The command operates as long as the unblock counter has not expired.
- ***CHANGE REFERENCE DATA:*** This APDU intends to create the PIN and PUK in the card. It is also used to update the PUK value.
- ***PUT KEY***: This APDU is used to either enter the RSA private key component or the SKI key for One Time Password generation. The APDU must be used with a secure channel established by CSC role. The APDU format is compliant with GP specifications.
- ***REGISTER APPLET:*** This APDU is to register 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 as well as record the ACR definition for the applet services.
- ***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:*** This APDU uses the RSA private key in the PKI buffer to sign data.
- ***SET PROPERTIES:*** This APDU creates and sets the object properties for GC/PKI applet.

5.4.2 Application Operator Role

- ***RESET RETRY COUNTER:*** This APDU is used to unblock the PIN with PUK string.

5.4.3 Card Holder Role

- ***VERIFY***: 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:*** 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.
- ***UPDATE CERTIFICATE / STATIC BUFFER:*** This APDU is used to update the data stored in the selected buffer.
- ***GET DATA***: This command is used to retrieve a single data object like PIV object content
- ***GENERAL AUTHENTICATE***: The APDU is for PKI operations (via the PIV EP wrapper)
- ***INTERNAL AUTHENTICATE***: The APDU is for SKI operations and to generate a cryptogram from the card for verification by the calling application.

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)
- ***GET DATA***: This command is used to retrieve a single data object, such as the Card Identification data.
- ***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.
- ***UPDATE PROPERTIES:*** This APDU modifies the applet properties (applet mode and Applet flag for Change PIN after first use). The APDU is accessible from ACA applet.
- ***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.
- ***LOGOUT:*** To logout all authenticated roles.
- ***GENERAL AUTHENTICATE***: The APDU is for PKI operations (via the PIV EP wrapper)
- ***GET VERSION***: The command fetches the applet version for the PIV EP applet wrapper (it has identical format than ***GET DATA*** above)

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)
INSTALL	X		
LOAD	X		
DELETE	X		
GET DATA			X
GET STATUS	X		
SET STATUS	X	X	
INITIALIZE UPDATE	X		
EXTERNAL AUTHENTICATE	X		
STORE DATA	X		
PUT 3DES KEY	X	X	
PUT PUBLIC KEY	X		
SELECT			X
DELEGATE MANAGEMENT	X		

Table 1: Role and possible ACR configuration for Card Manager

The access rules are listed in Table 2.

Role / Authentication Method Vs. Services	No Role / None	Cryptographic Officer (CSC) / SECURE CHANNEL	Application Operator / PUK	Card Holder / PIN	Applet 2.6.2a	
					ISO 7816	ISO 14443
RESET RETRY COUNTER (without PUK)		X			X	
CHANGE REFERENCE DATA (Create PIN/PUK + Update PUK)		X			X	
PUT KEY		X			X	
REGISTER APPLET		X			X	
REGISTER ACR		X			X	
RESET RETRY COUNTER (with PUK)			X		X	
VERIFY				X	X	
CHANGE REFERENCE DATA (change PIN)				X	X	
SELECT	X				X	X
GET RESPONSE	X				X	X
UPDATE PROPERTIES	X				X	
GET PROPERTIES	X				X	X
GET ACR	X				X	
LOGOUT	X				X	
GET VERSION	X				X	X
GENERATE KEY PAIR		X		X	X	
PRIVATE SIGN		X		X	X	X
SET PROPERTIES		X			X	
UPDATE CERTIFICATE / STATIC BUFFER		X		X	X	
READ CERTIFICATE / STATIC BUFFER	X	X		X	X	X
GET DATA	X			X	X	X
GENERAL AUTHENTICATE	X			X	X	X
INTERNAL AUTHENTICATE				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 for Extended PIV 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 v2.6.2a on OCS ID-One Cosmo 64 v5 to provide cryptographic services.

6.1 CRYPTOGRAPHIC ALGORITHMS, MODE AND KEY LENGTH

These include:

- TDES, (2 keys TDES CBC/ECB)
- TDES MAC
- SHA-1
- RSA PKCS1 (1024, 2048 bit keys for all keys)
- RNG (FIPS 186-2 FIPS Approved DRNG)

The TDES (CBC mode) algorithm is used for both authenticating the CSC (EXTERNAL AUTH command) and 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).
Non-FIPS Approved security functions include:

- DES (non-FIPS Approved)
- DES MAC (non-FIPS Approved)
- NDRNG to seed the FIPS Approved DRNG
- RSA encrypt/decrypt (key wrapping; key establishment methodology provides between 80 and 112 bits of encryption strength) – this is allowed for use in FIPS Approved mode for key transport)

6.2 RANDOM NUMBER GENERATOR

The cryptographic module offers the services of a FIPS 140-2 Approved DRNG (Deterministic Random Number Generator). The random number generation algorithm is compliant with the FIPS PUB 186-2 standard. More precisely, the method used is “Constructing the function G from the DES”, taken from the FIPS 186-2 appendix 3, section 3.4.

The cryptographic module also offers the services of a hardware based NDRNG (Non Deterministic Random Number Generator), which can be used to generate a seed to feed the DRNG and increase its quality.

7. SELF TESTS

7.1 POWER-UP SELF TESTS

Each time the ActivIdentity Digital Identity Applet Suite V2 for Extended PIV is powered by a reader (contact or contactless), a “reset” signal is sent from the reader to the module. The module then performs a series of GO/NO-GO tests to validate that the cryptographic module is in good working order before it answers to the reset signal with an Answer To Reset (ATR) packet of information as specified by ISO/IEC 7816 (for contact mode) or with an Answer To Select (ATS) as defined in ISO/IEC 14443 (for contactless mode).

The power-up self tests include:

- EEPROM integrity check using CRC-16 algorithm for:

  - System Data
  - Optional codes (firmware extensions), if any
  - Uploaded application packages (Executable Load Files), if any
- Cryptographic Known Answer Tests for
  - Triple DES – Encryption and decryption in CBC mode
  - SHA-1 Hashing
  - RSA signature generation and signature verification
  - RSA encryption and decryption
  - DES
  - Deterministic Random Number Generator (DRNG) per FIPS 186-2 Appendix 3.
- Critical Function Tests:
  - CRC-16 KAT
  - RAM functional test
  - Sensor bit test
  - Audit log scan
  - Resident applet life cycle

Additional tests to protect against new types of attacks such as SPA, DPA, “flash gun”, etc, are also performed at this stage.
Audit data is read using GET DATA command on the Card Manager.
No data of any type (except error status) is transmitted from the cryptographic module to the reading device while the self-tests are being performed.
If any of the above tests fail, the card enters an error state in which further APDU’s are not processed. Depending on the test that fails, the module may return the ATR/ATS with an error status before becoming mute.

7.2 CONDITIONAL TESTS

- **RSA key generation**: After generating an RSA key pair, the module performs a double pair wise consistency check to validate that the generated key pair is correct for both signature and encryption.
- **Random Number Generator**: Continuous testing is performed on every output of the Random Number Generator. Checks on the non-deterministic (Hardware) component are made on 16 bits and checks on deterministic part (FIPS Approved) are made on 160 bits.
- **Credentials, keys and PINs:** Each time a credential is used, whether a TDES or RSA key or a PIN, a signature of the credential value is computed and compared to the expected signature stored in the EEPROM along with the object itself. If these values are the same, the test is successful and the object can be used safely. If the values are different, the object cannot be used. The problem is recorded into a special “audit file” and a security exception is thrown, causing the execution to abort.
- **Software (applet) load tests:** A TDES CBC MAC on the applet executable load file is verified each time an applet is loaded onto the cryptographic module since applet loading always takes place within a Secure Channel.

7.3 CRITICAL SECURITY PARAMETERS

- **Initialization key set K_{init}**: 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. This key set is zeroized via the PUT KEY (3DES) command.
- **Key for receipts generation during Delegated Management:** It is called Receipt Signature Key and it is 3DES, this key generates the receipt to confirm the execution of the Delegated Management-based operation. This key is not managed by ActivIdentity Applets.
- **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). This key set is zeroized via the PUT KEY (3DES) command.

- **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. Keys 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.
- **PIV private key objects**: Four RSA keys are managed in the Applet Suite. Those keys are defined in the PIV specification (SP800-73-1) and are attached with key Identifiers: 9Ah (PIV Authentication Key), 9Ch (PIV Digital Signature Key), 9Dh (PIV Key Management Key), 9Eh (PIV Card Authentication Key).
- **Card Holder Personal Identification Number (CH PIN)**: It is used to authenticate the Card Holder and it is loaded or modified via the Change Reference Data command. The PIN object is minimum 6 bytes in the card and it contains authentication string that belongs to the Card Holder. CH PIN and associated 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.
- **PIN Unblocking Key (PUK):** The PUK is managed inside the ACA Applet too. It is used to authenticate the AO and the command Change Reference Data initializes the PUK. Its role is to unblock the PIN. The PUK is loaded protected with Global Platform secure channel using the CSC Card Manager / Security Domain key set. The PUK pattern is 8 bytes long in the card and it contains a static byte sequence unique in each card issued.
- **Secret Key for OTP:** TDES key is involved during generation of the One Time Password and then authentication from the card to the calling application.
- **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.

7.4 PUBLIC KEYS

- **RSA public keys in the ActivIdentity Applet:** Public keys are stored under the form of public key certificates and recorded in GC buffers that belong to the GC/PKI applet. There is a certificate slot booked for each RSA private key defined in the card.
- **RSA public keys from the Card Manager/Security Domain (DAP Verification Key)**: This key is a 1024-bits key stored in the Card Manager/Security Domain. This key is not used by the ActivIdentity applet and is under responsibility of the Card Manager/Security Domain application attached to the ActivIdentity applet
- **RSA public key for Delegated Management:** This key is stored in the Card Manager and is 1024 bits long. This key is also called Token Verification Key and is not managed by ActivIdentity applets.

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	CSC	Write
	REGISTER ACR	CSC	Execute
PIN	RESET RETRY COUNTER	CSC	Write
	CHANGE REFERENCE DATA	Card Holder	Write
	VERIFY	Card Holder	Execute
PUK	RESET RETRY COUNTER	AO	Execute
	CHANGE REFERENCE DATA	CSC	Write
SKI Key	PUT KEY	CSC	Write
	INTERNAL AUTHENTICATE	Card Holder	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 PAIR	Card Holder/ CSC	Create
	PRIVATE SIGN	Card Holder	Execute
Initialization Key Set	PUT 3DES KEY	CSC	Write
Receipt Signature Key	PUT 3DES KEY	CSC	Write
PIV Private Key Objects	GENERAL AUTHENTICATE	Card Holder / No Role	Execute

Table 3: Access to CSPs and the Services

9. SECURITY RULES

9.1 APPROVED MODE OF OPERATION

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

- The operator of the cryptographic module sends ATR, GET PROPERTIES, GET VERSION (for PIV EP applet) to the module to validate that the hardware and software version are the same as those listed in table 2.
- The operator of the cryptographic module sends GET ACR to the module to validate that module service Access Control Rules are configured per table 2.
- The module follows all security rules outlined in section 9 to maintain in FIPS mode.

9.2 AUTHENTICATION SECURITY RULES

The module implements specific methods for identifying and authenticating the different roles. The implementation consists of binding a identity-based ACR to each service.

- All CSPs are entered into the cryptographic module encrypted except the card holder PIN (and PUK during unblock with PUK).
- A PIN ID represents the identity of the Card Holder.
- The key ID of the GP 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 provide identity-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 the PUK which is seen as a key with Key ID (=81h, the Key ID value is not used by applet PIV EP).
- 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 Cardholder and Cryptographic Officer, might be both authenticate to access the Update Certificate / Static Buffer service.

9.3 APPLET LIFE CYCLE SECURITY RULES

The ActivIdentity Digital Identity Applet Suite V2 for Extended PIV only permits loading of FIPS Approved applets. Applets can only be loaded through a GP 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 ensure that the terminal and/or Card Acceptance Device are controlled by a valid role; Card Holder, Application Operator or CSC.
- Management of applet life cycles (load, install, delete, personalize keys), follows the Global platform standard.
- Applet and key APDU commands 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.

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 <= 127 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
- The ACA applet stores the unblock counter for the Cardholder PIN. The counter is set with a value between 1 <= M <= 127. The ACA Applet records the PUK pattern which is 8 bytes long.

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 (including PUK) 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 K_{enc} and the K_{kek} Key described in section 7.3).

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

The cryptographic keys storage integrity mechanism is described in a separate confidential document called Self Test Description.

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 or closing of secure channel for session keys**.** The Card Holder PIN is zerorized by setting it to zero value via the CHANGE REFERENCE DATA command (same for the PUK pattern). 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

9.6.1 Power Analysis (SPA/DPA)

Power analysis attacks use information gathered from non-invasive measurements to cryptanalyse and extract keys from tamper resistant devices.

Simple Power Analysis (SPA) attacks use direct observation of a device's power consumption. Because power consumption often varies significantly with computations performed by the crypto module, SPA observations can identify sensitive computational processes, reveal the presence of cryptographic subroutines, and significantly accelerate reverse engineering.

Differential Power Analysis (DPA) attacks use statistical analysis and error correction techniques to extract information leaked across multiple operations. This aggregation of data allows extremely small differences in power consumption to be isolated, including effects that are many orders of magnitude smaller than "noise".

The ID-One Cosmo 64 v5 has been designed to mitigate both Simple Power Analysis (SPA) and Differential Power Analysis (DPA).

The module includes protections against SPA and DPA attacks for all embedded cryptographic algorithms involving secret elements. The chip protection level was evaluated against state-of-the art attacks (at the time of design).

The cryptographic module mitigates Simple Power Analysis (SPA) and Differential Power Analysis (DPA) attacks using a combination of hardware and software design that makes differentiation of key values impractical by equalizing or scrambling current consumption of the card during algorithm cryptographic computation.

Based on the algorithm used, the defense mechanisms vary, as the internal hardware implementations of these algorithms do not use the same underlying hardware.

9.6.2 Timing Analysis

Timing attacks are non-invasive attacks that rely on the variation in computation time required for the microprocessor to perform its secret calculation.

All cryptographic algorithms as well as Java Card API comparison functions offered by the chip are designed to be protected against Timing Analysis.

This is done by enforcing the fact that any sensitive operation is achieved in a constant time regardless of the value of keys or data involved.

9.6.3 Fault Induction

This type of attack is based on the theoretical possibility of flipping some random bits of the secret key, stored in RAM or EEPROM, before or during the computation done by the module. Another fault induction attack is to induce decoding error during the execution of one instruction.

The ID-One Cosmo 64 v5 includes a combination of software and hardware protections in order for the chip not to operate in extreme conditions that may cause processing errors that could lead to revealing the values of cryptographic keys or secret elements. Extreme conditions refer to abnormal temperature, external power supply and external clock supply.

In addition, every keys and PINs are protected by a signature that is checked prior to every use of the keys or PINs.

9.6.4 Flash Gun

The ID-One Cosmo 64 v5 includes a combination of software and hardware protections in order to detect "Flash Gun" type of attacks and abort any current processing before becoming mute.

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	GP secure channel TDES key set of three
Application Operator	PIN unblock	PUK presentation
Card Holder	Verify service	PIN

10.2 STRENGTH OF AUTHENTICATION MECHANISMS

Authentication Mechanism	Strength of Mechanism
TDES authentication	> 1:2 ^{112}
PIN	2^{64}
PUK	2^{64}

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 (K_{enc}, K_{Mac}, K_{Kek}), Create/Update PIN/PUK	Execute (encrypt, decrypt, update PUK), Write (put key, create PIN/PUK)
Application Operator Service	Unblock PIN with PUK	Execute (unblock with PUK)
Card Holder Service	PIN	Execute (Verify), write (Change Reference Data)

10.5 MITIGATION OF OTHER ATTACKS

Other Attacks	Mitigation Mechnism	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
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
- "Special Publication SP800-73-1", April 20, 2006 with May 2 errata, National Institute of Standards and Technology
- "Cryptographic Algorithms and Key Sizes for PIV, SP800-78", April 2005, 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
CH	Card Holder
CO	Cryptographic Officer
CSC	Card Security Controller
CSP	Critical Security Parameter
DES	Data Encryption Standard
ECB	Electronic Code Book
EEPROM	Electrically Erasable and Programmable Read Only Memory
GC	Generic Container
GP	Global Platform
GSC-IS	Government Smart Card Interoperability Standard
JCRE	Java Card ™ Runtime Environment
MAC	Message Authentication Code
OTP	One Time Password
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PUK	PIN Unblocking Key
RAM	Random Access Memory
ROM	Read only Memory
SD	Security Domain
SC	Secure Channel
TDES	Triple DES (112-bit length keys)
XAUT	External Authentication