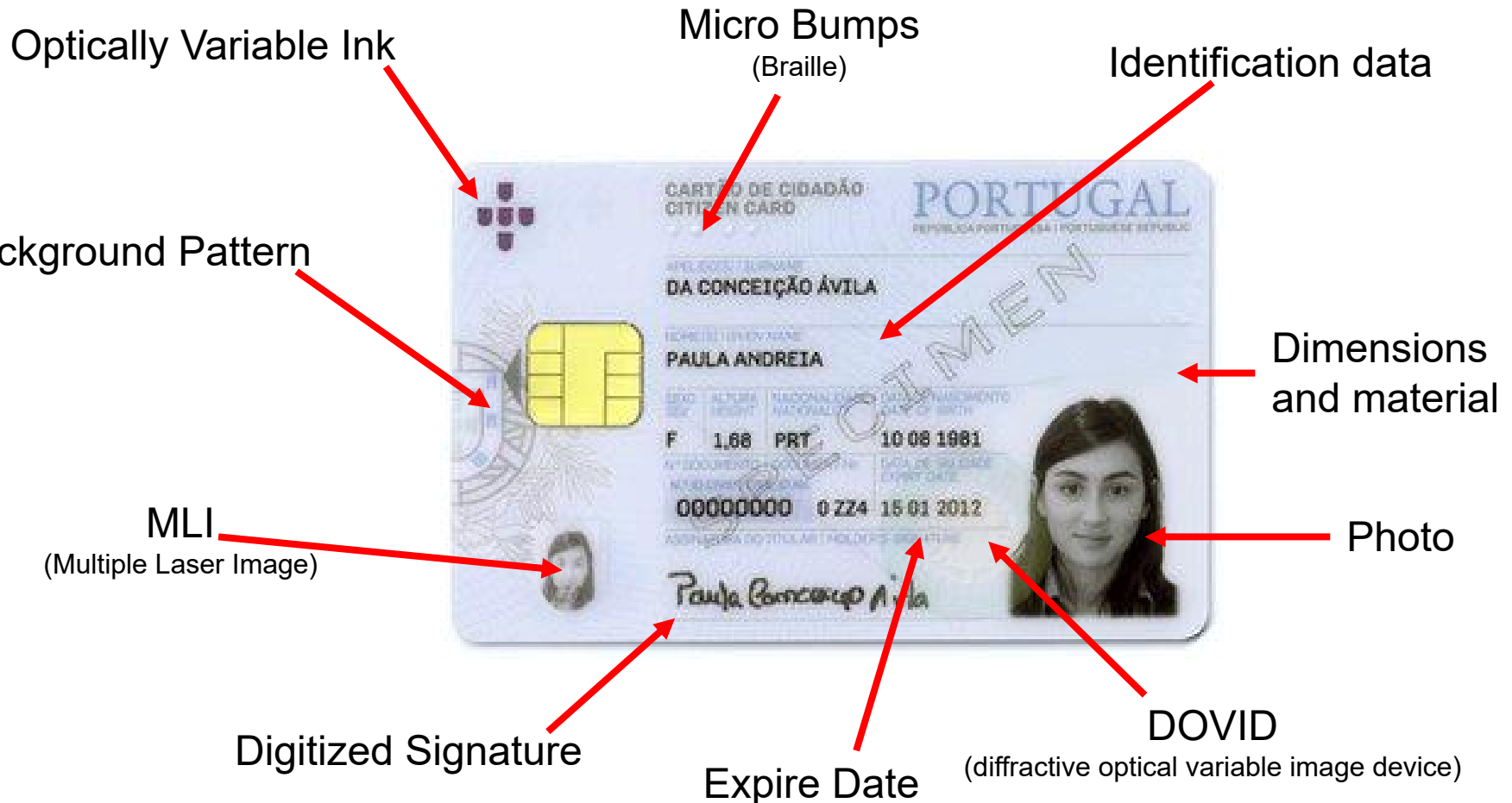


Portuguese Electronic Identity Card (PTeID)

Visual Security Attributes



Digital Attributes

All visible attributes except the digitized signature

Address

Template of the biometric fingerprint

2 cryptographic key pairs (Authentication and Signing)

5 public key certificates

- 2 related to the key pairs
- 3 with the intermediate CAs of the certification path

1 symmetric secret key, for EMV-CAP

- Europay, MasterCard, and Visa Chip Authentication Program

4 User Codes (PINs)

- Authentication, Signature, Address, PUK

PIN protection

Having physical access to the card is enough to:

- Obtain the owner address
- Obtain or use the private key for authentication
- Obtain or use the private key for digital signature
- Obtain or use the key for EMV-CAP (deprecated in 2016)

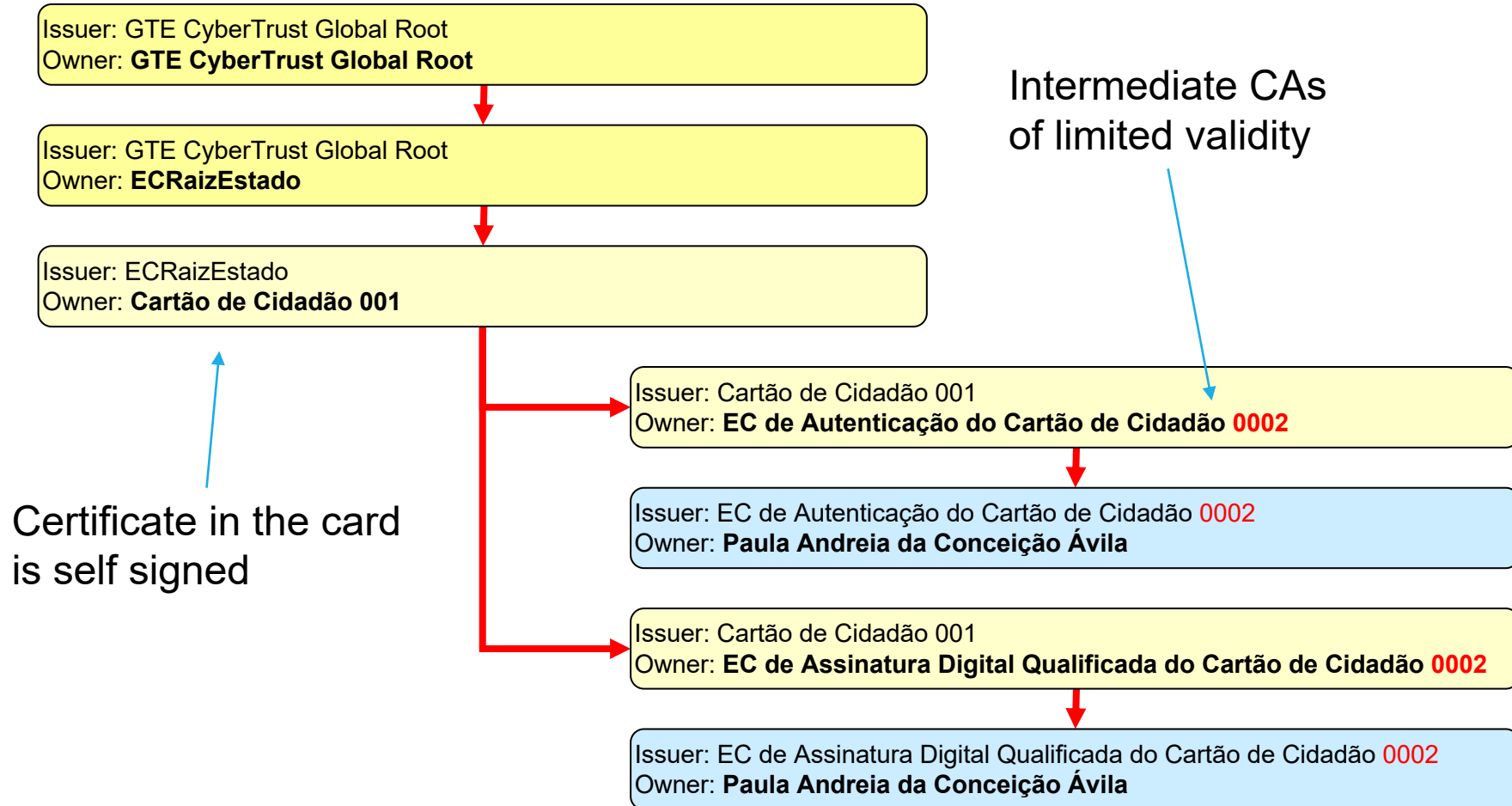
Actions are protected by an authentication code

- PIN with 4 numbers
- PIN is blocked after 3 incorrect attempts

Exceptions

- the address pin code in recent cards is '0000'

SmartCard Certificates



Objectives of the SmartCard certificates

Authenticate the card owner

- The owner can manually distribute the certificate to other individuals/services so that they can verify his identity

Authenticate other citizens with similar cards

- Certification chain is present in the card
- CC Certificate in the card is self signed
- CC Certificate publicly available has a different issuer

Certificates for two different operations

- Authentication in services
- Sign of digital documents (certificate only activated upon request)

Certificates in the SmartCard: Interoperation with other applications

Watchdog applications detect insertion and removal

Insertion

- Applications obtain certificates and can load them in the browser keystores
- A cache is created to speedup access to data
- Keys usage is still limited by knowing the PIN codes

Removal

- Applications remove certificates from the local keystores

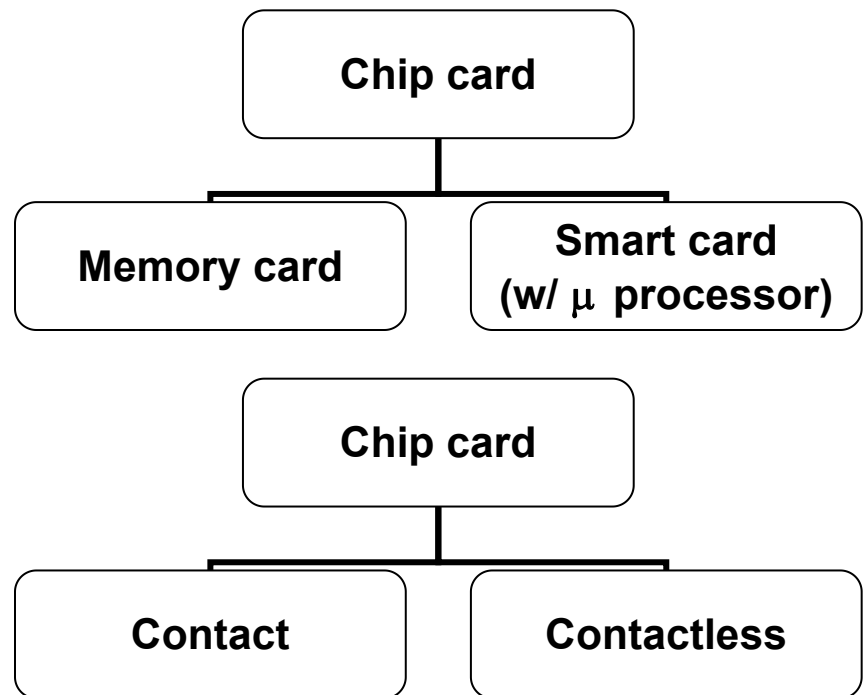
SmartCards: Concept

Card with computation capabilities

- CPU
- ROM
- EEPROM
- RAM

Interface

- With electric contacts
- Contactless



SmartCards: Components

CPU

- 8/16 bit
- Crypto-coprocessor (opt.)

ROM

- Operation System
- Communication
- Cryptographic algorithms

EEPROM

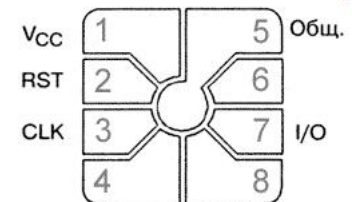
- File system
 - Programs / applications
 - Keys / Passwords

RAM

- Temporary data
- Lost when card is disconnected

Mechanical Contacts

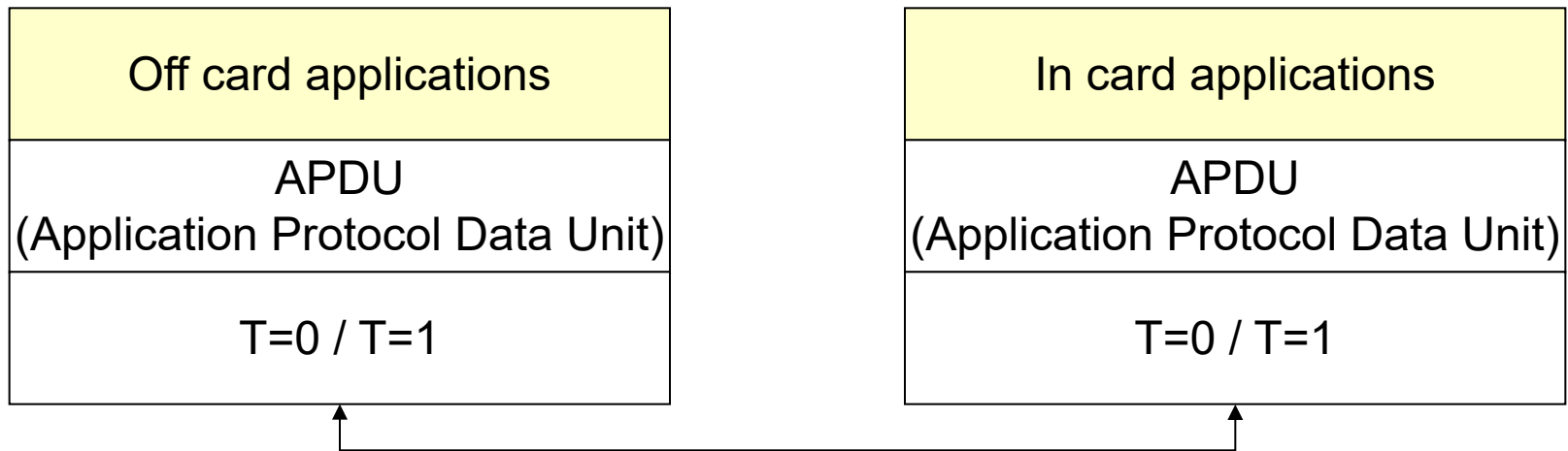
- ISO 7816-2
 - Power
 - Soft reset
 - Clock
 - Half duplex I/O



Physical Security

- Resistant to direct physical attacks
- Resistant to side channel attacks

Applications in SmartCards: Communication Stack



Applications in SmartCards: the Portuguese Citizen Card

IAS

- Authentication and Digital Signature
- Management of Asymmetric Cryptographic Keys

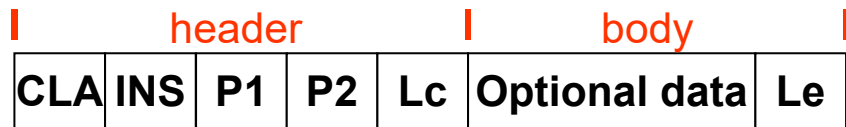
EMV-CAP

- Generation of one-time-passwords for alternative channels (telephone, fax, etc..)
- Removed in 2016

Match-on-Card

- Validation of biometric fingerprints

Interacting with the SmartCard: APDU (ISO 7816-4)



Command APDU

- CLA (1 byte)
 - Instruction Class
- INS (1 byte)
 - Command
- P1 e P2 (2 bytes)
 - Command specific parameters
- Lc
 - Length of the optional data
- Le
 - Length of the data contained in the response
 - Zero (0) means all data available

Response APDU

- SW1 e SW2 (2 bytes)
 - State byte
 - 0x9000 means SUCCESS

Interacting with the SmartCard: Lower level protocols: T=0 and T=1

T=0

- Data is sent one byte at a time
- Slower but widely supported
- Default mode

T=1

- Data is sent in blocks
- Faster but requires support

ATR (ISO 7816-3)

- Response to the RESET operation
- Provides many information, including the protocols


```
ATR: 3B 7D 95 00 00 80 31 80 65 B0 83 11 00 C8 83 00 90 00
+ TS = 3B --> Direct Convention
+ T0 = 7D, Y(1): 0111, K: 13 (historical bytes)
  TA(1) = 95 --> Fi=512, Di=16, 32 cycles/ETU
    125000 bits/s at 4 MHz, fMax for Fi = 5 MHz => 156250 bits/s
  TB(1) = 00 --> VPP is not electrically connected
  TC(1) = 00 --> Extra guard time: 0
+ Historical bytes: 80 31 80 65 B0 83 11 00 C8 83 00 90 00
  Category indicator byte: 80 (compact TLV data object)
    Tag: 3, len: 1 (card service data byte)
      Card service data byte: 80
        - Application selection: by full DF name
        - EF.DIR and EF.ATR access services: by GET RECORD(s) command
        - Card with MF
    Tag: 6, len: 5 (pre-issuing data)
      Data: B0 83 11 00 C8
    Tag: 8, len: 3 (status indicator)
      LCS (life card cycle): 00 (No information given)
      SW: 9000 (Normal processing.)
```

Possibly identified card (using /usr/share/pcsc/smartcard_list.txt):

```
3B 7D 95 00 00 80 31 80 65 B0 83 11 00 C8 83 00 90 00
3B 7D 95 00 00 80 31 80 65 B0 83 11 .. .. 83 00 90 00
  Portuguese ID Card (eID)
  http://www.cartaodecidadao.pt/
```

SmartCard Internal Object Representation

Tag-Length-Value (TLV)

- Tag: Object type
- Length: Object Length
- Value: Object Data

Each TLV is encoded according to eh ASN.1 BER rules

- Abstract Syntax Notation, Basic Encoding Rules

An object can contain other TLV

- Recursive Structure

Compact notation, allowing applications to ignore unknown object types

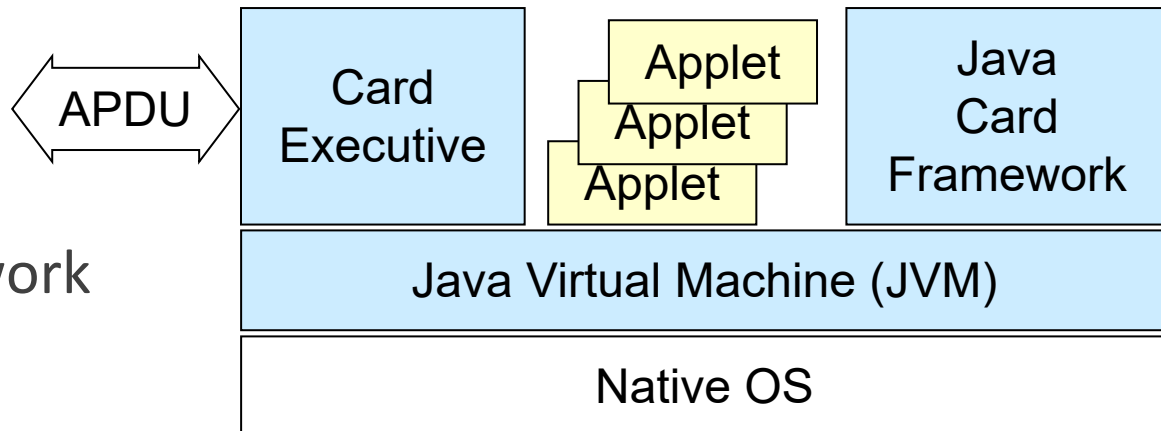
SmartCard Computation Model

SmartCards execute Applets Java

- Use the Java Card Runtime Environment (JCRC)
- JCRC executes on top of a native OS

JCRC

- Java Virtual Machine
- Card Executive
 - Card management
 - Communications
- Java Card Framework
 - Library and Functions



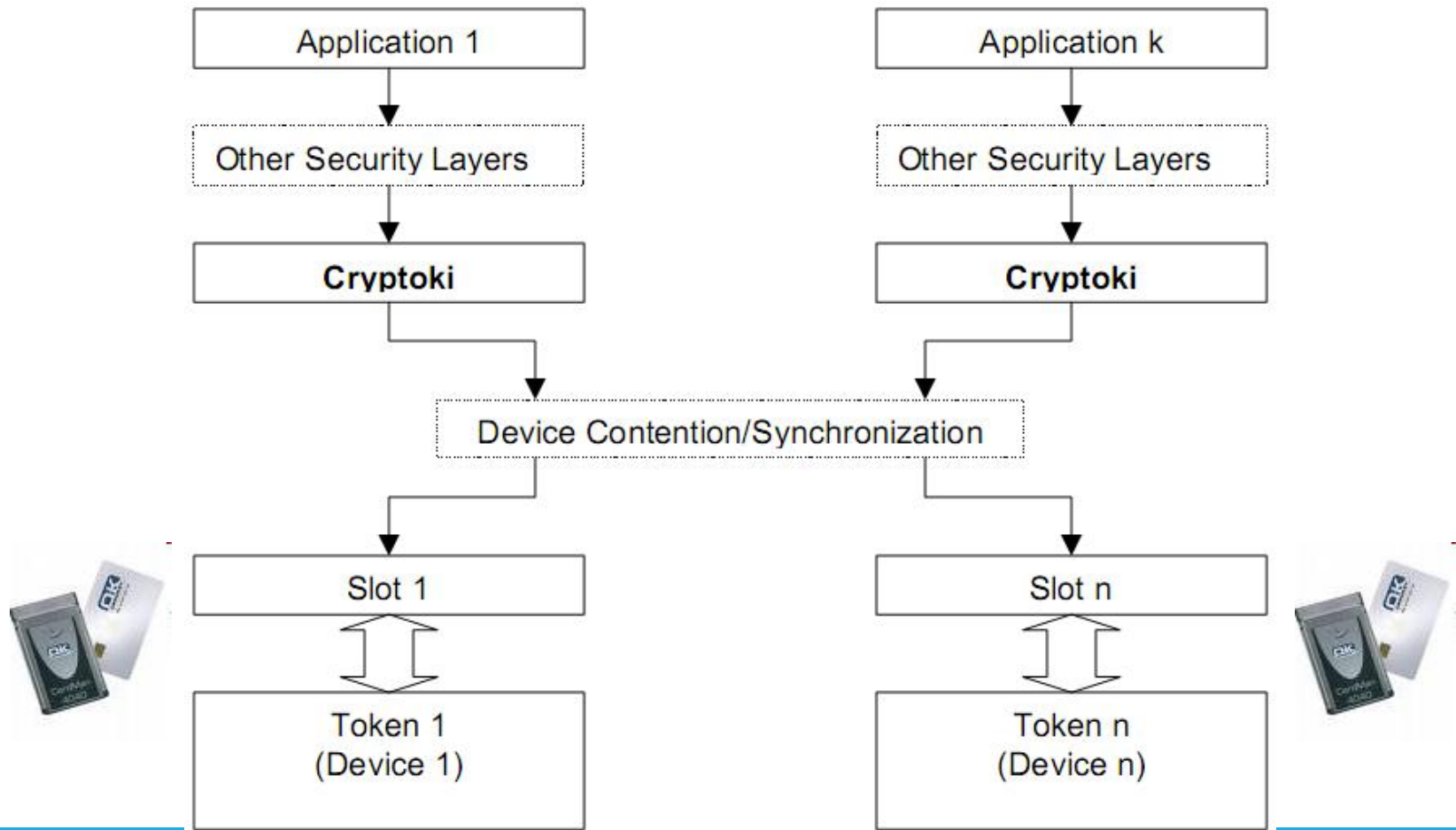
SmartCard Cryptographic Services Middleware

Libraries acting as bridges between the SmartCard and Higher Layer Applications

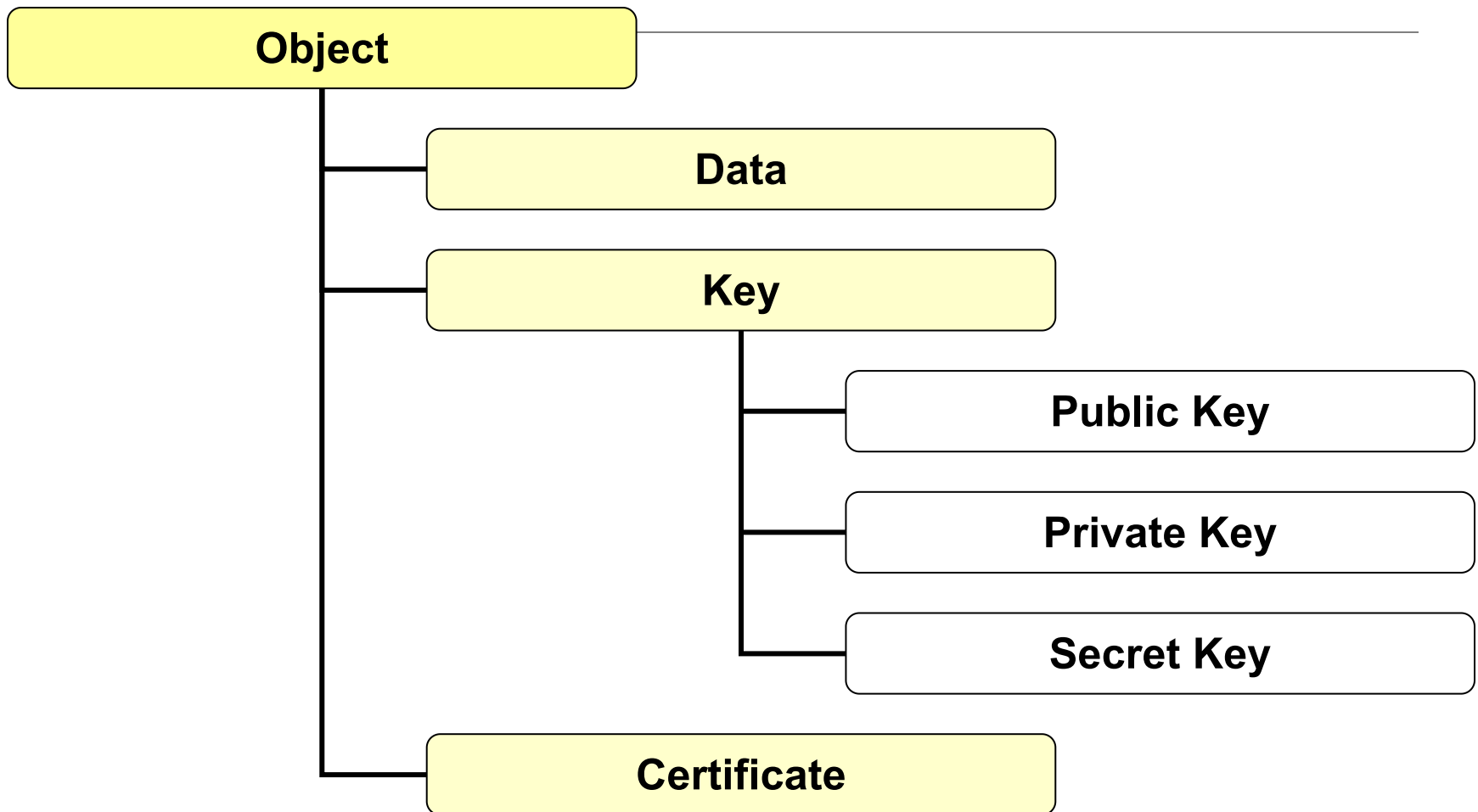
Based on standardized solutions:

- **PKCS #11: Token Access Primitives**
 - Cryptographic Token Interface Standard (cryptoki)
 - Defined by RSA Security Inc.
- **PKCS #15: Information Structure In the Token**
 - Cryptographic Token Information Format Standard
 - Defined by RSA Security Inc.
- **CAPI CSP: API**
 - CryptoAPI Cryptographic Service Provider
 - Defined by Microsoft for Windows applications
- **PC/SC: API**
 - Personal computer/Smart Card
 - Platform for access in Windows and Linux

PKCS #11: Interaction with applications



PKCS #11: Cryptoki Object Hierarchy



PKCS #11: Sessions

Logical connections between applications and SmartCards (tokens)

- Read-only Sessions
- Read-Write Sessions

Session Operations

- Administrative
 - Login/logout
- Object Management
 - Create or destroy objects in the card
- Cryptographic

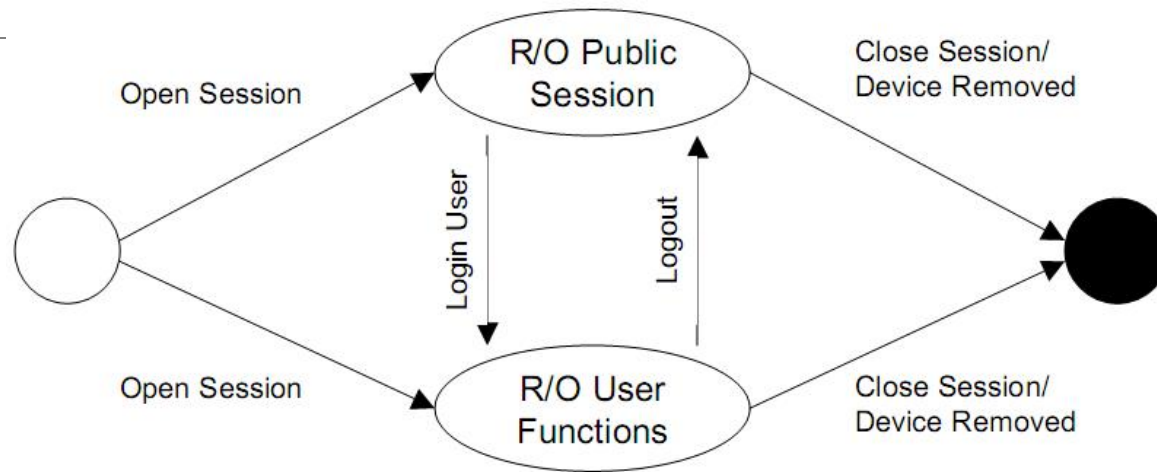
Session Objects

- Temporary objects created and valid during the session existence

Session Duration

- Usually only for a single operation

PKCS #11: Read-only sessions



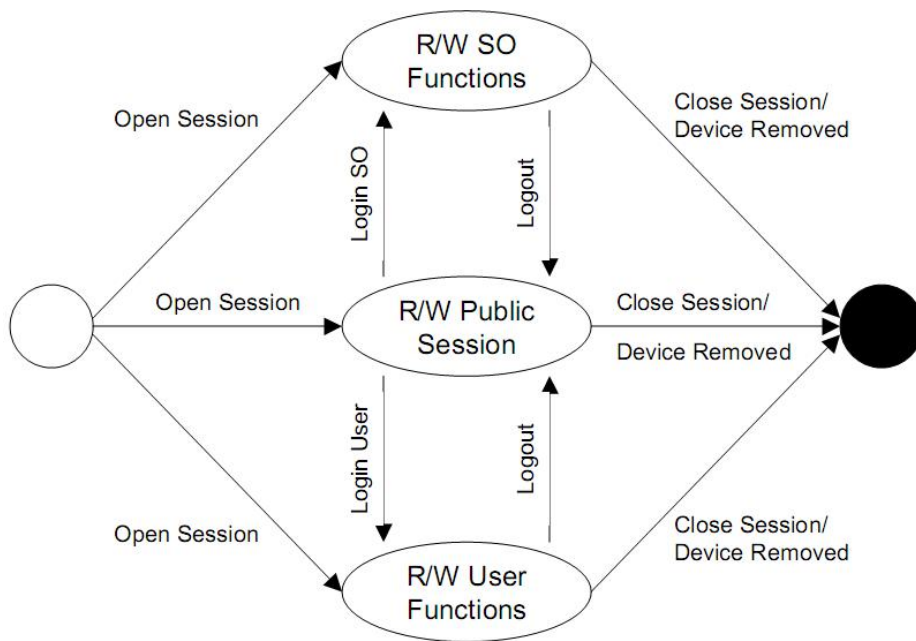
Public Read-Only Sessions

- Read access to the publicly readable objects
- Read-Write Access public session objects

User Specific Sessions

- Requires an authentication process (PIN code)
- Read access to public objects and objects available to that user
- Read-Write to all session objects (public and private)

PKCS #11: Read-Write Sessions



Read-Write Public Session

- Read or Write any public object

Read-Write Security Officer (SO) functions

- Read/Write Public Objects
- No access to private objects
- SO can redefine the user PIN codes

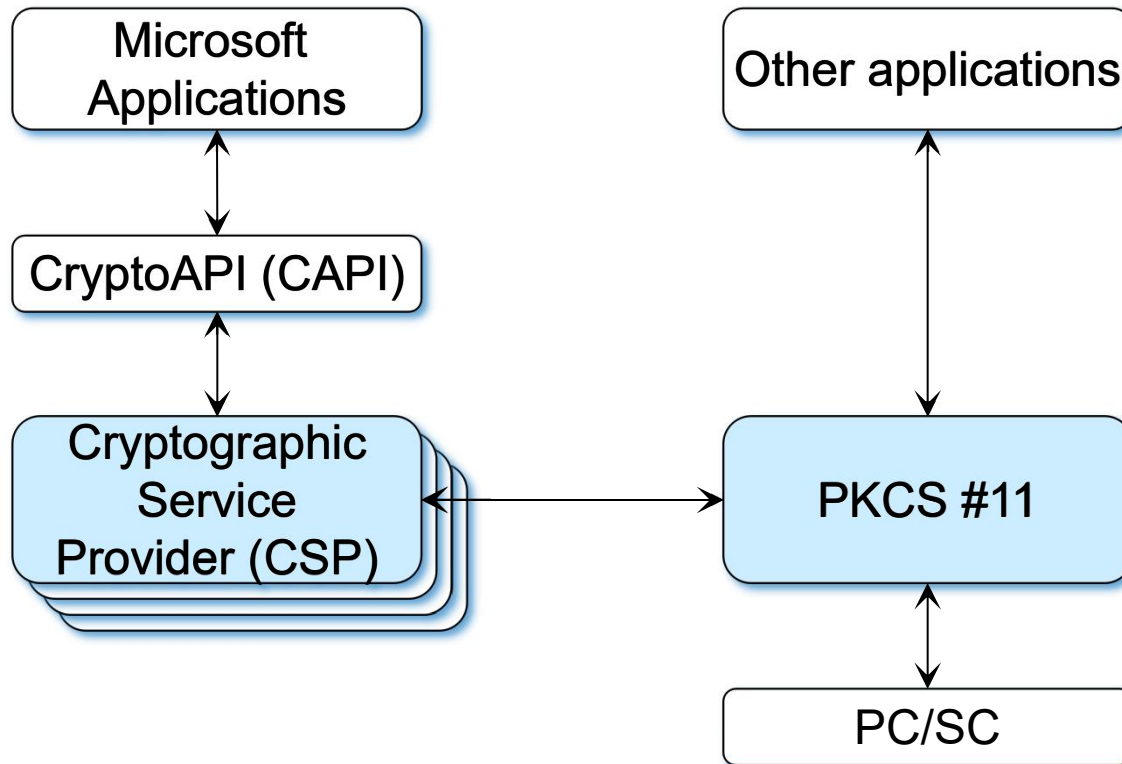
Read-Write User functions

- Read-Write all objects available to that user

Access is conditioned per user

- Objects (e.g. Objects)
- Functions (e.g., Sign)

PT Citizen Card: Windows



PKCS #11: Applied to the CC

Authentication PIN

- PKCS #11 User PIN

Signature PIN

- Not exposed by the PKCS #11 interface

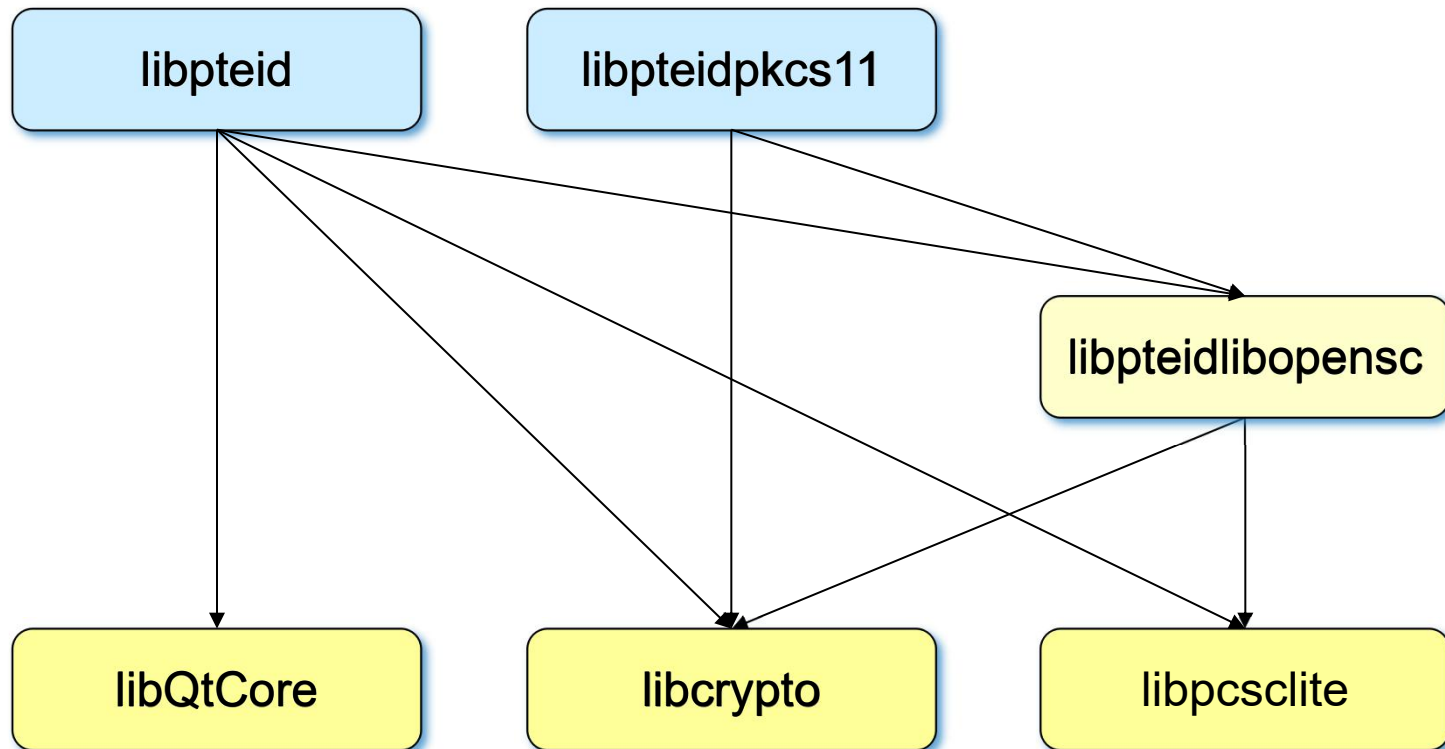
Address PIN

- Not exposed by the PKCS #11 interface

PKCS #11 SO PIN

- Not used by owners
- Used for recovery of remaining PIN codes
- Can be recovered using the biometric fingerprint

Citizen Card: Other OS



Citizen Card: Middleware

Public Distribution

- Windows
- macOS
- Linux
 - Caixa Mágica, Fedora, OpenSuse, Red Hat, Ubuntu

Languages

- Dynamic Libraries for C/C++
- Java Wrapper (JNI) to the C/C++ libraries
- C#.NET Wrapper C# .NET for the C/C++ libraries

Documentation

- Validação de Número de Documento do Cartão de Cidadão
- Autenticação com Cartão de Cidadão
- Manual Técnico do Middleware do Cartão de Cidadão
- Certificados e Entidades de Certificação
- Other

PT Citizen Card: PKI Services

Certificate Creation

- LDAP and Web

Certificate Revokation

- OCSP, delta-CRL e and CRL

PT Citizen Card: PTEID API

Additional API to interact with the Card

- Provided by libpteid.so

Allows access to Citizen Data

- Names, Photo, etc...

PTEID objects stored in the card as standard files

- 3f000003 = Trace
- 3f005f00ef02 = Citizen Data (Identification Data, Photo, etc...)
- 3f005f00ef05 = Citizen Address Data (Pin Protected)
- 3f005f00ef06 = SOd (Security Object Data)
- 3f005f00ef07 = Citizen Notepad