Smart Cards and the Electronic Citizen Cards

Smartcards

Hardware devices to store keys and do operations over the keys

- Sealed, resistant to side channel attacks or virus

Objective: allow the use of keys without its compromise

- Owner can use keys to do cryptographic operations
  - Symmetric or asymmetric ciphers
  - Authenticate the owner, generate document signatures, generate answers to challenges, store values

Uses:

- Authenticated, bank cards, Identity cards, SIM cards

Card has computational capabilities

- CPU
- ROM
- EEPROM
- RAM

Interface

- Contact
- Contactless

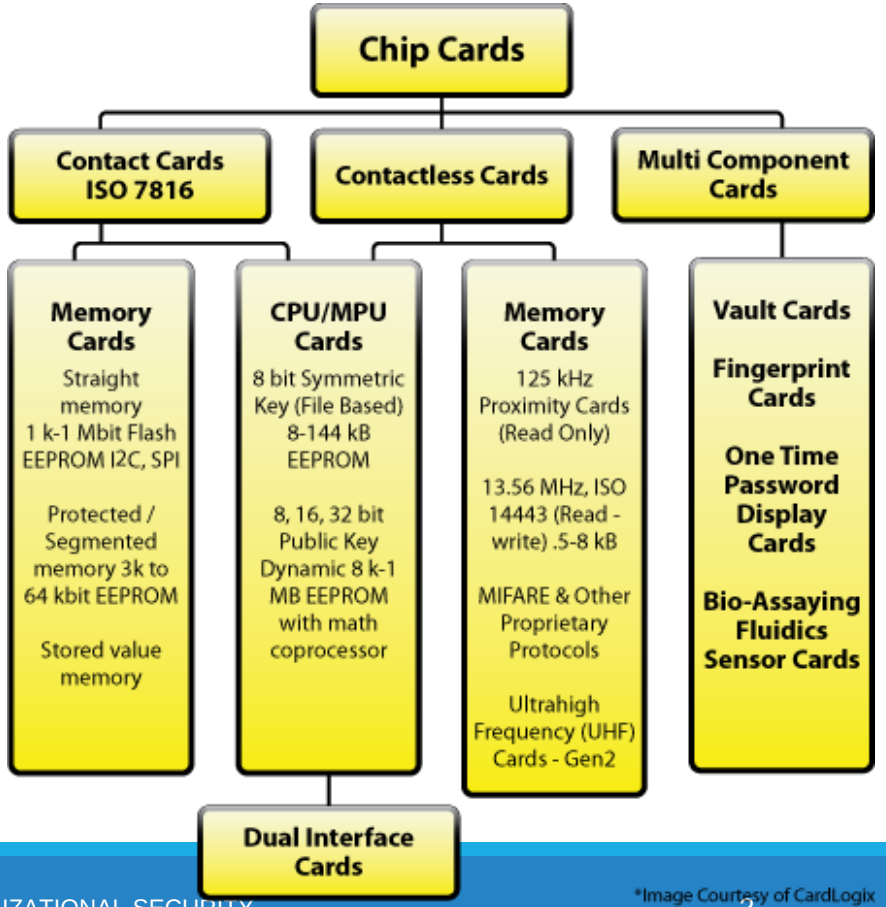


*Image Courtesy of CardLogix

SmartCards: Components

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

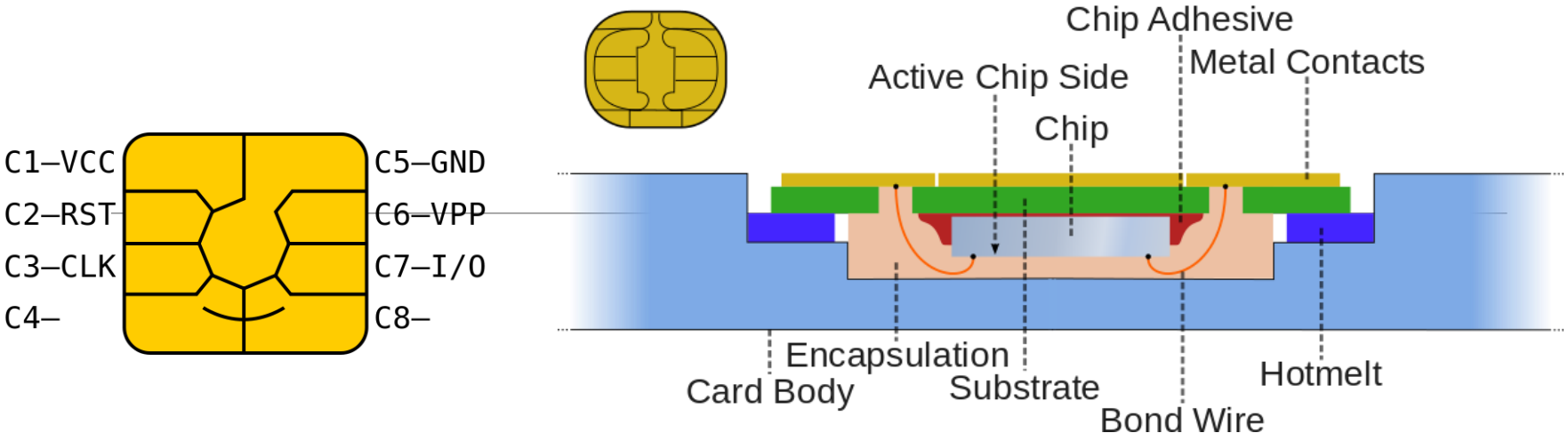
ROM
- Operation System
- Communication
- Cryptographic algorithms

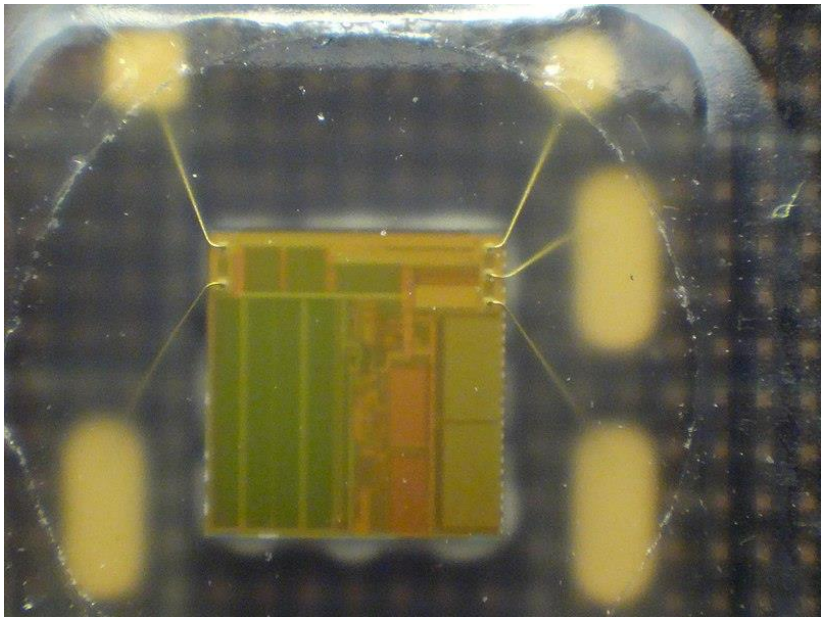
EEPROM
- File system
  - Programs / applications
  - Keys / Passwords

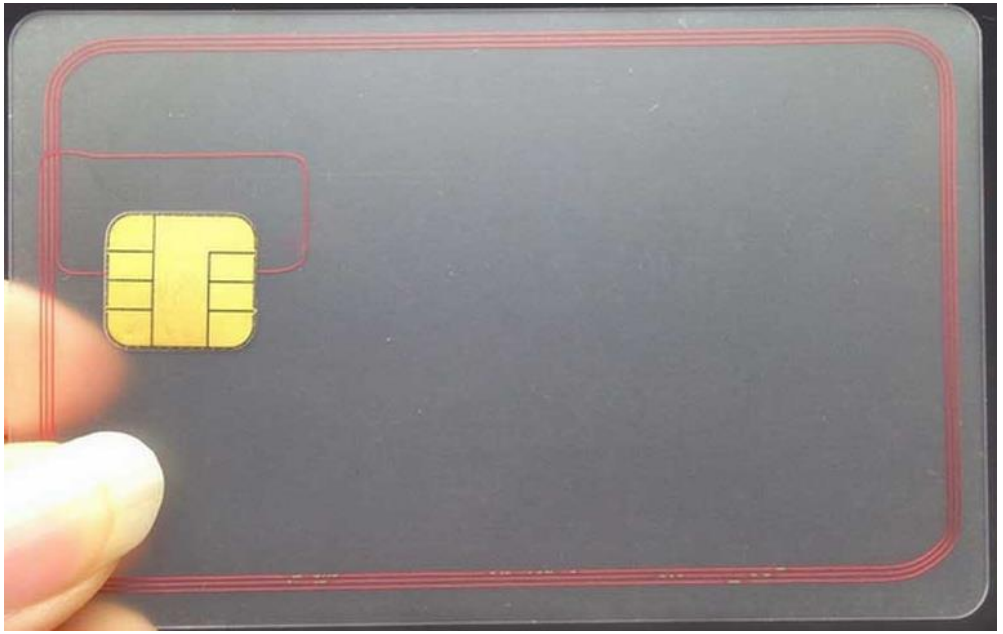
RAM
- Temporary data
  - Lost when card is disconnected

Mechanical Contacts
- ISO 7816-2

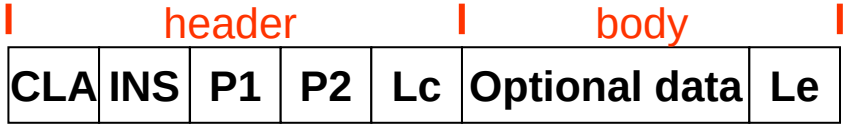
Physical Security
- Resistant to direct physical attacks
- Resistant to side channel attacks

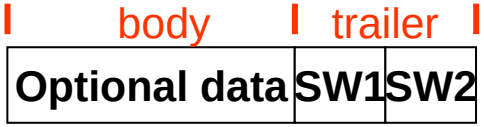

C1–VCC
C2–RST
C3–CLK
C4–
C5–GND
C6–VPP
C7–I/O
C8–
Chip Adhesive
Metal Contacts
Active Chip Side
Chip
Encapsulation
Card Body
Substrate
Bond Wire
Hotmelt





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

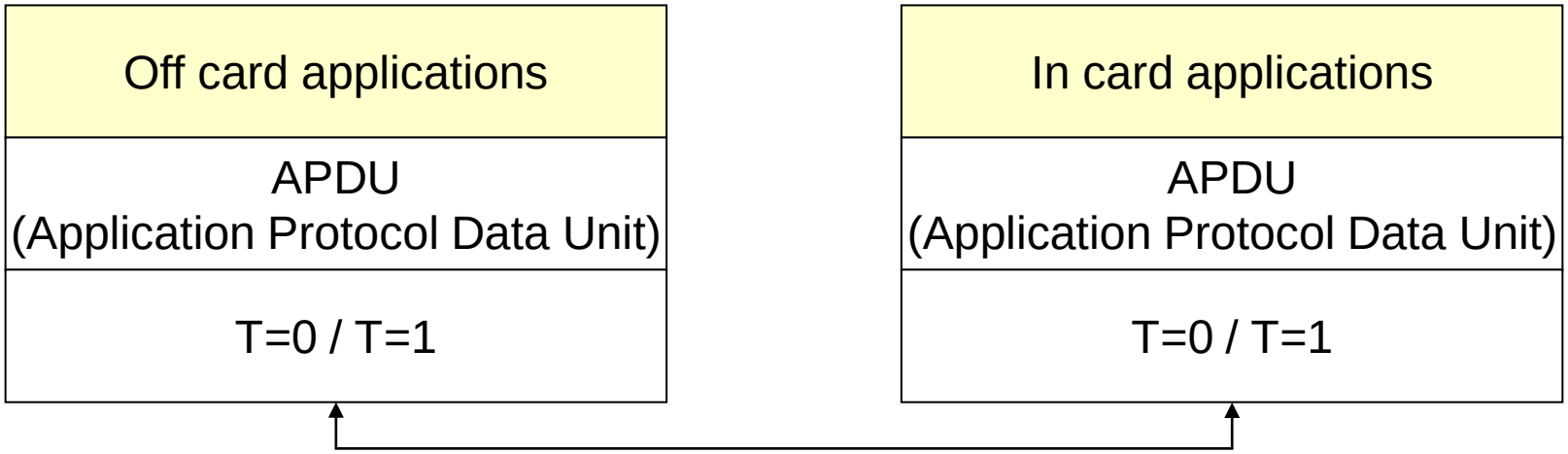
T=1

- Data is sent in blocks
- Faster but requires support

ATR (ISO 7816-3)

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

Applications in SmartCards: Communication Stack



```
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

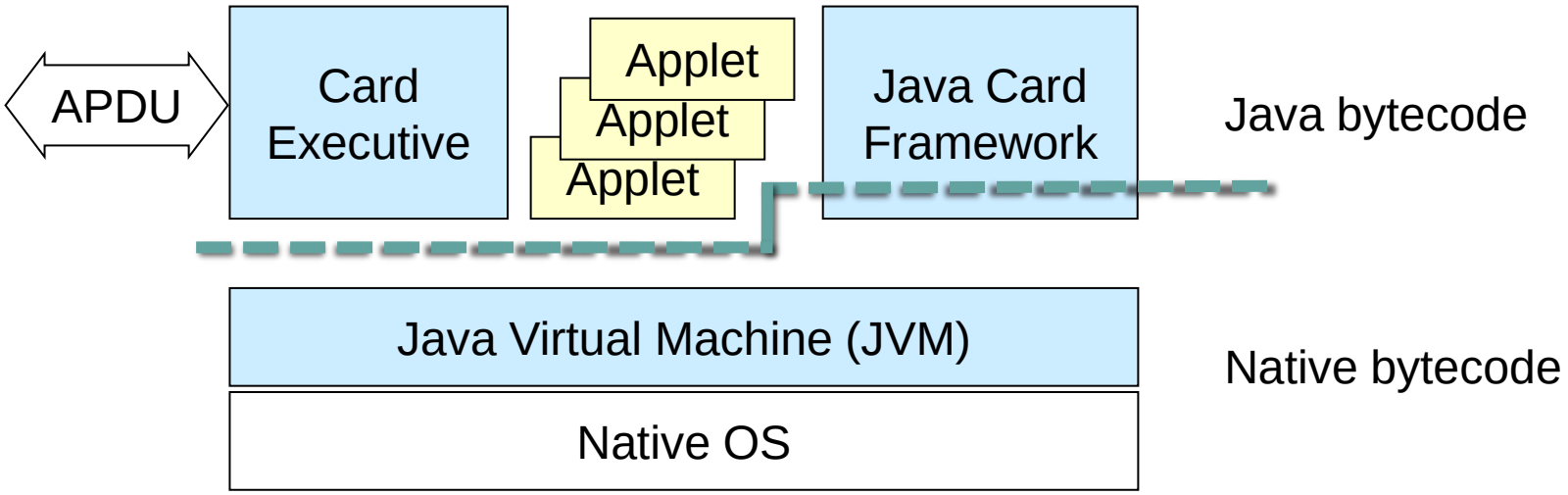
SmartCards execute Applets Java

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

JCRE

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

SmartCard Computation Model



PT Citizen Card

Identification Card with the same dimensions as a bank card

Provides information through multiple ways

- Digital
  - Interacting with the smart card chip
- Visual, readable by humans
  - Photo, numbers, name
- Visual, readable by machines
  - MRZ (Machine Readable Zone)

Visual Attributes Readable by Humans

Name
- Surname, Given Name, Parents

Physical attributes
- Gender and Height

Others
- Nationality
- Photo
- Written signature

Numbers
- Civil Identification Number
- Card number and validity
- other: VAT, Social Security, Public Health System

Card Version

Visual Attributes
Readable by machines

Name
- Surname, First Name, Other names
- Número de nomes

Physical attributes
- Gender

Others
- Birth date, and Nationality

Numbers
- Civil identification (and checksum)
- Doc number (and checksum)
- Documents created

Expiration Date


```
I<PRT000000000<<0<ZZ4<<<<<<<<2
8108108F1201158PRT<<<<<<<<<<1
AVILA<<PAULA<ANDREIA<CONCEICAO
```

Visual Security Attributes

Optically Variable Ink

Micro Bumps
(Braille)

Identification data

Background Pattern

Dimensions
and material

MLI
(Multiple Laser Image)

Photo

Digitized Signature

Expire Date

DOVID
(diffractive optical variable image device)

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'

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

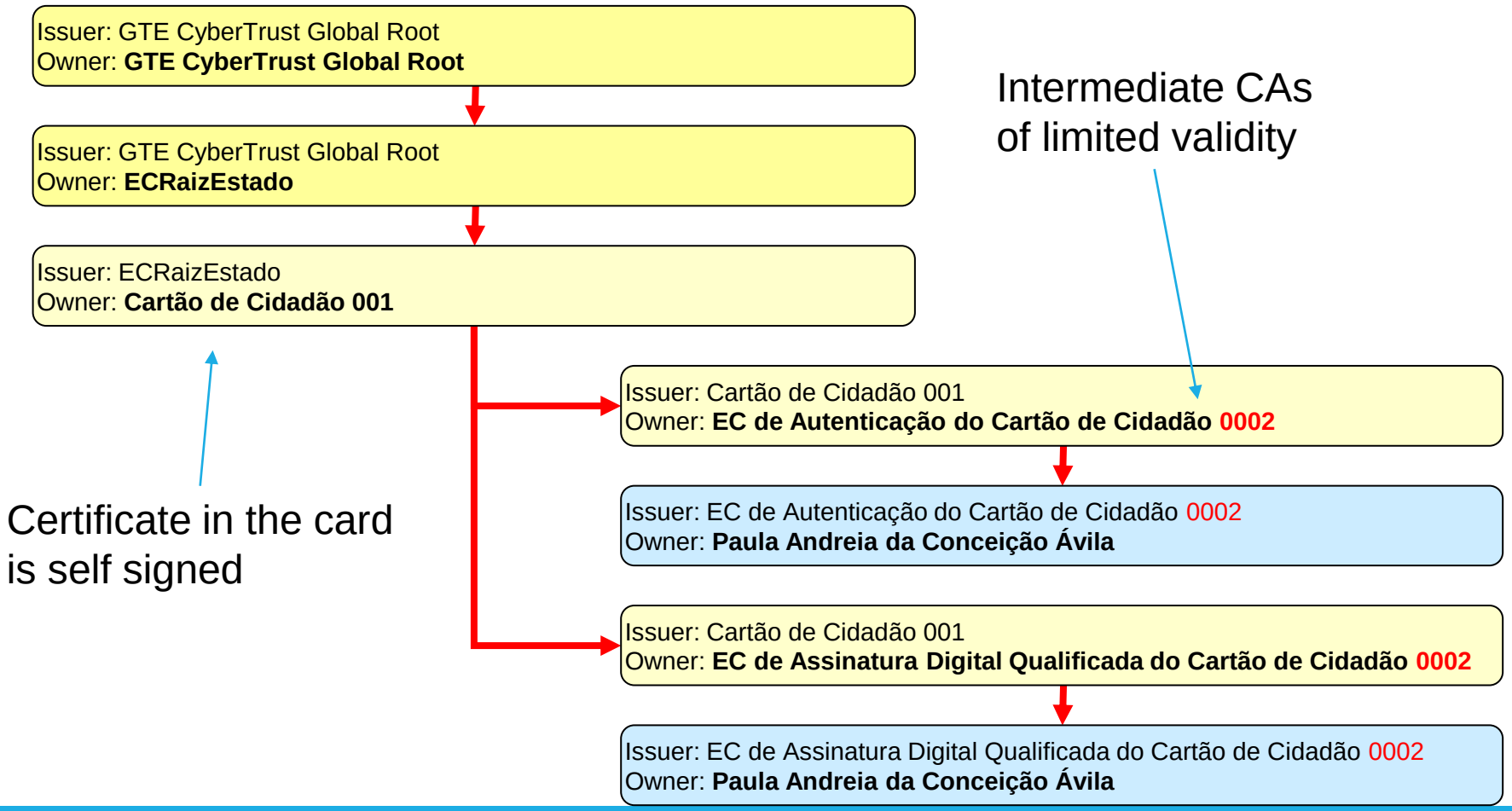
Authenticate other citizens with similar cards

- 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)

SmartCard Certificates



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

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

SmartCard Cryptographic Services Middleware

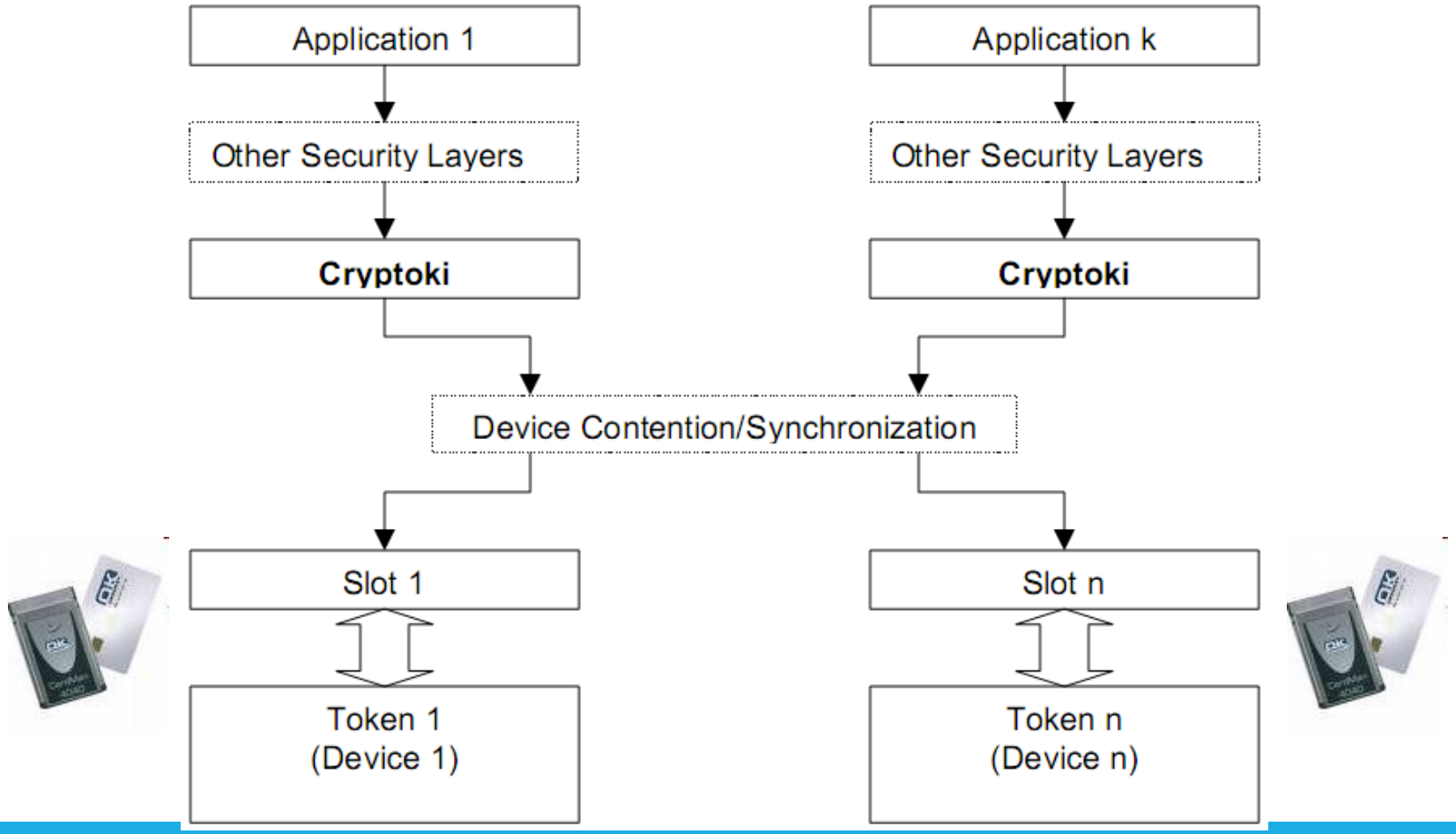
Libraries acting as bridges between the SmartCard and Higher Layer Applications

Based on standardized solutions:

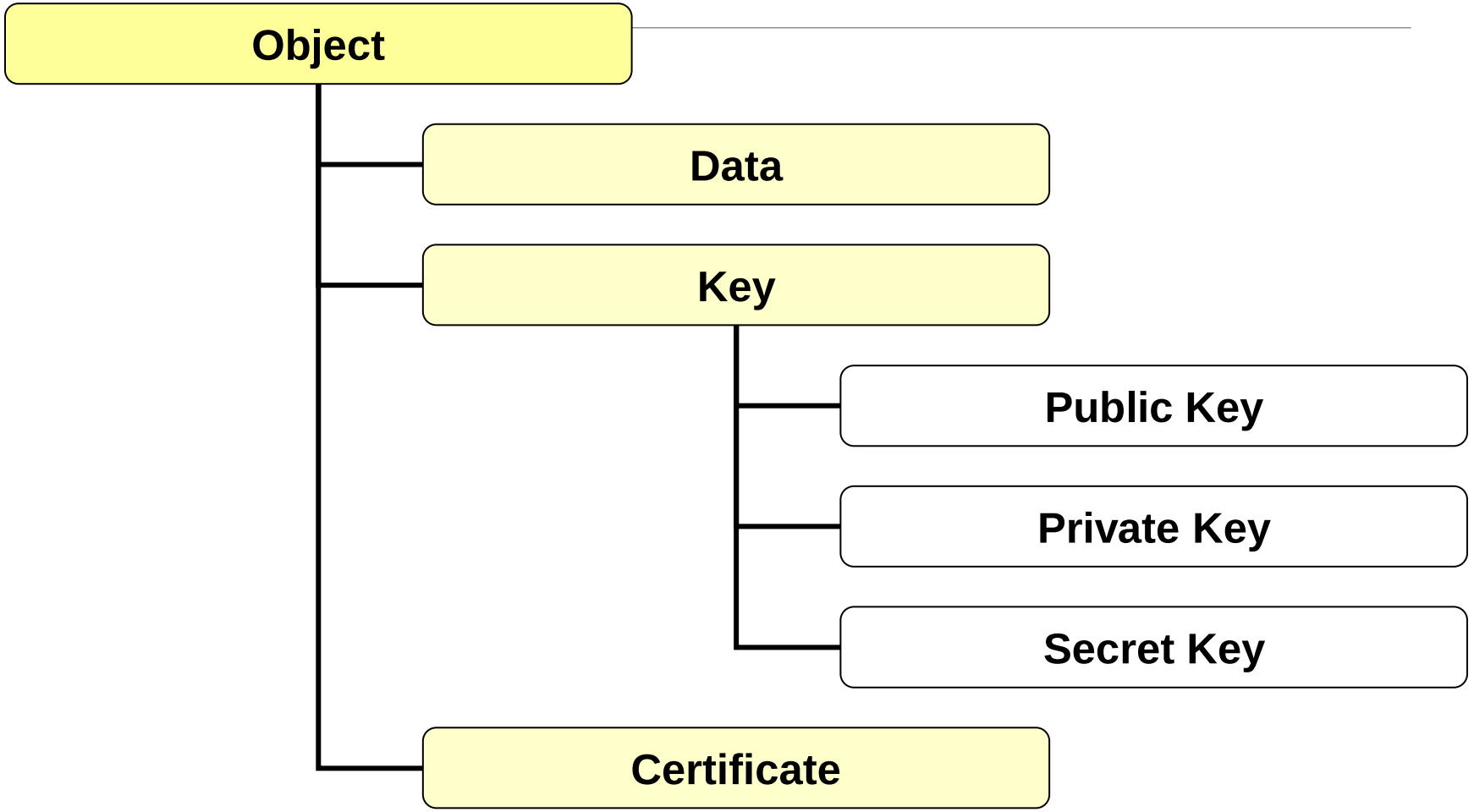
- PKCS #11: Token Access Primitives
  - Cryptographic Token Interface Standard (cryptoki)
  - Defined by RSA Security Inc.
- PKCS #15: Information Structure In the Token
  - Cryptographic Token Information Format Standard
  - Defined by RSA Security Inc.
- CAPI CSP: API
  - CryptoAPI Cryptographic Service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

PKCS#11

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

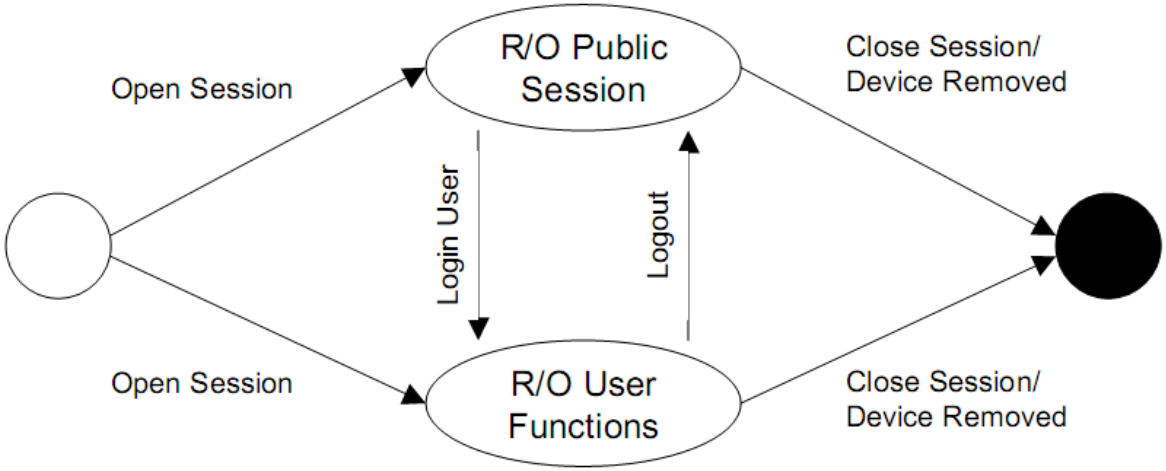
Session Objects

- Temporary objects created and valid during the session existence

Session Duration

- Usually only for a single operation

PKCS #11: Read-only sessions



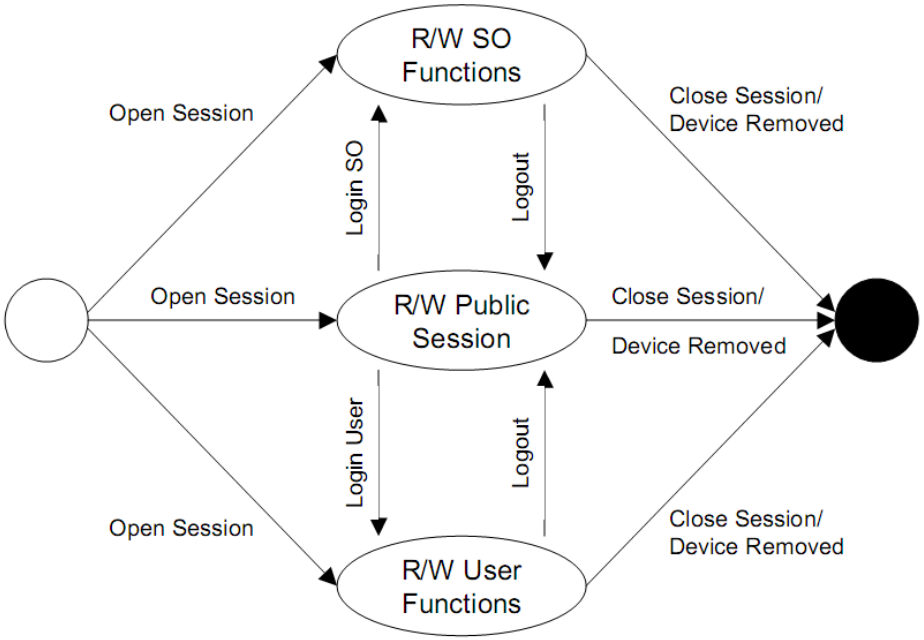
Public Read-Only Sessions

- 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)

PKCS #11: Concepts used

Authentication PIN

- User Code used in PKCS #11

Signing PIN

- Not exposed through PKCS #11

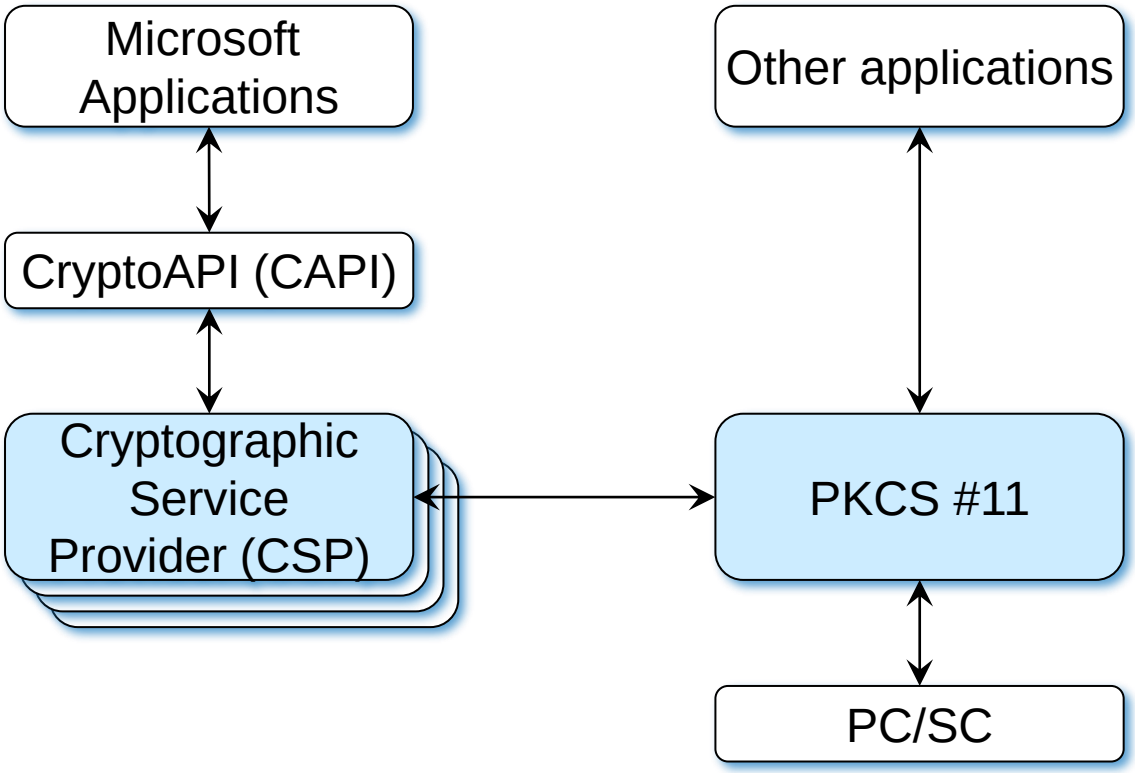
Address PIN

- Not exposed through PKCS #11
- 0000 by default in recent cards

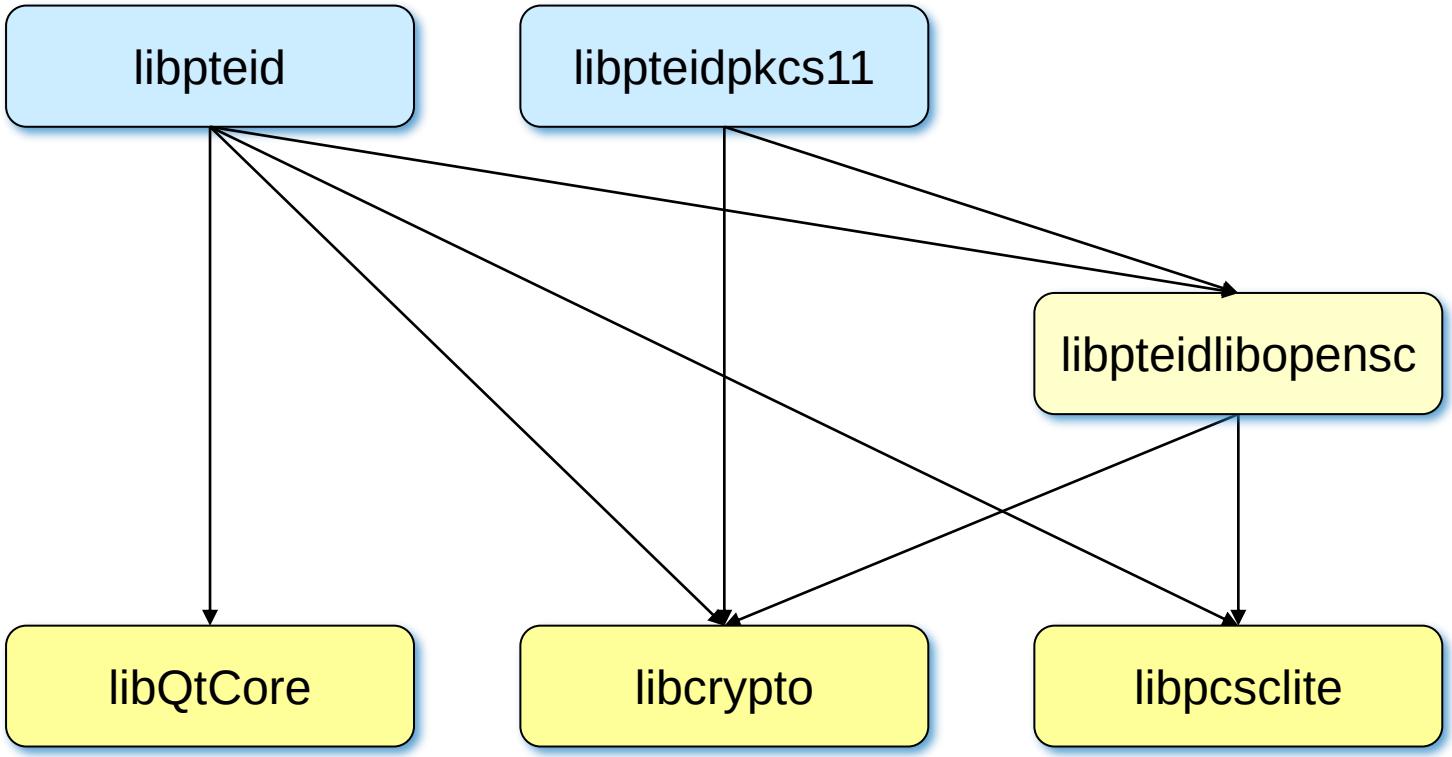
PKCS #11 SO PIN

- Not used by card owners

PT Citizen Card: Windows



Citizen Card: Other OS



PTEID middleware & SDK

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

PTEID middleware & SDK

Additional API to interact with the CC

- Provided by the libpteid.so library

Provides access to the data associated with the card

- Name, Picture, etc…

PTEID Objects stored as files

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

Document signing

PTEID allows the generation of signatures and these can be inserted in objects

- Email, PDF documents, …

Digital Signature replaces calligraphic signature

- Important in some regulatory contexts, public administration (UA grades)
- Natively supported in some formats

Uses the private key and the PKI temporal seal

- CC: http://ts.cartaodecidadao.pt/tsa/server
- Temporal Seal is vital to ensure the signature timestamp

Authentication with the PTEID

Authenticator sends NONCE to the CC to be signed with the private key

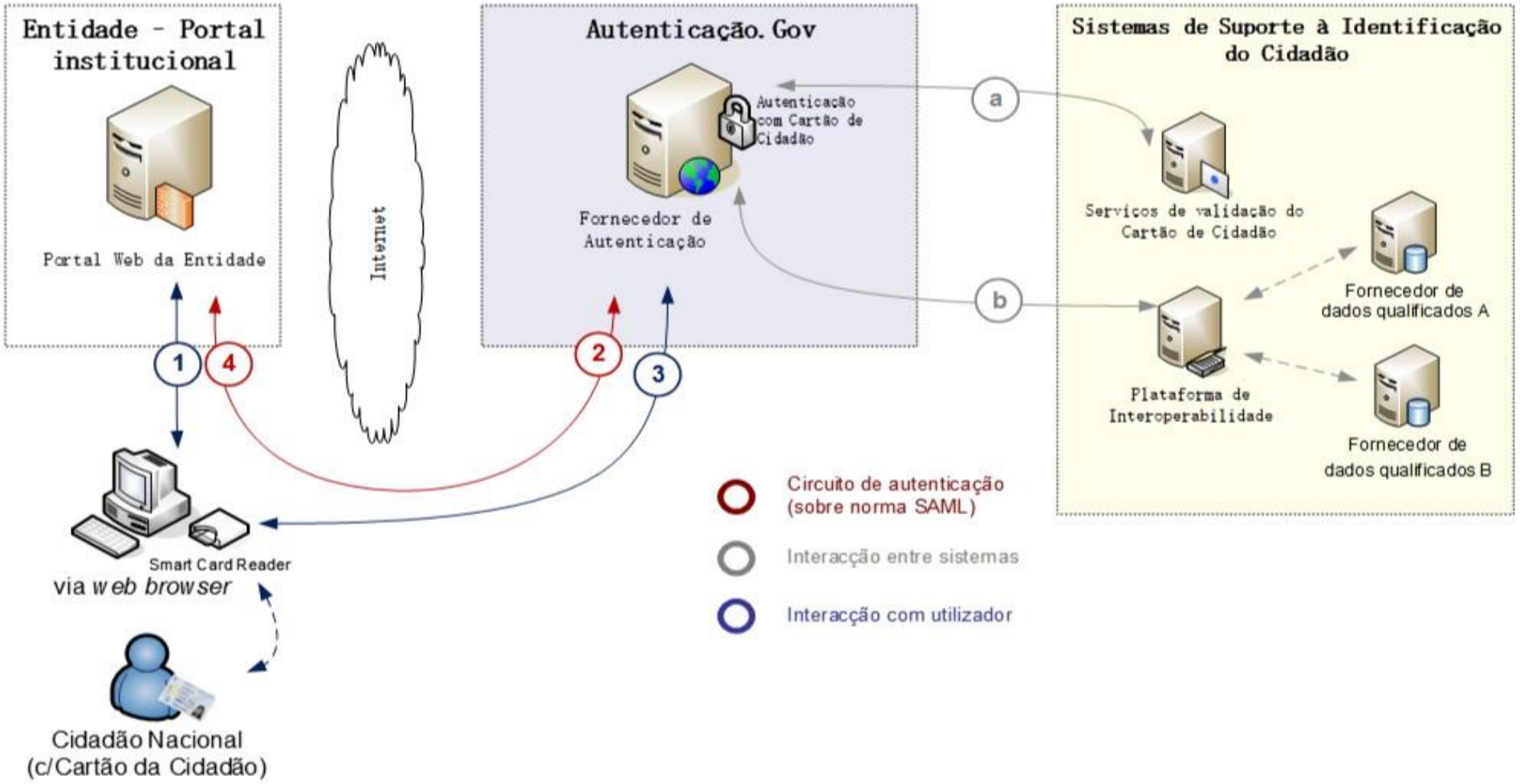
Issue: Browser do not have direct access to the CC

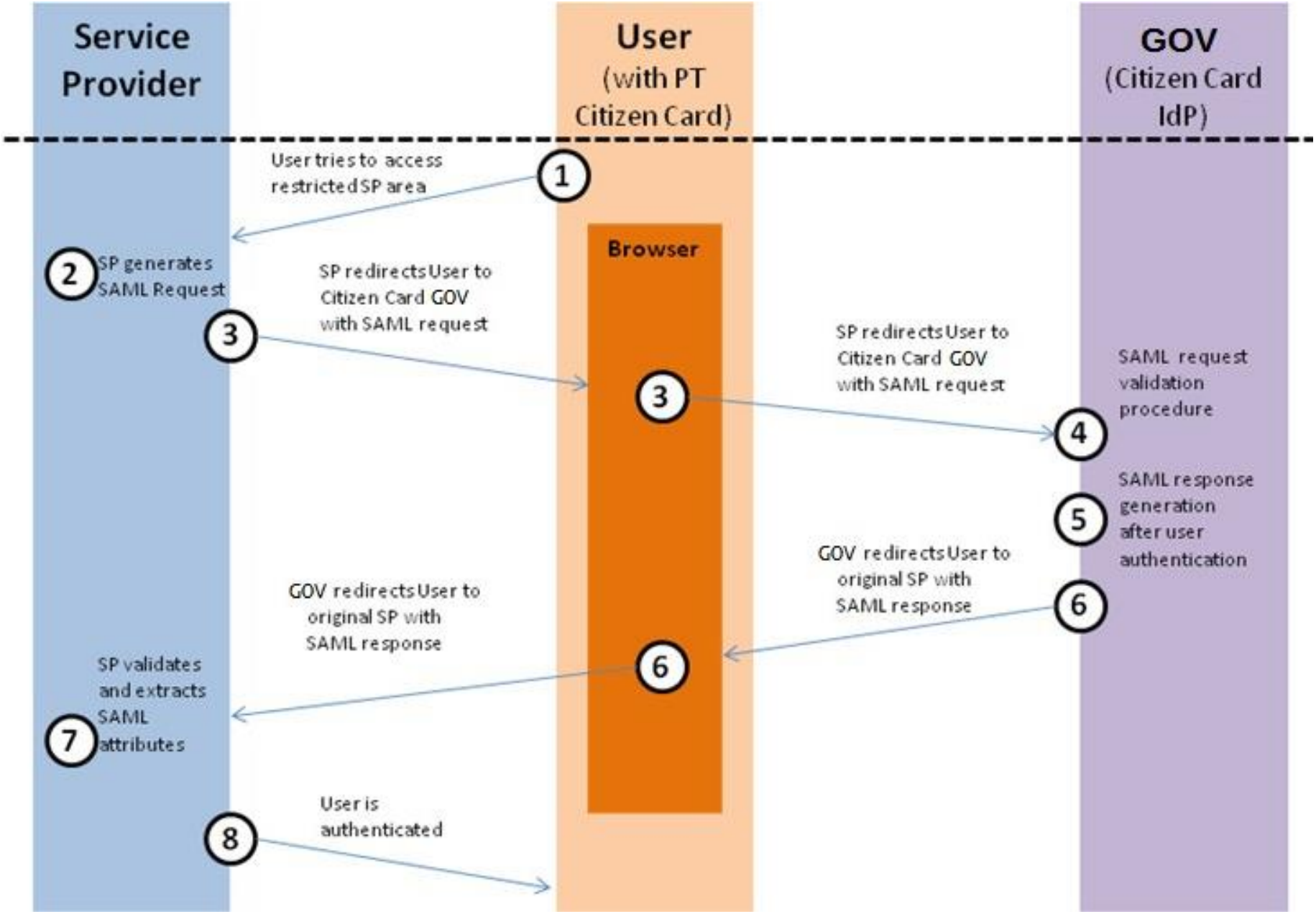
- Possible to configure libpteidpkcs11.so, limited to the PKCS#11 API
- Possible to use a java applet (obsolete)

Solution: Use a plugin installed in the user computer

- Exposes a web server to the localhost
- Allows access to the card through the web server
  - Only to authenticated requests through the CC infrastructure
- Required the previous approval of each new integration

Authentication Plugin




Service Provider
User (with PT Citizen Card)
GOV (Citizen Card IdP)
Browser
User tries to access restricted SP area
1
SP generates SAML Request
2
SP redirects User to Citizen Card GOV with SAML request
3
SP redirects User to Citizen Card GOV with SAML request
3
SAML request validation procedure
4
SAML response generation after user authentication
5
GOV redirects User to original SP with SAML response
6
GOV redirects User to original SP with SAML response
6
SP validates and extracts SAML attributes
7
User is authenticated
8

Mobile Digital Key (CMD)

Objective: allow authentication/signature even without the smartcard

- But with a similar level of security

Operation principles

- Requires a smartcard to authenticate the request of a CMD
- Users can authenticate themselves/sign documents using the CMD
- Doesn’t require any plugin installed
- Doesn’t require the card in future uses
- Uses 2FA: PIN code in the site + code through another channel
  - E.g: SMS or Twitter