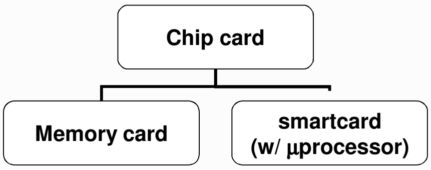
Smartcards

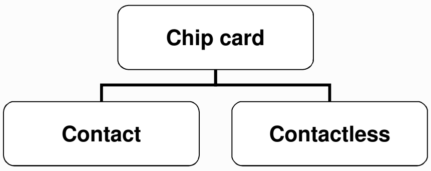
https://pplware.sapo.pt/informacao/saiba-como-renovar-online-o-seu-cartao-de-cidadao/
https://knowtechie.com/security-matters-5-benefits-of-contactless-smart-cards/

Smartcard: Definition

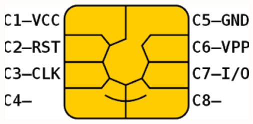
▷ Card with computing processing capabilities
- CPU
- ROM
- EEPROM
- RAM



▷ Interface
- With contact
- Contactless

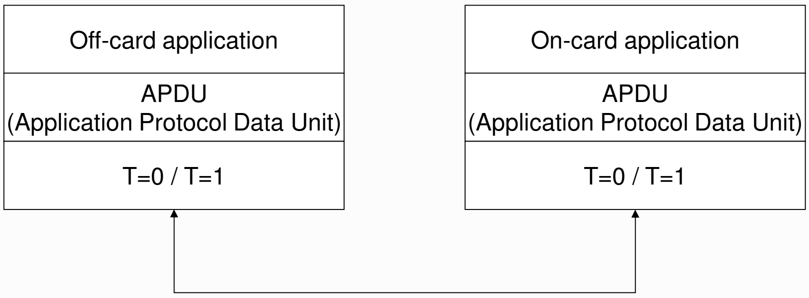


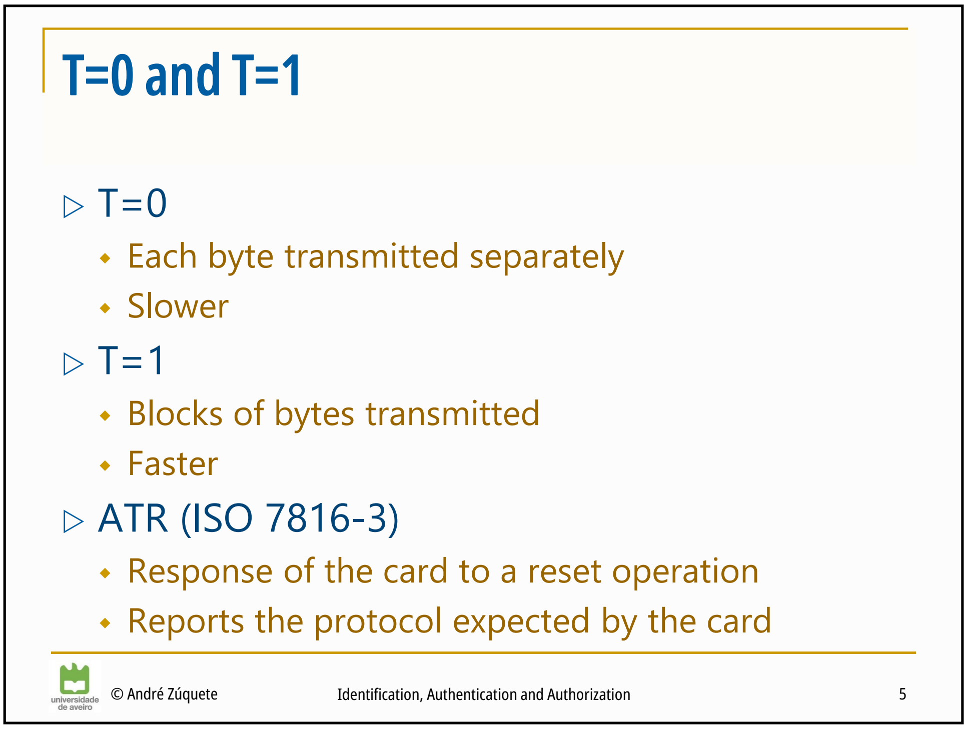
Smartcard: Components



- ▷ CPU
  - 8/16 bit
  - Crypto-coprocessor (opt.)
- ▷ ROM
  - Operating system
  - Communication
  - Cryptographic algorithms
- ▷ EEPROM
  - File system
    - Programs / applications
    - Keys / passwords
- ▷ RAM
  - Transient data
    - Erased on power off
- ▷ Mechanical contacts
  - ISO 7816-2
    - Power
    - Soft reset
    - Clock
    - Half duplex I/O
- ▷ Physical security
  - Tamperproof case
  - Resistance to side-channel attacks

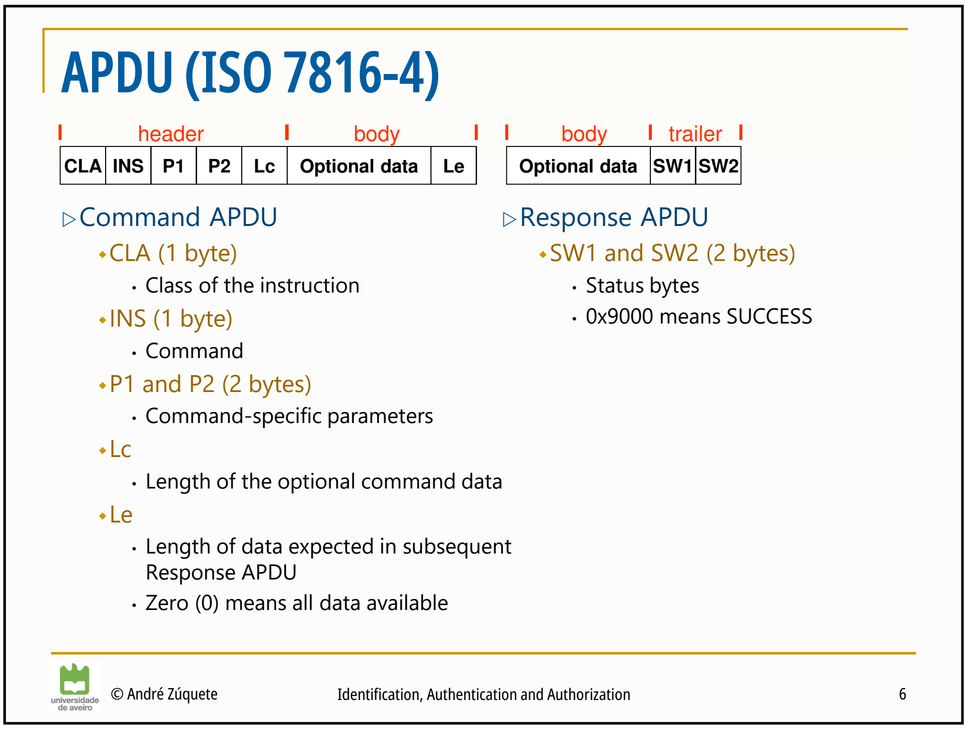
Smartcard applications: Communication protocol stack





T=0 and T=1

- T=0
  - Each byte transmitted separately
  - Slower
- T=1
  - Blocks of bytes transmitted
  - Faster
- ATR (ISO 7816-3)
  - Response of the card to a reset operation
  - Reports the protocol expected by the card

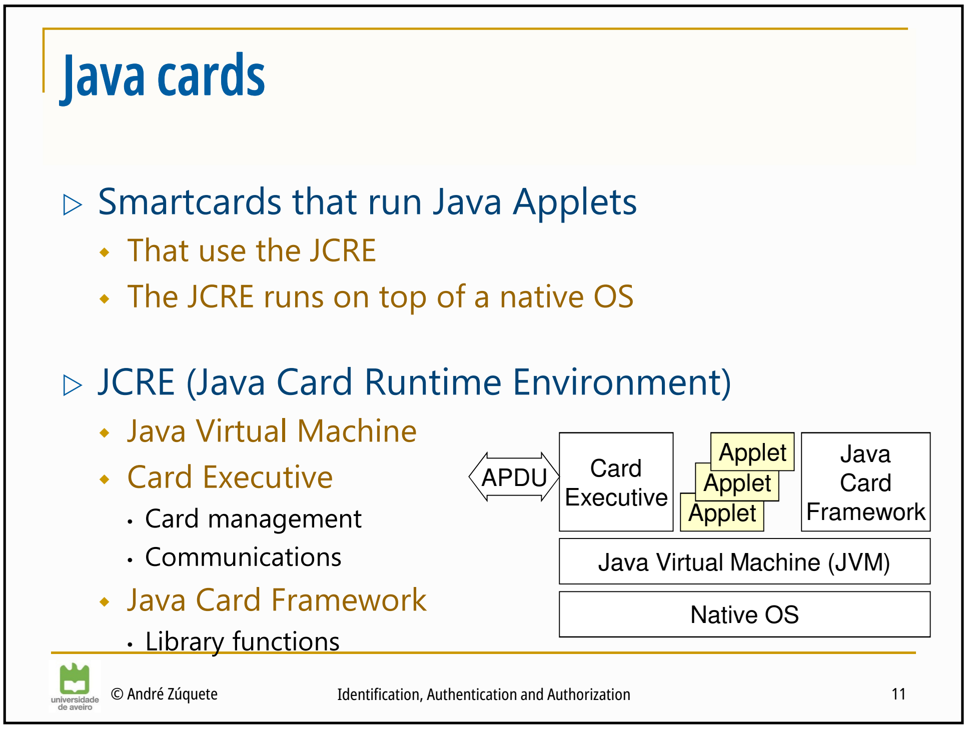


APDU (ISO 7816-4)

header					body	
CLA	INS	P1	P2	Lc	Optional data	Le

body	trailer	
Optional data	SW1	SW2

- Command APDU
  - CLA (1 byte)
    - Class of the instruction
  - INS (1 byte)
    - Command
  - P1 and P2 (2 bytes)
    - Command-specific parameters
  - Lc
    - Length of the optional command data
  - Le
    - Length of data expected in subsequent Response APDU
    - Zero (0) means all data available
- Response APDU
  - SW1 and SW2 (2 bytes)
    - Status bytes
    - 0x9000 means SUCCESS



Java cards

- ▷ Smartcards that run Java Applets
  - That use the JCRE
  - The JCRE runs on top of a native OS
- ▷ JCRE (Java Card Runtime Environment)
  - Java Virtual Machine
  - Card Executive
    - Card management
    - Communications
  - Java Card Framework
    - Library functions

APDU

Card Executive

Applet

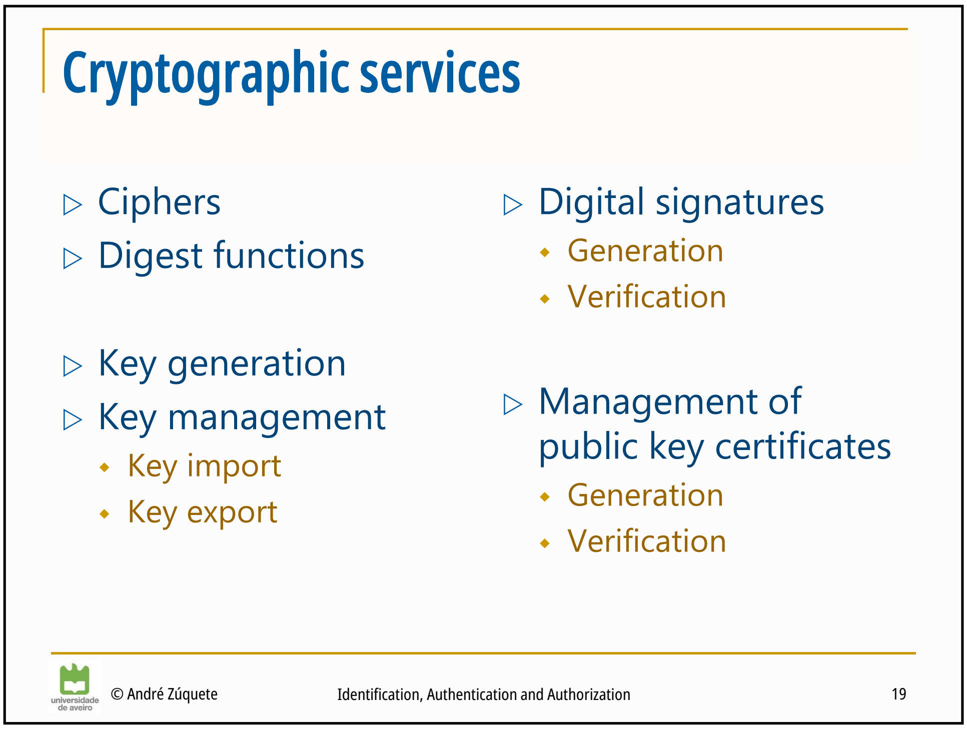
Applet

Applet

Java Card Framework

Java Virtual Machine (JVM)

Native OS



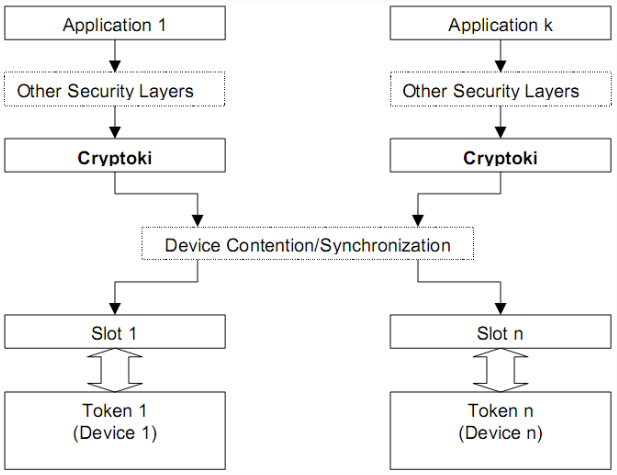
Cryptographic services

- ▷ Ciphers
- ▷ Digest functions
- ▷ Key generation
- ▷ Key management
  - Key import
  - Key export
- ▷ Digital signatures
  - Generation
  - Verification
- ▷ Management of public key certificates
  - Generation
  - Verification

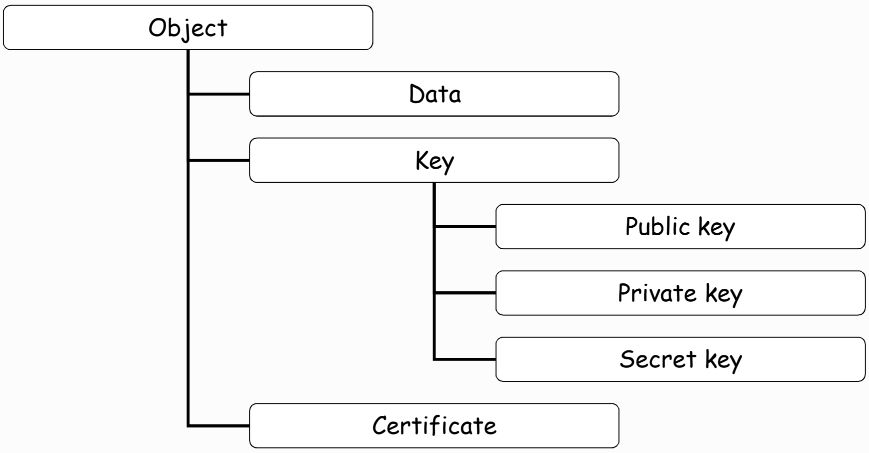
Cryptographic services: Middleware

- ▷ Libraries that bridge the gap between functionalities of smartcards and high-level applications
- ▷ Some standard approaches:
  - PKCS #11
    - Cryptographic Token Interface Standard (Cryptoki)
    - Defined by RSA Security Inc.
  - PKCS #15
    - Cryptographic Token Information Format Standard
    - Defined by RSA Security Inc.
  - CAPI CSP
    - CryptoAPI Cryptographic Service Provider
    - Defined by Microsoft for Windows systems
  - PC/SC
    - Personal computer/smartcard
    - Standard framework for smartcard access on Windows systems

PKCS #11: Cryptoki middleware integration

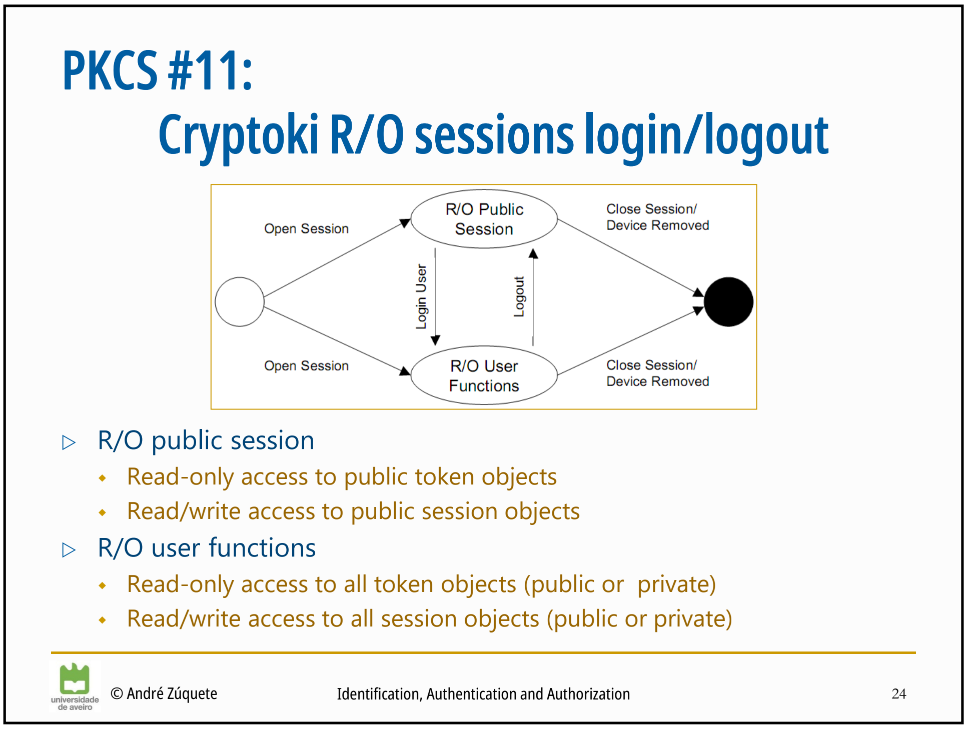


PKCS #11: Cryptoki object hierarchy



PKCS #11: Cryptoki sessions

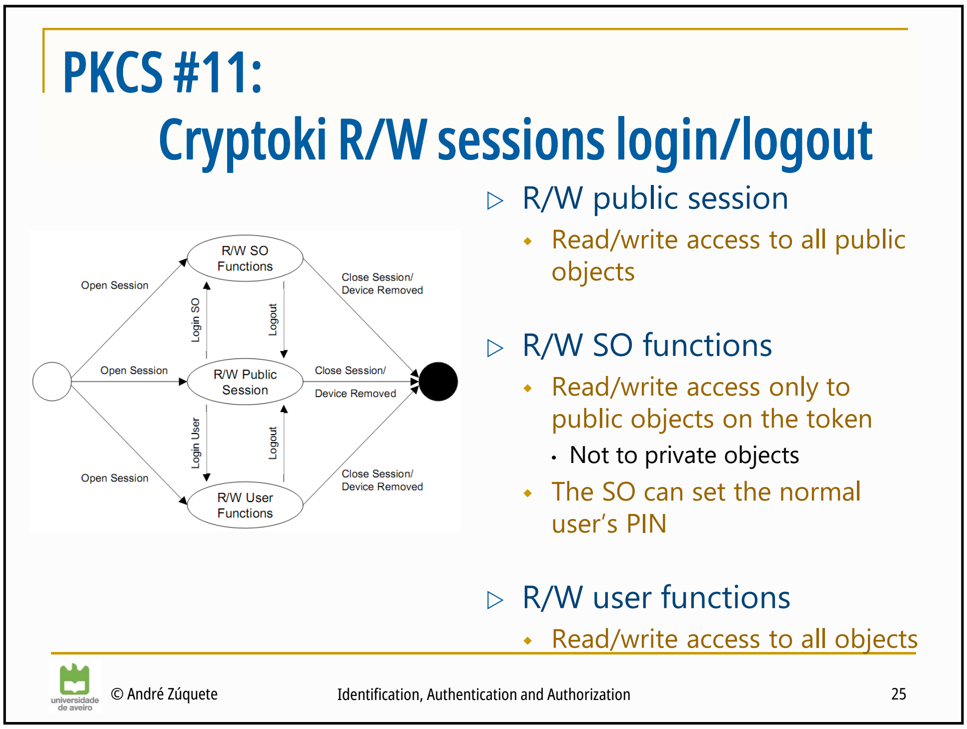
- Logical connections between applications and tokens
  - R/O and R/W sessions
  - Session owners
    - Public
    - User
    - Security Officer (SO)
- Lifetime of sessions
  - Usually for a single operation on the token
- Operations on open sessions
  - Administrative
    - Login/logout
  - Object management
    - Create / destroy an object on the token
  - Cryptographic
- Session objects
  - Transient objects created during sessions



PKCS #11: Cryptoki R/O sessions login/logout

Open Session
R/O Public Session
Close Session/ Device Removed
Login User
Logout
Open Session
R/O User Functions
Close Session/ Device Removed

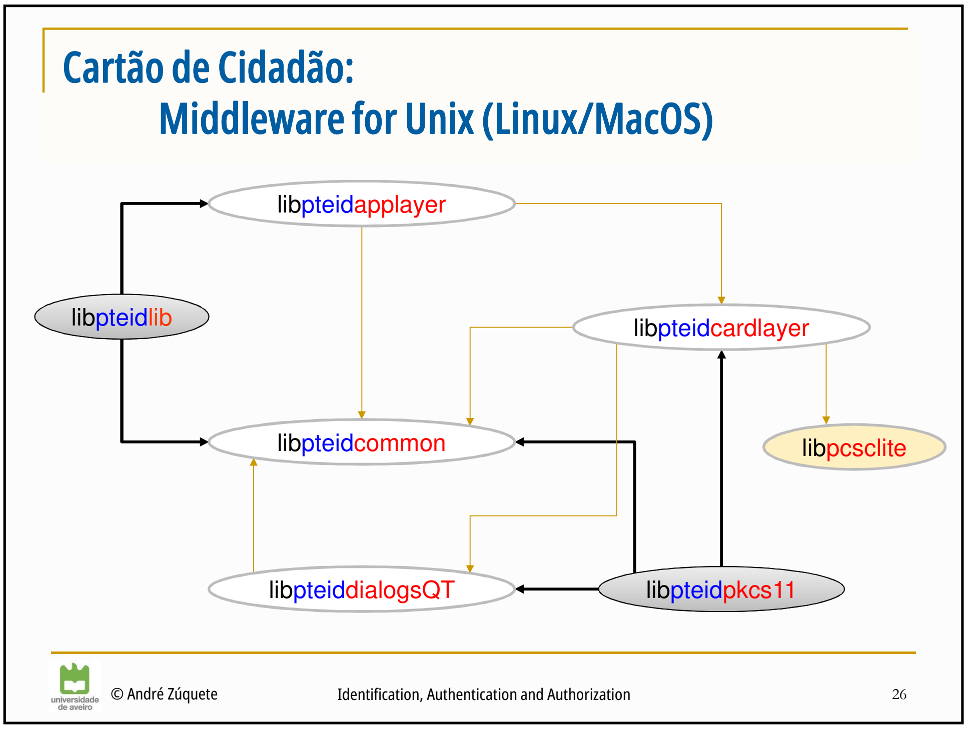
- R/O public session
  - Read-only access to public token objects
  - Read/write access to public session objects
- R/O user functions
  - Read-only access to all token objects (public or private)
  - Read/write access to all session objects (public or private)



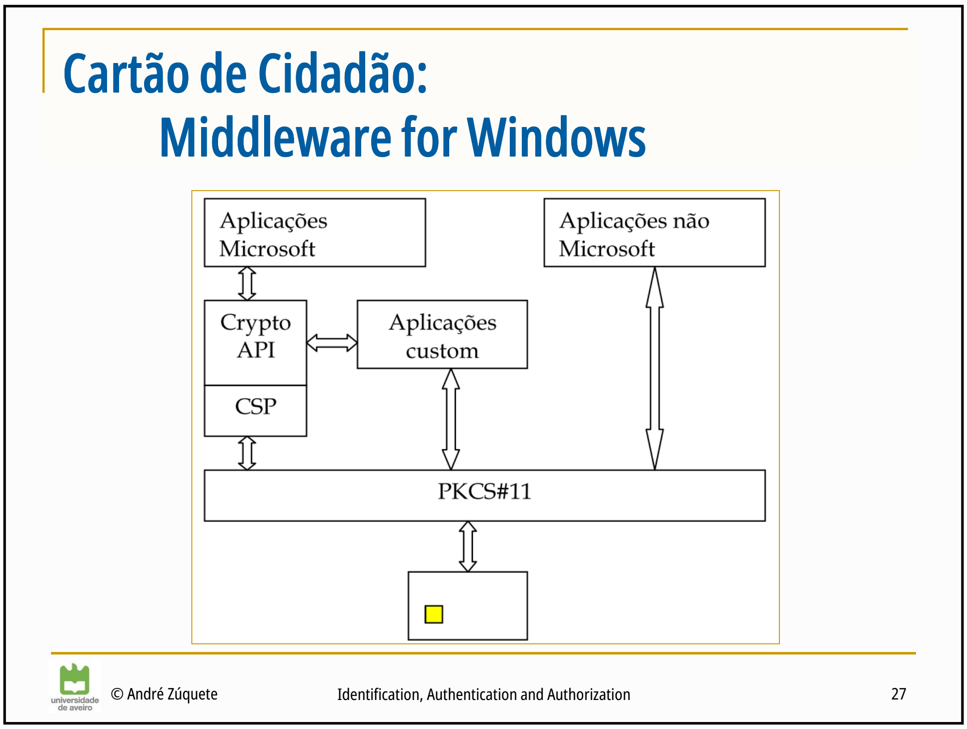
PKCS #11: Cryptoki R/W sessions login/logout

R/W SO Functions
Open Session
Close Session/ Device Removed
Login SO
Logout
Open Session
R/W Public Session
Close Session/
Device Removed
Login User
Logout
Open Session
Close Session/ Device Removed
R/W User Functions

- R/W public session
  - Read/write access to all public objects
- R/W SO functions
  - Read/write access only to public objects on the token
    - Not to private objects
  - The SO can set the normal user’s PIN
- R/W user functions
  - Read/write access to all objects



Cartão de Cidadão: Middleware for Unix (Linux/MacOS)



Cartão de Cidadão: Middleware for Windows