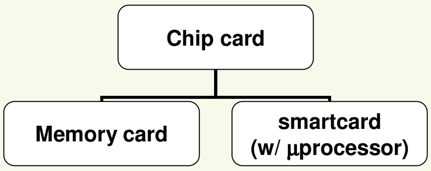
Smartcards

Smartcard: Definition

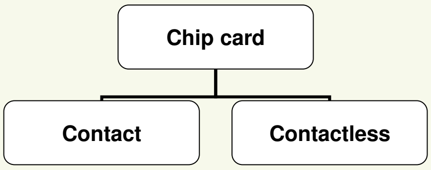
- Card with computing processing capabilities
  - CPU
  - ROM
  - EEPROM
  - RAM
- Interface
  - With contact
  - Contactless



Chip card

Memory card

smartcard (w/ µprocessor)



Chip card

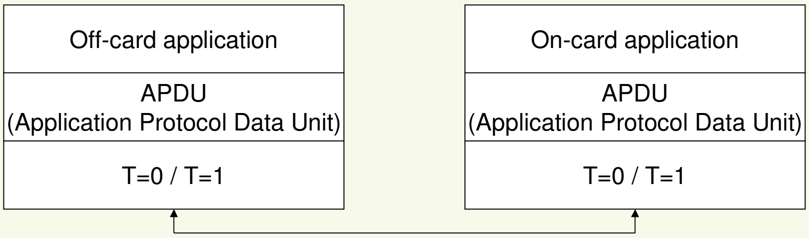
Contact

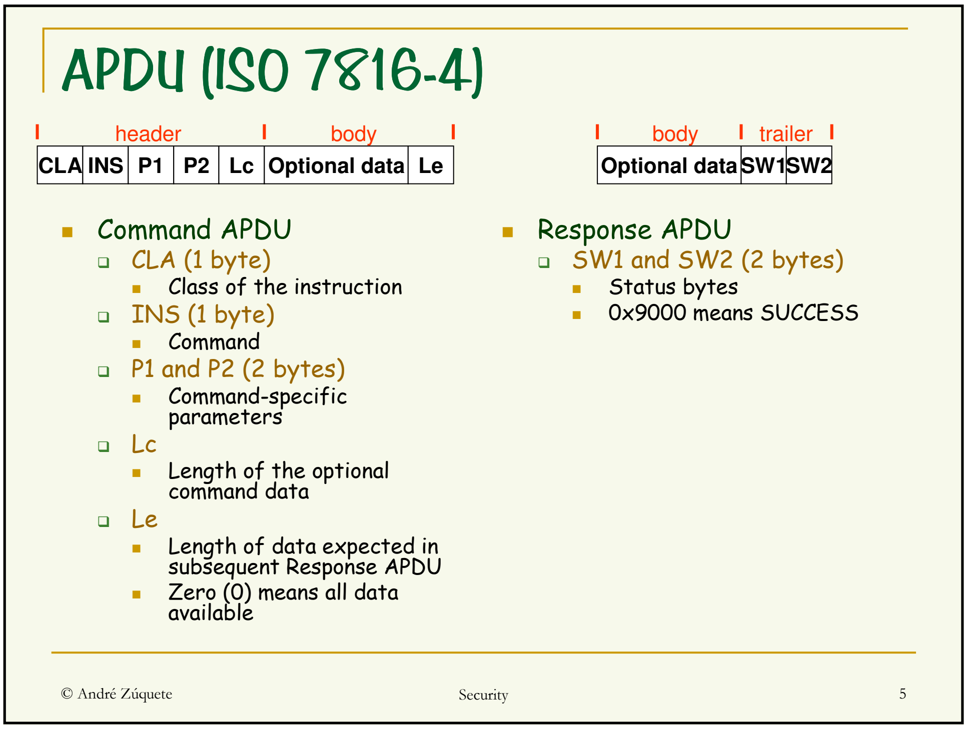
Contactless

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-effect attacks

Smartcard applications: Communication protocol stack



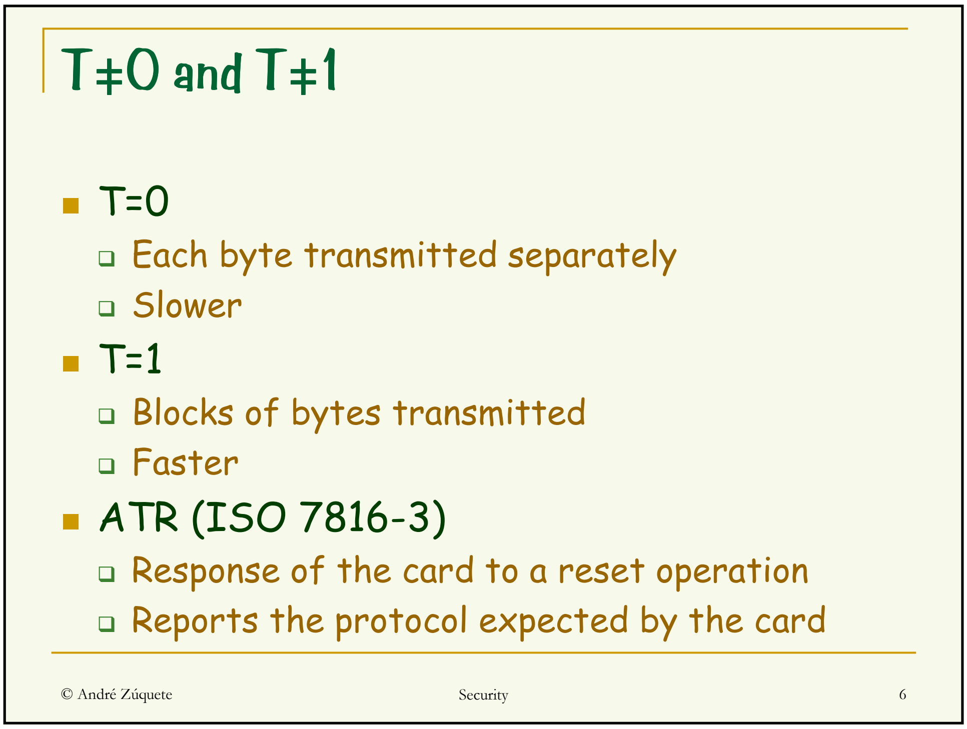


APDU (ISO 7816-4)

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



T‡0 and T‡1

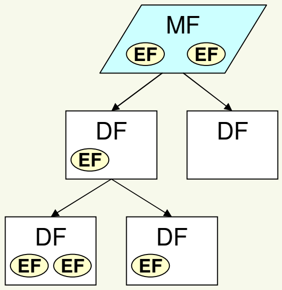
- T=0
  - Each byte transmitted separately
  - Slower
- T=1
  - Blocks of bytes transmitted
  - Faster
- ATR (ISO 7816-3)
  - Response of the card to a reset operation
  - Reports the protocol expected by the card

Encoding objects in smartcards: TLV and ASN.1 BER

- Tag-Length-Value (TLV)
  - Object description with a tag value, the length of its contents and the contents
  - Each element of TLV is encoded according with ASN.1 BER
- Values can contain other TLV objects
  - The structure can be recursive

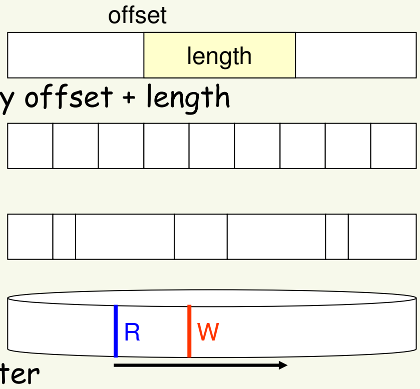
Smartcard: File system (1/3)

- File identification
  - Name or number
- File types
  - Master File (MF)
    - File system root, ID 0x3F00
  - Elementary File (EF)
    - Ordinary data file
    - File size fixed and determined when created
  - Dedicated File (DF)
    - Similar to a directory
    - Can contain other EFs or DF



Smartcard:
File system (2/3)

- File system types
  - Transparent
    - Data blocks identified by offset + length
  - Fixed records
    - Indexed records
  - Variable records
    - Indexed records
  - Cyclic
    - Read pointer, write pointer
    - Cyclic increments

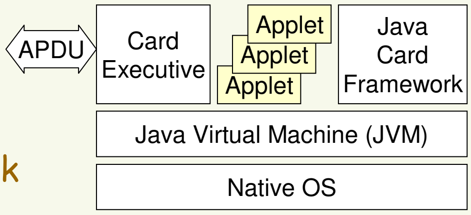


Smartcard:
File system (3/3)

- Access control
  - No restrictions
  - Protected
    - The file access APDU must contain a MAC computed with a key shared between the card and the off-card application
  - External authentication
    - The file access APDU is only allowed if the card already checked the existence of a common shared key with the off-card application

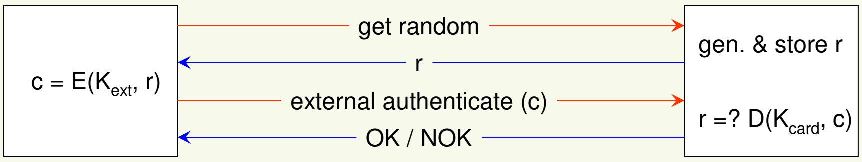
Java cards

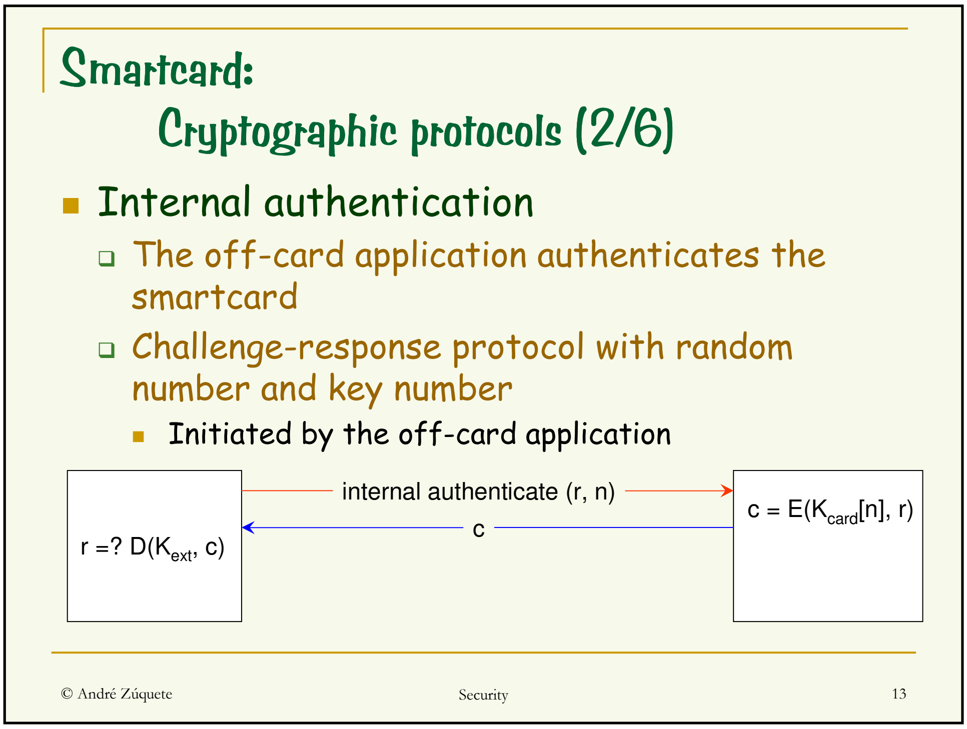
- Smartcards that run Java Applets
  - That use the JCRE
  - The JCRE runs on top of a native OS
- JCRE (Java Card Runtime Environment)
  - Java Virtual Machine
  - Card Executive
    - Card management
    - Communications
  - Java Card Framework
    - Library functions



Smartcard: Cryptographic protocols (1/6)

- External authentication
  - The smartcard authenticates the off-card application
  - Challenge-response protocol with random number
    - Initiated by the off-card application





Smartcard: Cryptographic protocols (2/6)

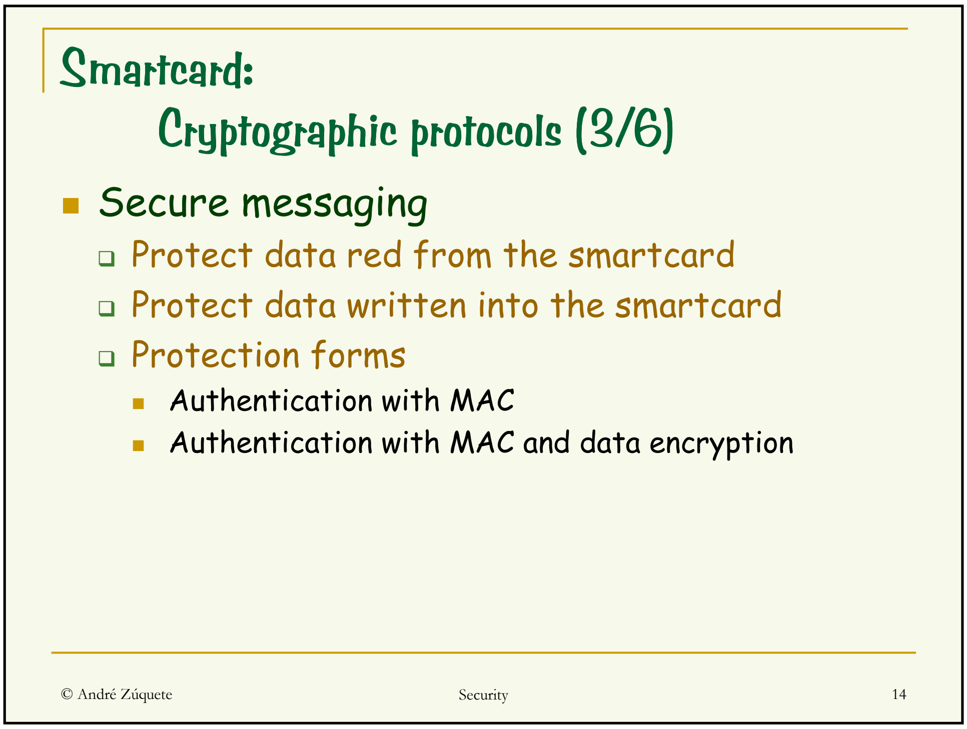
- Internal authentication
  - The off-card application authenticates the smartcard
  - Challenge-response protocol with random number and key number
    - Initiated by the off-card application

internal authenticate (r, n)

$c = E(K_{card}[n], r)$

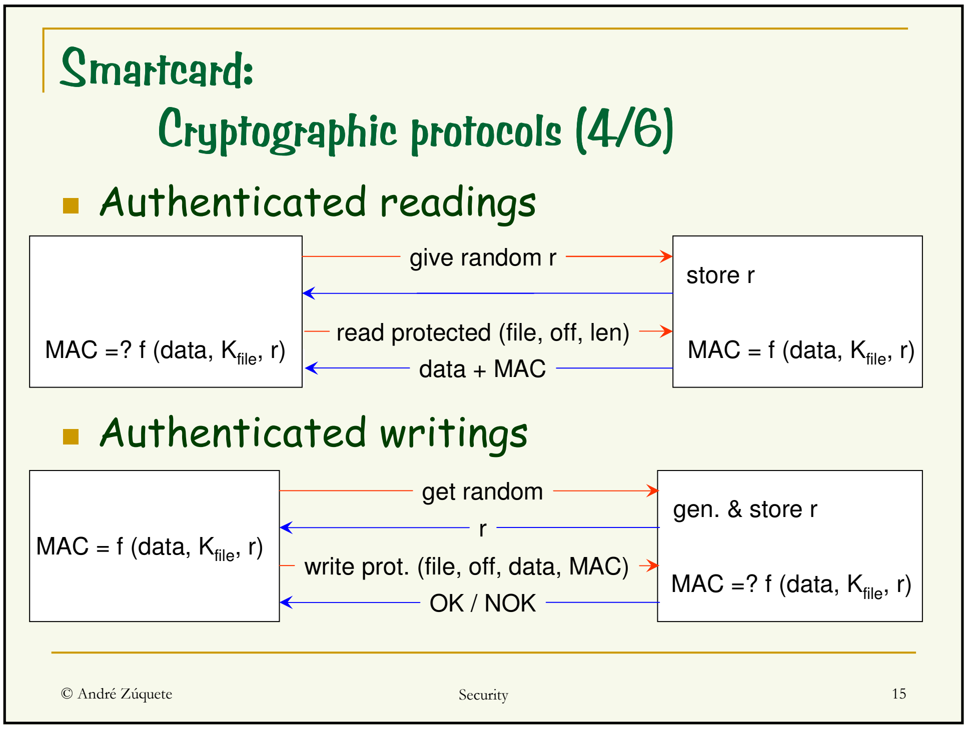
c

$r =? D(K_{ext}, c)$



Smartcard: Cryptographic protocols (3/6)

- Secure messaging
  - Protect data red from the smartcard
  - Protect data written into the smartcard
  - Protection forms
    - Authentication with MAC
    - Authentication with MAC and data encryption



Smartcard: Cryptographic protocols (4/6)

- Authenticated readings

MAC =? f (data, K_{file}, r)

give random r →

store r

←

read protected (file, off, len) →

← data + MAC

MAC = f (data, K_{file}, r)

- Authenticated writings

MAC = f (data, K_{file}, r)

get random →

gen. & store r

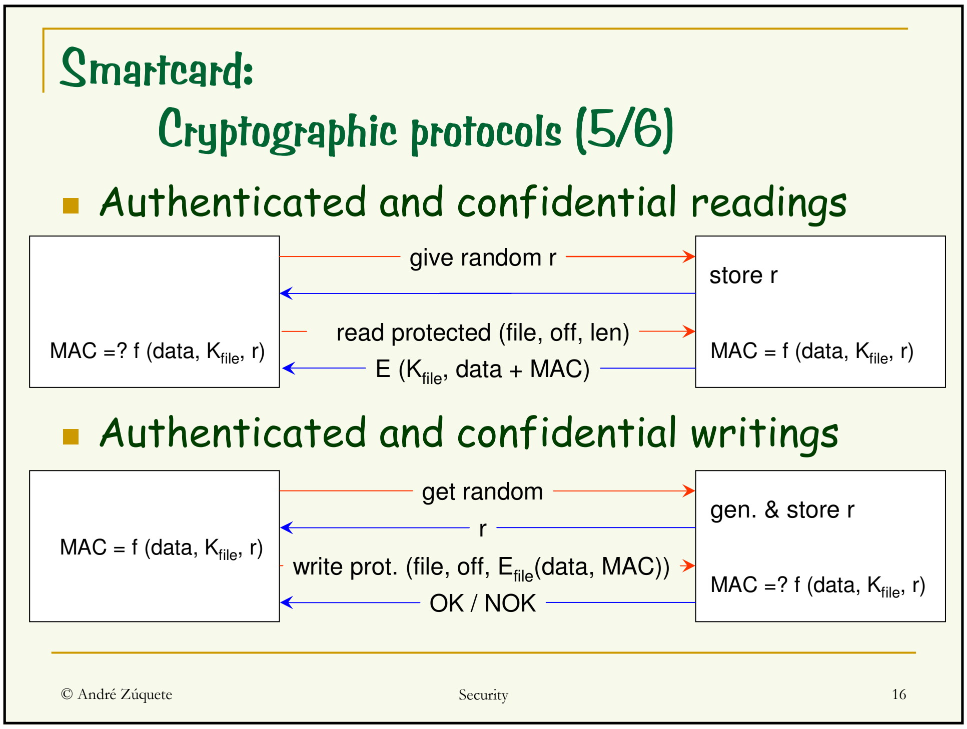
← r

write prot. (file, off, data, MAC) →

← OK / NOK

MAC =? f (data, K_{file}, r)

© André Zúquete Security 15



Smartcard: Cryptographic protocols (5/6)

- Authenticated and confidential readings

MAC =? f (data, K_{file}, r)

give random r →

store r

←

read protected (file, off, len) →

← E (K_{file}, data + MAC)

MAC = f (data, K_{file}, r)

- Authenticated and confidential writings

MAC = f (data, K_{file}, r)

get random →

gen. & store r

← r

write prot. (file, off, E_{file}(data, MAC)) →

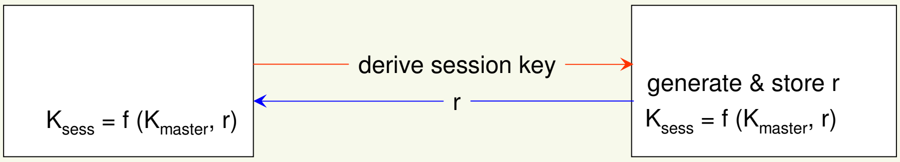
← OK / NOK

MAC =? f (data, K_{file}, r)

© André Zúquete Security 16

Smartcard: Cryptographic protocols (6/6)

- Session key derivation



derive session key

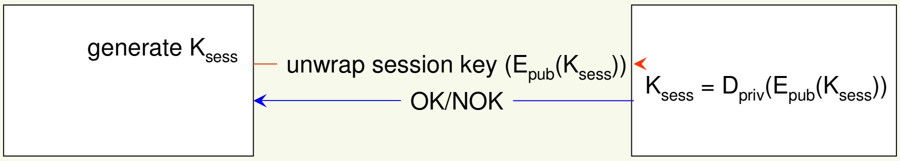
r

generate & store r

$K_{sess} = f\ (K_{master}, r)$

$K_{sess} = f\ (K_{master}, r)$

- Session key uploading



generate K_{sess}

unwrap session key $(E_{pub}(K_{sess}))$

OK/NOK

$K_{sess} = D_{priv}(E_{pub}(K_{sess}))$

OpenCard Framework (OCF)

- Goal: facilitate the development of smartcard-based solutions
  - Make the parts of the solution, typically provided by different parties, independent of each other
- Parties:
  - Card issuer
    - Card initialization, personalization and issuing
  - Card OS provider
    - Basic, lowest level card behavior
  - Card reader / terminal provider
    - Interfaces that deal with reading from and writing into cards
  - Application / service provider
    - Development of off-card (and possibly on-card) applications

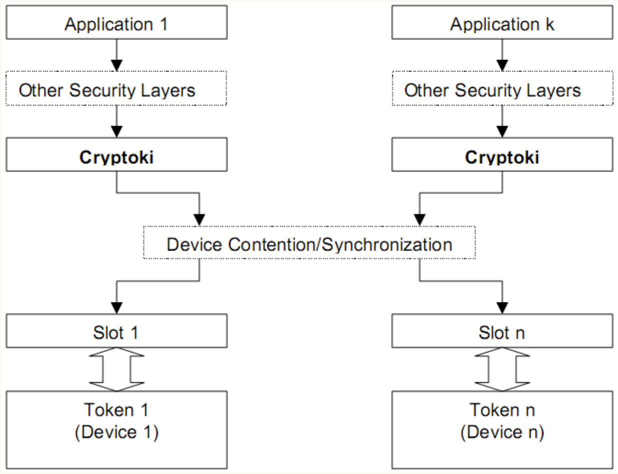
Cryptographic services

- Symmetric and asymmetric ciphers
- Key generation
- Key management
  - Key import
  - Key export
- Digital signatures
  - Generation
  - Verification
- Digest functions
- 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

PKCS #11: Cryptoki middleware integration



Application 1

Other Security Layers

Cryptoki

Application k

Other Security Layers

Cryptoki

Device Contention/Synchronization

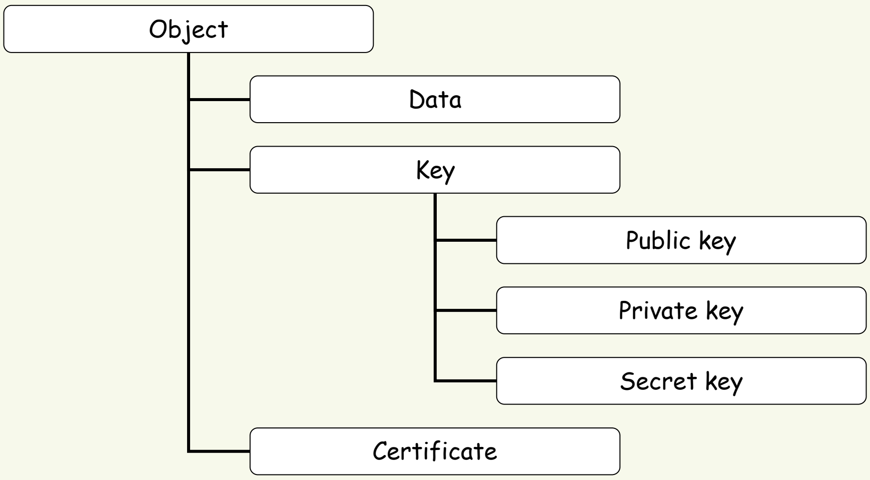
Slot 1

Token 1
(Device 1)

Slot n

Token n
(Device n)

PKCS #11: Cryptoki object hierarchy

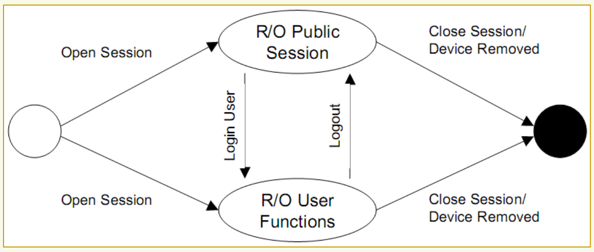


- Object
  - Data
  - Key
    - Public key
    - Private key
    - Secret key
  - Certificate

PKCS #11:
Cryptoki sessions

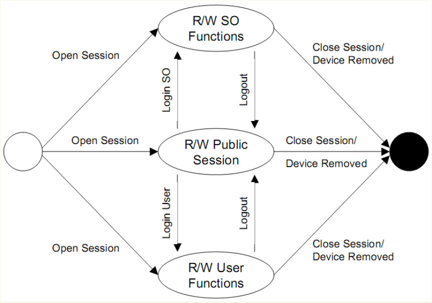
- Logical connections between applications and tokens
  - Read-only sessions
  - Read/write sessions
  - Session owners
    - Public
    - User
    - Security Officer (SO)
- Operations on open sessions
  - Administrative
    - Login/logout
  - Object management
    - Create / destroy an object on the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

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



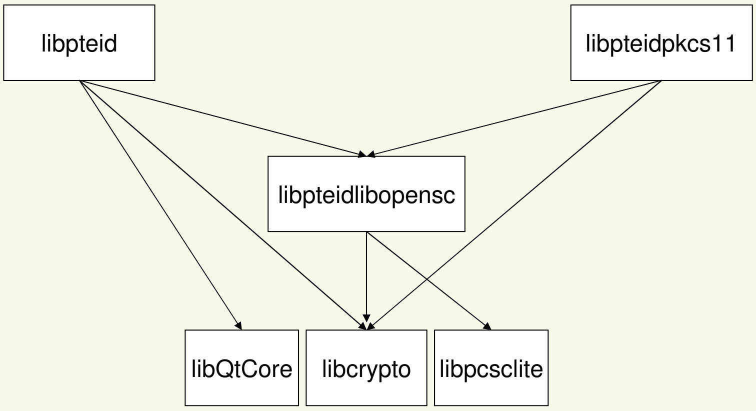
- R/O Public Session
  - Read-only access to public token objects
  - Read/write access to public session objects
- R/O User Functions
  - Read-only access to all token objects (public or private)
  - Read/write access to all session objects (public or private)

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

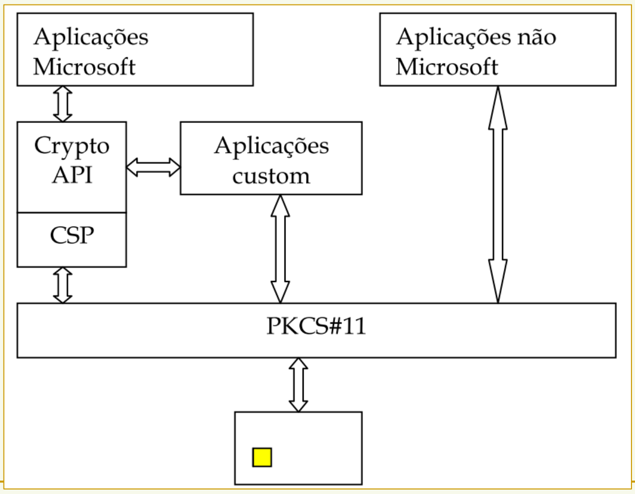


- R/W Public Session
  - Read/write access to all public objects
- R/W SO Functions
  - Read/write access only to public objects on the token
    - Not to private objects
  - The SO can set the normal user's PIN
- R/W User Functions
  - Read/write access to all objects

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



Cartão de Cidadão:
Middleware for Windows



Aplicações Microsoft

Aplicações não Microsoft

Crypto API

CSP

Aplicações custom

PKCS#11