Caso do Cartão do Cidadão

Henrique Domingos

Cartão de Cidadão

Cartão de identificação das dimensões de um cartão de crédito

Contém vários métodos de fornecer informação identidade

- Informática
  - Interação com o smartcard
- Visual, legível por humanos
  - Fotografia, números e nomes
- Visual, legível por dispositivos
  - MRZ (Machine Readable Zone)

Atributos visuais legíveis por humanos

Nome
- Sobrenome, Nome próprio, Pais

Atributos físicos
- Sexo e Altura

Outros
- Data de nascimento, nacionalidade
- Fotografia
- Assinatura caligráfica

Números
- Número de identificação Civil (e checksum)
- Num: Identificação Fiscal, Sistema Nacional de Saúde, Segurança Social
- Número do documento e validade

Versão do cartão

Atributos visuais legíveis por dispositivos

Nome
- Sobrenome, Nome próprio, Nomes adicionais
- Número de nomes

Atributos Físicos
- Sexo

Outros
- Data de nascimento e nacionalidade

Números
- Identificação Cívil (e checksum)
- Número do documento (e checksu
- Número de documentos emitidos

Validade

I<PRT000000000<<0<ZZ4<<<<<<<<2

8108108F1201158PRT<<<<<<<<<<<1

AVILA<<PAULA<ANDREIA<CONCEICAO

Atributos Informáticos

Todos os anteriores, excepto assinatura caligráfica

Morada

Template da impressão digital biométrica

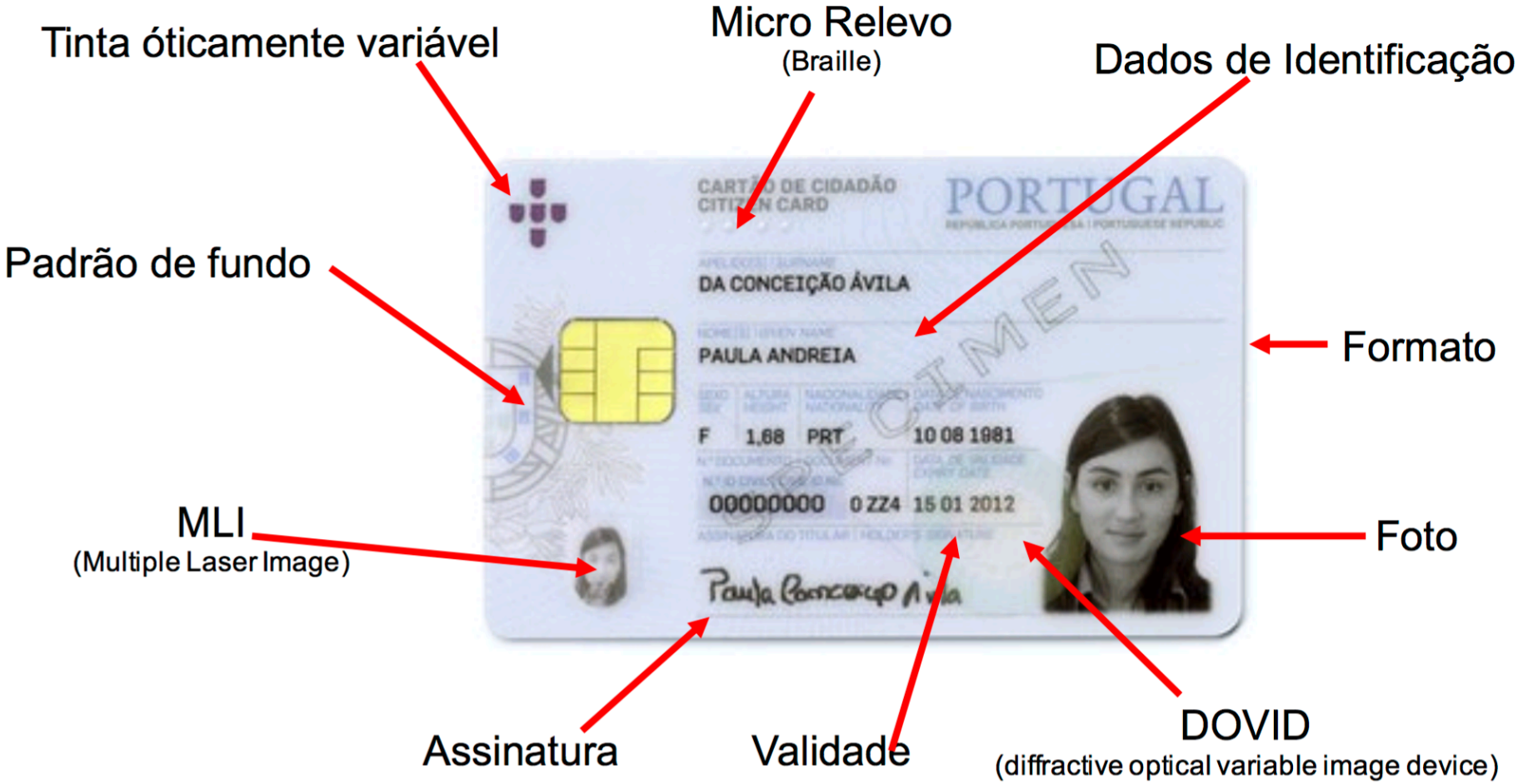
2 pares de chaves criptográficos (Assinatura e Autenticação)

7 certificados de chave pública
- 2 relativos às chaves do próprio
- 5 para indicar a cadeia de certificação

1 chave secreta, simétrica para EMV-CAP
- Europay, MasterCard, and Visa Chip Authentication Program

4 PINs

Atributos Visuais de Segurança



Proteção por PIN

Possuir o cartão é insuficiente para

- Obter morada
- Obter ou usar a chave privada de autenticação
- Obter ou usar a chave privada de assinatura
- Obter ou usar a chave secreta de EMV-CAP

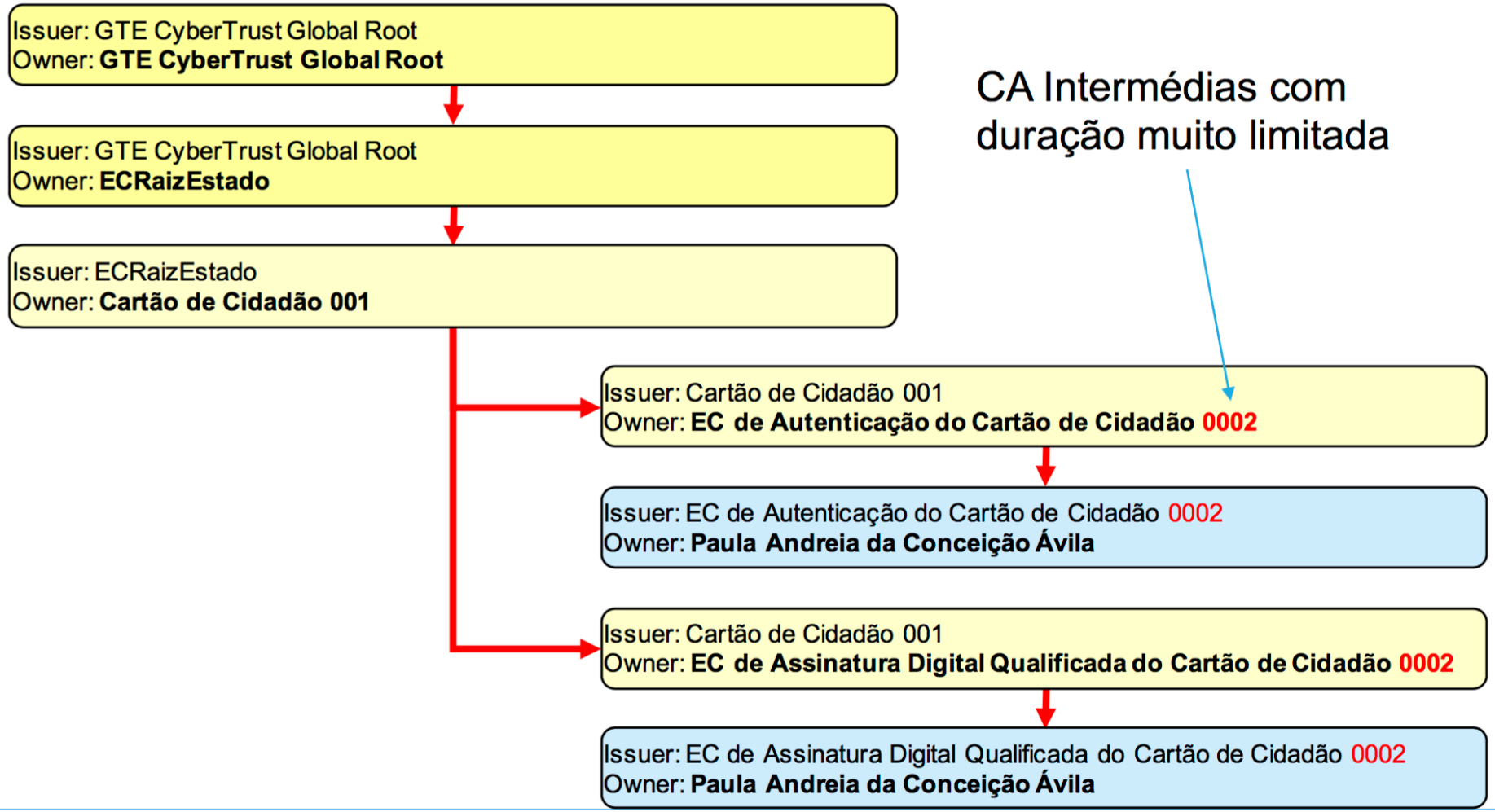
Operações protegidas por PIN

- PIN de 4 números
- PIN é bloqueado após 3 tentativas incorretas

Excepções

- Forças policiais podem obter a morada sem o PIN

Certificados no SmartCard



Certificados no SmartCard
Objectivos

Possibilita autenticar o dono do cartão

- O dono pode distribuir o seu certificado para outras pessoas/serviços que passar a poder verificar a sua identidade

Possibilita o dono autenticar outras pessoas com cartões semelhantes

- Cadeia de certificação presente no cartão

Possibilita o cartão autenticar clientes com certificados semelhantes

- Algumas operações podem ser pedidas ao cartão com certificados "especiais" que o cartão valida

Certificados no SmartCard: Interoperação com outras aplicações

Aplicações de *watchdog* detetam inserção e remoção

Inserção

- Aplicações obtêm certificados e inserem-nos nos repositórios dos navegadores
- Utilização das chaves respetivas é condicionada pelos PIN

Remoção

- Aplicações removem certificados dos repositórios dos navegadores

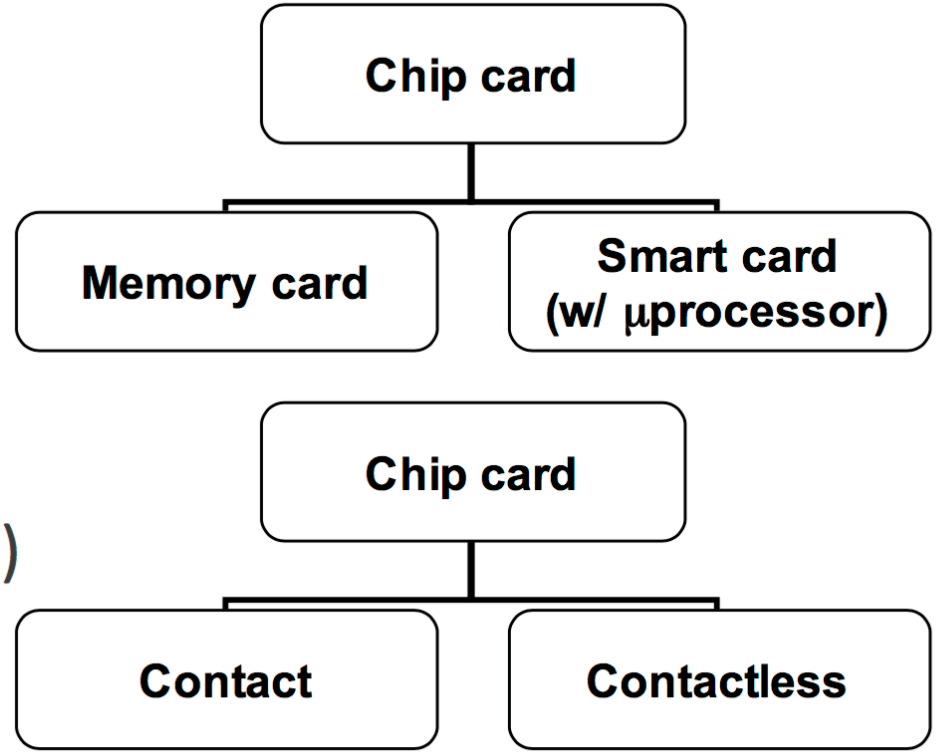
Smartcards: Definição

Cartão com capacidades de computação

- CPU
- ROM
- EEPROM
- RAM

Interface

- Com contactos
- Sem contactos (Contactless)



Smartcard: Componentes

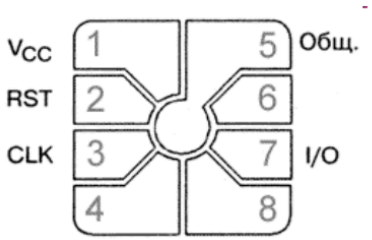
CPU
- 8/16 bit
- Crypto-coprocessor (opt.)

ROM
- Sistema Operativo
- Comunicação
- Algoritmos criptográficos

EEPROM
- Sistema de Ficheiros
  - Programas / applicações
  - Chaves/ passwords

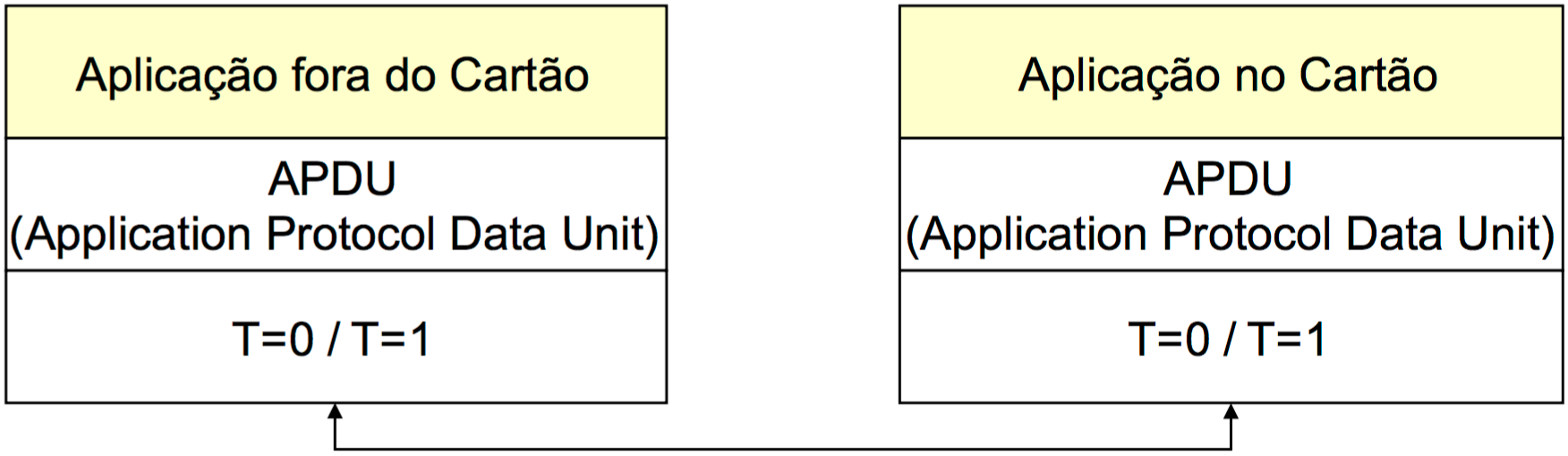
RAM
- Dados temporários
  - Apagados quando cartão é desligado

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



Segurança Física
- Resistente a acessos físicos diretos
- Resistente a ataques por canais paralelos

Aplicações em SmartCards: Pilha protocolar de comunicação



Aplicações em SmartCards: Aplicações no Cartão de Cidadão

IAS

- Autenticação e assinatura digital
- Utilização de pares de chaves assimétricas

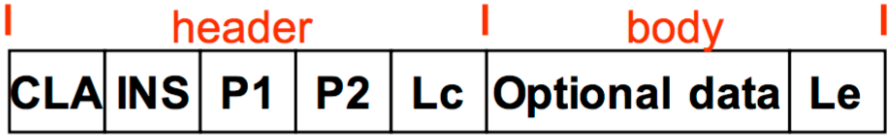
EMV-CAP

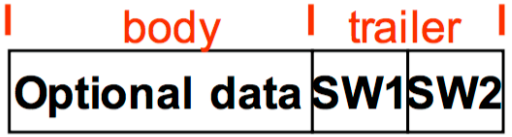
- Geração de one-time-passwords para canais alternativos (telefone, Fax, etc..)

Match-on-Card

- Validação de impressões digitais

Interação com o Smartcard: APDU (ISO 7816-4)





APDU de Comando

- CLA (1 octeto)
  - Classe da instrução
- INS (1 octeto)
  - Comando
- P1 e P2 (2 octetos)
  - Parâmetros específicos do comando
- Lc
  - Comprimento dos dados opcionais
- Le
  - Comprimento dos dados esperados na resposta
  - Zero (0) significa todos os dados disponíveis

APDU de Resposta

- SW1 e SW2 (2 octetos)
  - Octeto de estado
  - 0x9000 significa SUCESSO

Interação com o Smartcard: Protoclos de baixo-nível T=0 e T=1

T=0

- Enviado um octeto de cada vez
- Mais lento

T=1

- Octetos transmitidos em blocos
- Mais rápido

ATR (ISO 7816-3)

- Resposta à operação de RESET
- Reporta o protocolo esperado pelo cartão

Codificação de objetos nos smartcards: TLV e ASN.1 BER

Tag-Length-Value (TLV)

- Tag: Tipo de objeto
- Length: Tamanho do objeto
- Value: Dados do objeto

Cada TLV é codificado através das regras ASN.1 BER

- Abstract Syntax Notation, Basic Encoding Rules

Dados de um objeto podem conter outros TLV

- Estrutura recursiva

Permite ignorar objetos desconhecidos

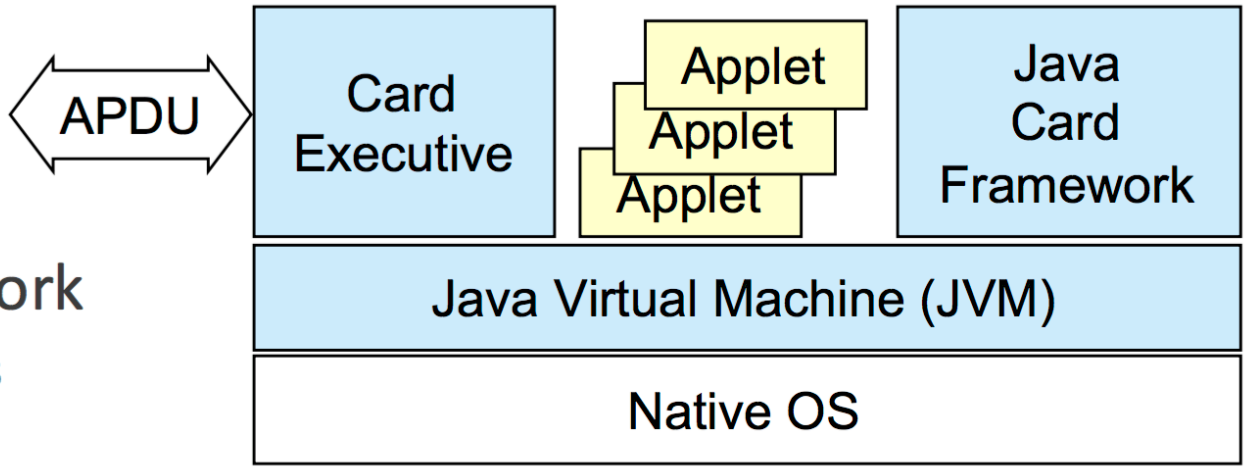
Modelo de computação do Smartcard Cartões Java

Smartcards executam Applets Java

- Utilizam o JCRE
- O JCRE executa no topo do SO nativo

JCRE (Java Card Runtime Environment)

- Java Virtual Machine
- Card Executive
  - Gestão do Cartão
  - Comunicações
- Java Card Framework
  - Bibliotecas de funções



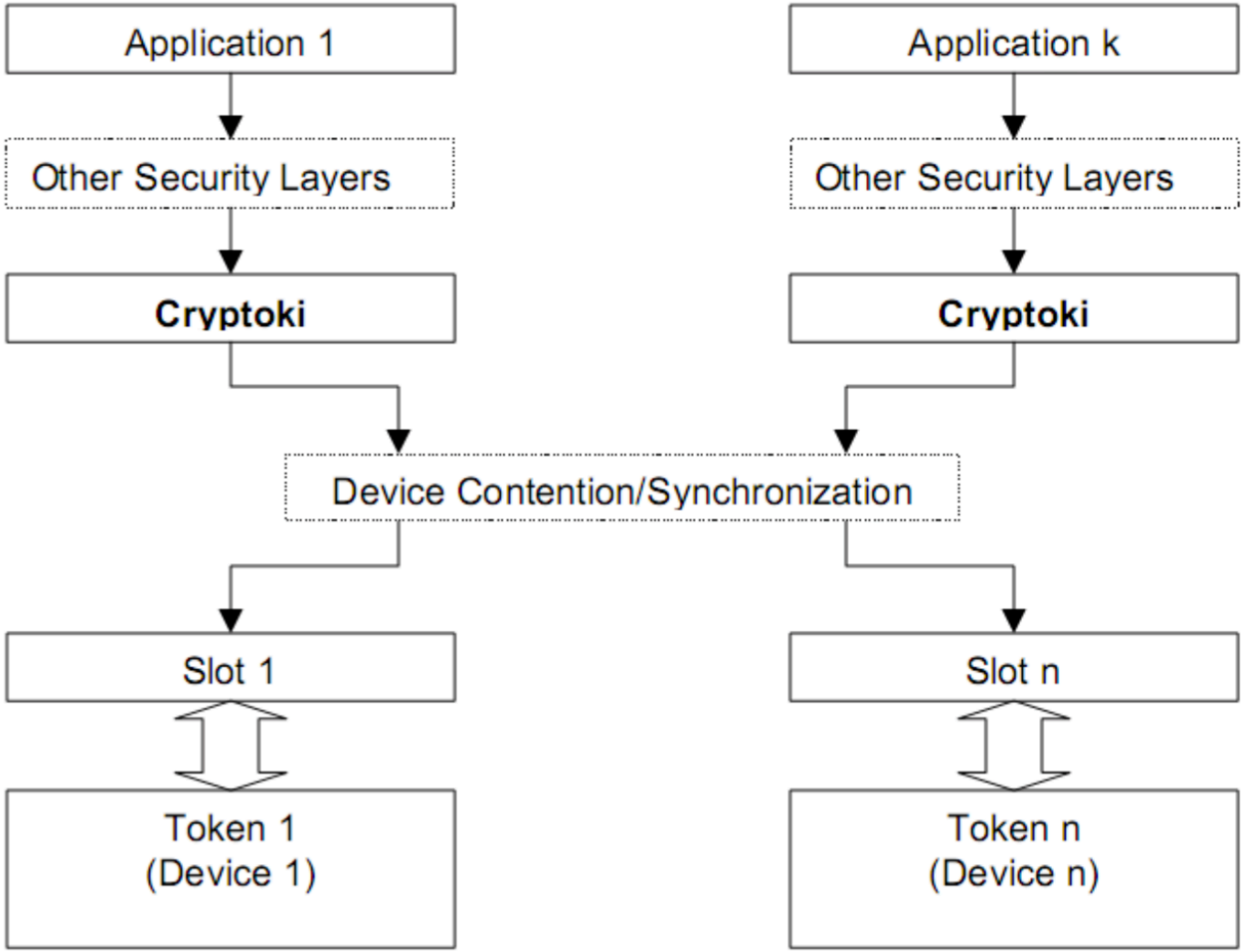
Serviços criptográficos do Smartcard: Middleware

Bibliotecas que servem de ponte entre as funcionalidades do SmartCard e as aplicações de mais alto nível

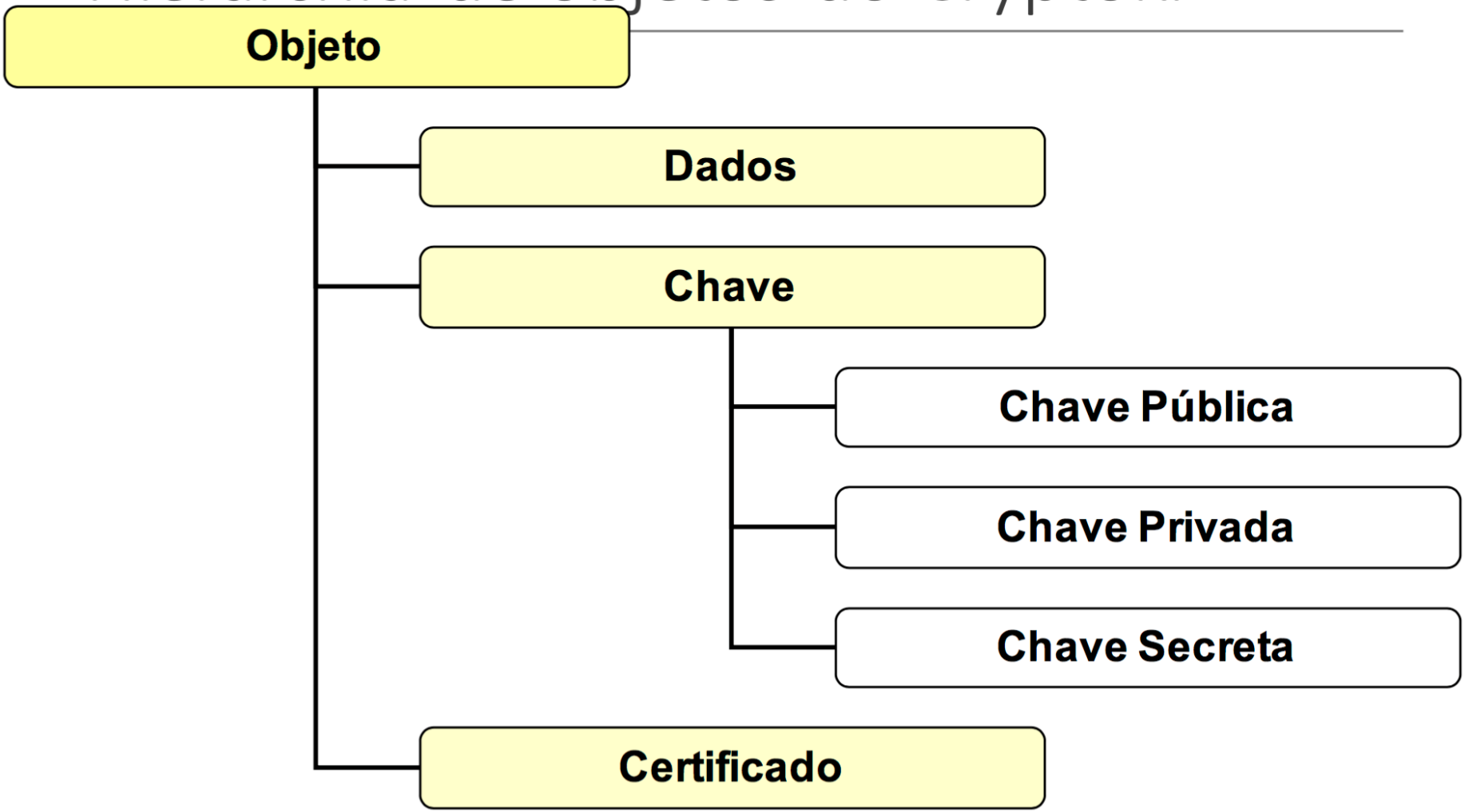
Baseado em soluções normalizadas:

- PKCS #11
  - Cryptographic Token Interface Standard (cryptoki)
  - Definido pela RSA Security Inc.
- PKCS #15
  - Cryptographic Token Information Format Standard
  - Definidopela RSA Security Inc.
- CAPI CSP
  - CryptoAPI Cryptographic Service Provider
  - Definido pela Microsoft para sistemas Windows
- PC/SC
  - Personal computer/Smart Card
  - Plataforma para acesso a smartcards em Windows e Linux

PKCS #11: Integração do Middleware Cryptoki



PKCS #11:
Hierarchia de objetos do Cryptoki



PKCS #11
Sessões do Cryptoki

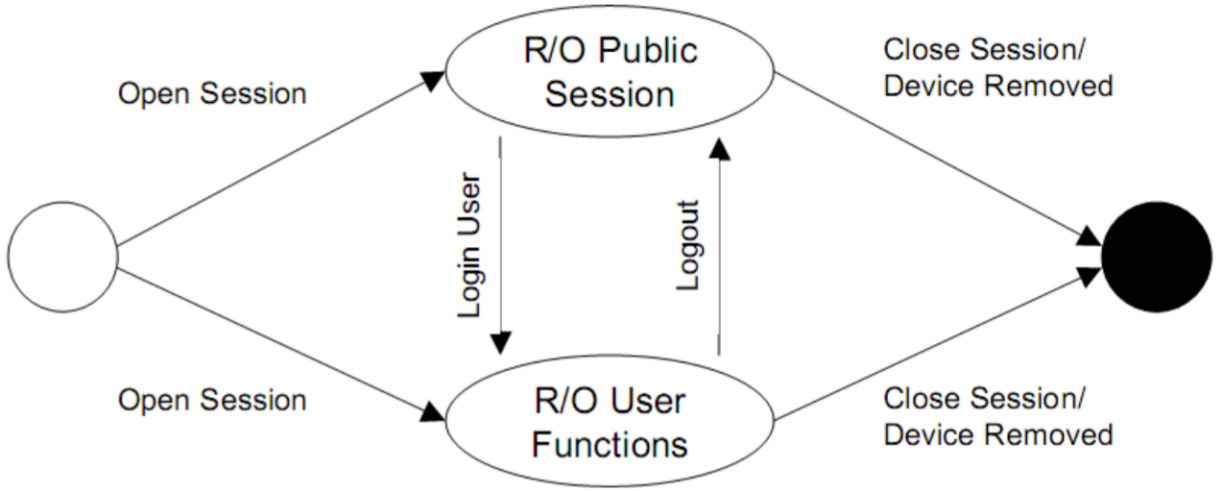
Ligações lógicas entre aplicações e cartões (tokens)
- Sessões de leitura
- Sessões de leitura e escrita

Operações em sessões ativas
- Administrativas
  - Login/logout
- Gestão de objetos
  - Criar ou destruir um objeto no cartão
- Criptográficas

Objetos de sessão
- Objetos temporários criado (e válidos) durante a sessão

Tempo de vida das sessões
- Normalmente apenas para uma única operação

PKCS #11:
Cryptoki Sessões de Leitura



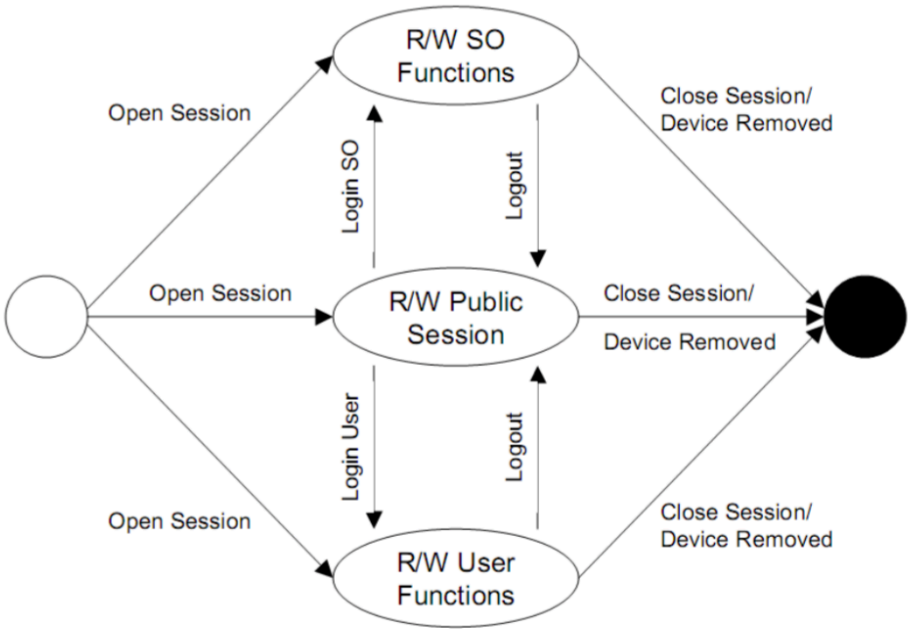
Sessão pública de Leitura

- Acesso de leitura aos objetos públicos
- Acesso de leitura/escrita aos objetos de sessão públicos

Funções de leitura do utilizador

- Acesso de leitura a todos os objetos do cartão (públicos ou privados)
- Acesso de leitura/escrita a todos os objetos de sessão (públicos ou privados)

PKCS #11: Cryptoki Sessões de leitura e escrita



Sessão pública e Leitura e Escrita

- Ler e escrever todos os objetos públicos

Funções do SO de Leitura e Escrita

- Ler/escrever objetos públicos
  - Não os objetos privados
- O SO pode definir o PIN dos utilizadores
- SO = Security Officer

Funções do utilizador de Leitura e Escrita

- Ler e escrever todos os objetos

PKCS #11: Conceitos utilizados pelo CC

PIN de Autenticação

- PIN do utilizador no PKCS #11

PIN de Assinatura

- Não exposto pelo interface PKCS #11

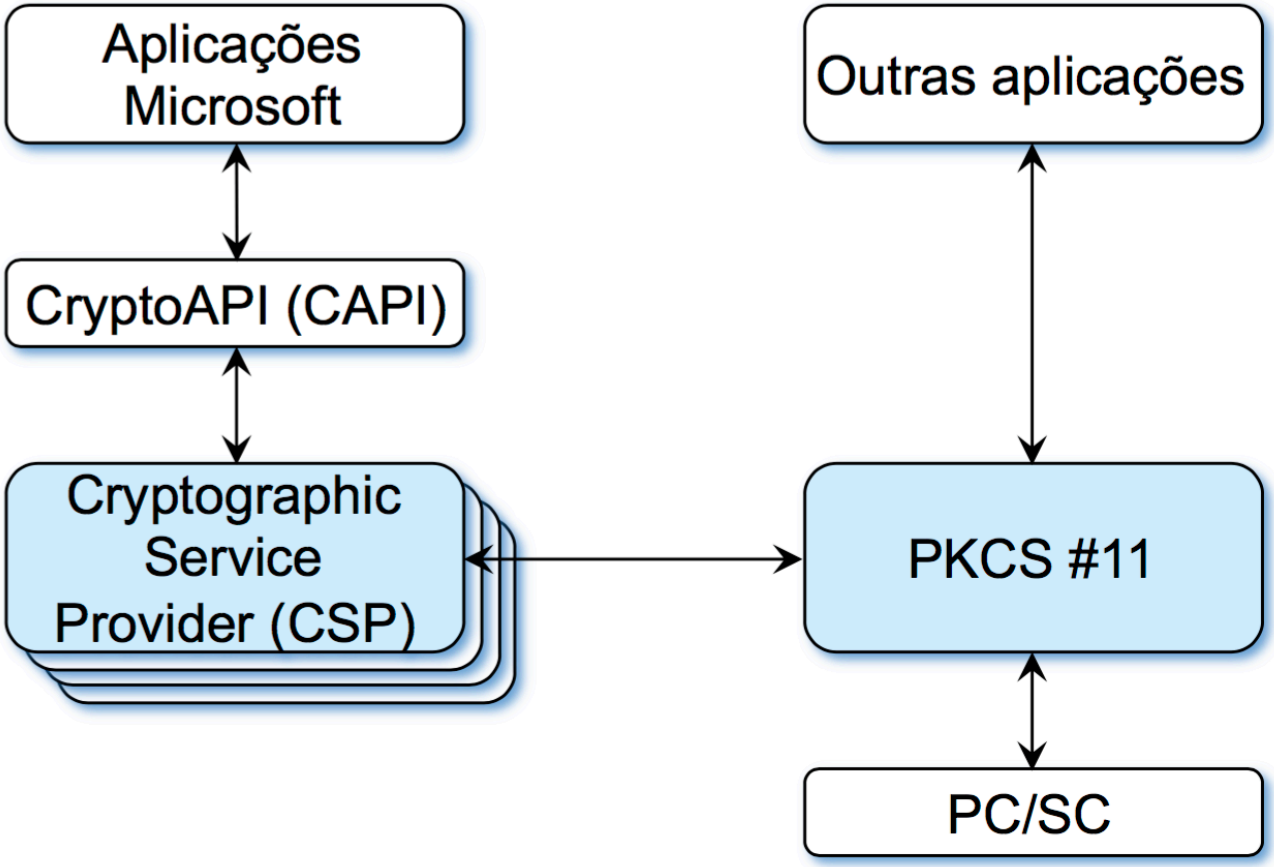
PIN de Morada

- Não exposto pelo interface PKCS #11

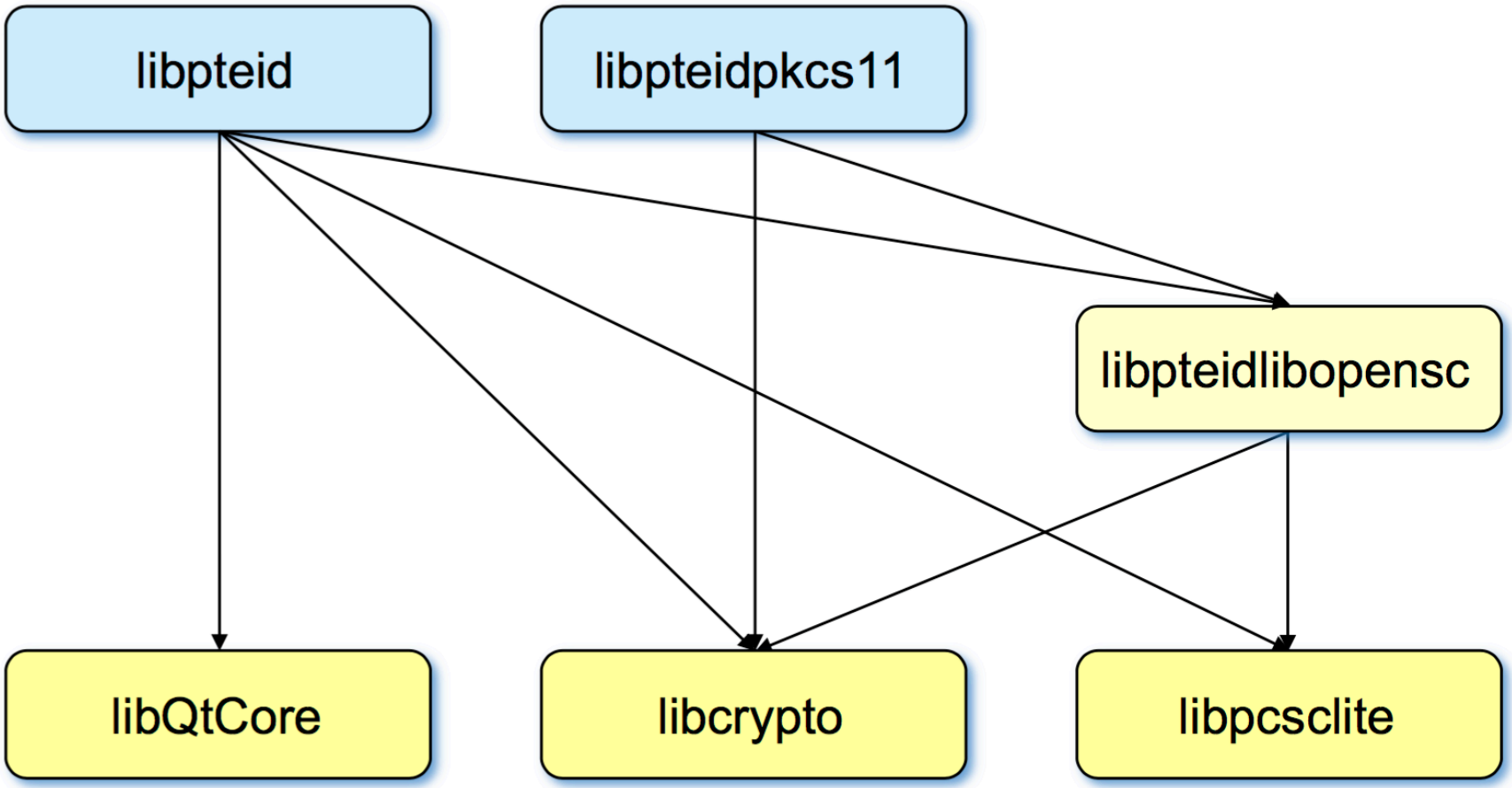
PKCS #11 SO PIN

- Not used by owners

Cartão de Cidadão: Middleware PTEID para Windows



Cartão de Cidadão: Middleware PTEID para Unix



Cartão de Cidadão: PTEID middleware & SDK

Distribuição pública

- Windows
- MAC OS X Yosemite
- Linux
  - Caixa Mágica, Fedora, OpenSuse, Red Hat, Ubuntu

Linguagens

- Bibliotecas dinâmicas para C/C++
- Wrapper Java (JNI) para as bibliotecas C/C++
- Wrapper C# .NET para as bibliotecas C/C++

Manuais

- 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
- Outros

Cartão de Cidadão: Serviços da PKI

Certificados Emitidos

- LDAP e Web

Certificados revogados

- OCSP, delta-CRL e serviços CRL