Segurança Informática e nas Organizações

Resumos
2016/2017

João Alegria | 68661

Capítulo 5

Cartão de Cidadão

O cartão de cidadão é um *smartcard*, porque possui um microcomputador embebido (*chip*).

Funcionalidades

• ***Guardar informação pessoal*** - para validação informática interna da identidade do titular. Concretamente, esta informação é constituída por elementos descritivos de impressões digitais do titular.

• ***Guardar informação privada*** - informação que o titular pode usar, mas não conhecer ou divulgar. Concretamente, esta informação é constituída por três chaves criptográficas:

-Uma chave simétrica de autenticação do titular

-Uma chave privada de um par de chaves assimétricas RSA, que serve para autenticar o titular.

-Uma chave privada de um par de chaves assimétricas RSA, que serve para produzir assinaturas digitais do titular

• ***Guardar informação reservada*** - informação que o titular conhece mas que apenas disponibiliza de forma fidedigna, via *smartcard* - morada do titular.

• ***Guardar informação pública de grande dimensão, não memorizável*** - esta informação é constituída pela fotografia do titular e por certificados X.509v3 de chaves públicas do titular, chaves essas que podem ser usadas para autenticar o titular ou a sua assinatura.

• ***Guardar informação observável no CC*** - fotografia, nome, data nascimento, diversos números de identificação, validade do cartão

• ***Efetuar operações criptográficas usando as chaves que fazem parte da sua informação privada***

Atributos informáticos

Morada	**Template de impressão digital biométrica**	**2 pares de chaves criptográficos (Assinatura e Autenticação)**	**7 certificados de chave pública**	**1 chave secreta, simétrica para EMV-CAP**	**4 PIN**
			- 2 relativos às chaves do próprio - 5 para indicar a cadeia de certificação	*Europay, MasterCard, and Visa Chip Authenticantion Program*	

Proteção por PIN

- **Possuir o cartão é insuficiente para**
  - Obter morada
  - Obter / usar a chave privada de autenticação
  - Obter / usar a chave privada de assinatura
  - Obter / usar a chave secreta da EMV-CAP

- **Operações protegidas por PIN**
  - PIN de 4 números
  - PIN é bloqueado após 3 tentativas incorretas

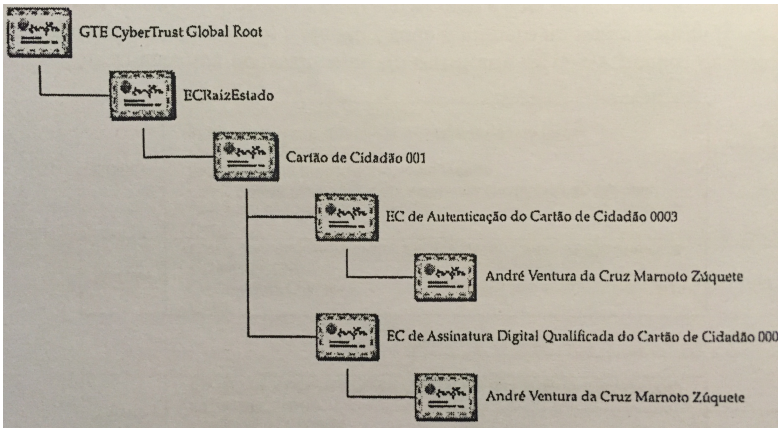
- **Exceções**
  - Forças policiais podem obter a morada sem o PIN

Assinaturas digitais com o Cartão Cidadão

O Cartão de Cidadão possui um par de chaves assimétricas de assinatura digital qualificada, para assinar documentos. O *smartcard* possui e disponibiliza um certificado X.509v3 com a chave pública de validação da assinatura digital qualificada do titular.

- **Como ativar a assinatura digital**
  - Através da publicação de um certificado de revogação, na CRL da sua EC, das credenciais de assinatura digital presentes no *smartcard*.
- **CC tem 2 pares de chaves criptográficos (autenticação e assinatura)**

Hierarquias de certificação no Cartão Cidadão



7 certificados de chave pública: 2 relativas às chaves do próprio, 5 para indicar a cadeia de certificação

Certificados no *SmartCard*: Objetivos

- **Possibilita autenticar o dono do cartão**
  - O dono pode distribuir o seu certificado para outras pessoas/serviços que passa 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

Smartcards

Cartão com capacidade de computação.

Componentes

CPU	ROM	EEPROM
•8/16 bit •Crypto-coprocessor	•Sistema Operativo •Comunicação •Algoritmos criptográficos	•Sistema de Ficheiros - programas / aplicações - chaves / passwords
RAM	**Contactos Mecânicos**	**Segurança Física**
•Dados temporários - apagados quando cartão é desligado	•ISO 7816-2 - power ; soft reset ; clock ; half duplex I/O	•Resistente a acessos físicos diretos •Resistente a ataques por canais paralelos

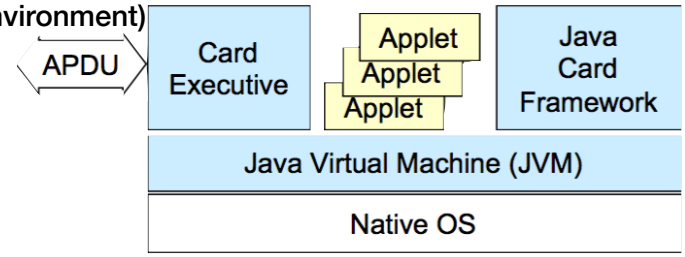
Aplicações em *SmartCards*: Exemplo Cartão Cidadão

IAS	EMV-CAP	Match-on-Card
•Autenticação e assinatura digital •Utilização de pares de chave assimétricas	•Geração de one-time-password para canais alternativos (telefone, fax, etc)	•Validação de impressões digitais

Modelo de computação do *Smartcard*: Cartões Java

- **Smartcards executem 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

Para fazer a ponte entre uma aplicação e um conjunto alargado de *smartcards* é preciso que exista um middleware que permita usar diversos tipos de *smartcards* e que as aplicações estejam preparadas para utilizar esses middleware.

- **No caso do Cartão de Cidadão:**
  - Existem dois tipos de middleware:
  1. pteidpkcs11 - é o que permite usar o Cartão de Cidadão como um dispositivo criptográfico. São disponibilizadas bibliotecas PKCS #11 com um subconjunto da interface Cryptoki
  2. pteidlib - permite realizar operações com o Cartão de Cidadão que são específicas da sua natureza de documento de identificação e que não têm paralelo nos dispositivos criptográficos.