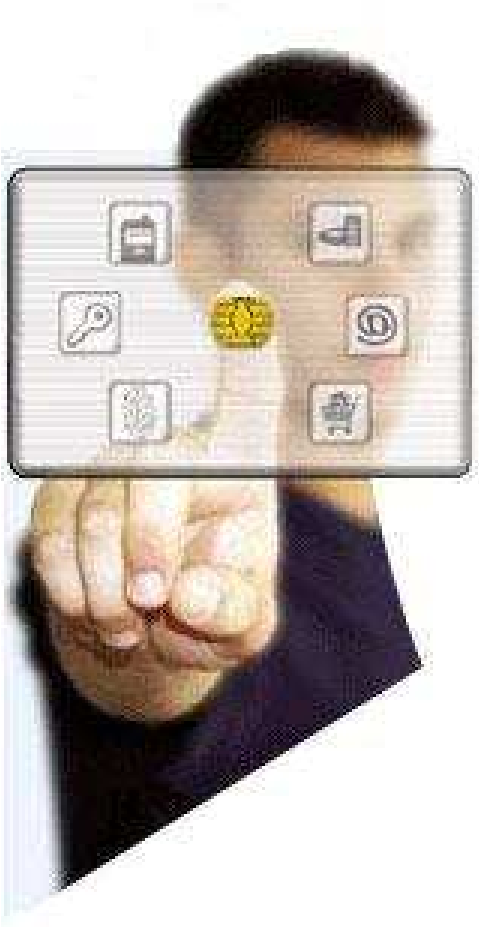
DOCUMENTOS E DINHEIRO ELETRÔNICO COM *SMART CARDS* UTILIZANDO A TECNOLOGIA JAVA *CARD*

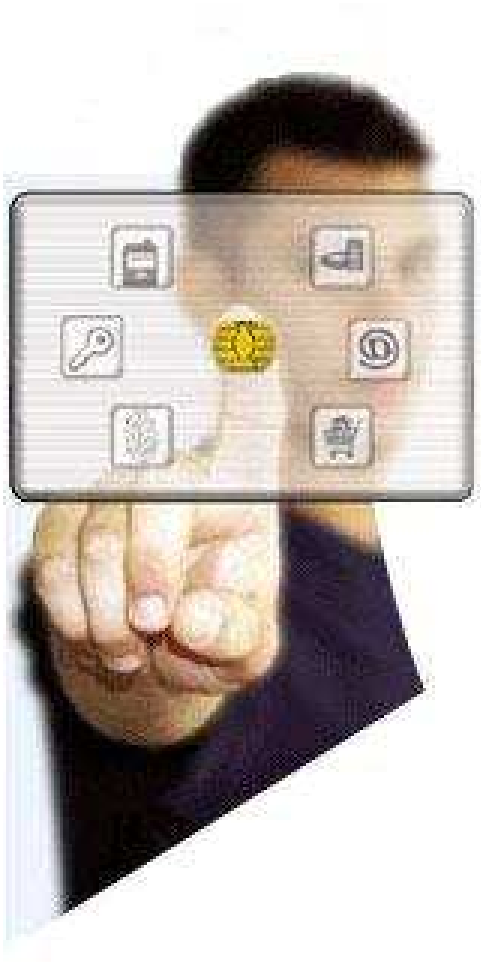


Cleber Giovanni Suavi

Orientador: Marcel Hugo

DOCUMENTOS E DINHEIRO ELETRÔNICO COM *SMART CARDS* UTILIZANDO A TECNOLOGIA JAVA *CARD*

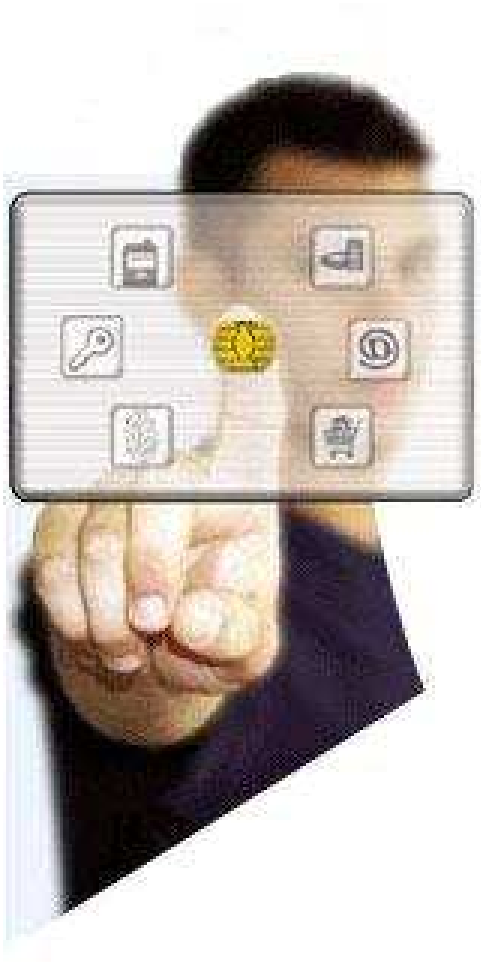
Roteiro



- ✓ **introdução**
  - ✓ objetivos
  - ✓ relevância
- ✓ **fundamentação teórica**
  - ✓ *smart cards*
  - ✓ tecnologia Java *card*
  - ✓ protocolo APDU
  - ✓ trabalhos correlatos
- ✓ **especificação**
  - ✓ requisitos do problema a ser trabalhado
  - ✓ técnicas e ferramentas utilizadas
  - ✓ diagramas de casos de uso
  - ✓ estrutura básica de um *applet*
  - ✓ diagramas de classes
- ✓ **desenvolvimento**
  - ✓ Java *Card Software Development Kit - SDK*
  - ✓ *Jcop Tools*
  - ✓ *hardware*
  - ✓ operacionalidade da implementação
- ✓ **considerações finais**
  - ✓ conclusões
  - ✓ extensões

DOCUMENTOS E DINHEIRO ELETRÔNICO COM *SMART CARDS* UTILIZANDO A TECNOLOGIA JAVA *CARD*

Roteiro



- ✓ **introdução**
  - ✓ objetivos
  - ✓ relevância
- ✓ **fundamentação teórica**
  - ✓ *smart cards*
  - ✓ tecnologia Java *card*
  - ✓ protocolo APDU
  - ✓ trabalhos correlatos
- ✓ **especificação**
  - ✓ requisitos do problema a ser trabalhado
  - ✓ técnicas e ferramentas utilizadas
  - ✓ diagramas de casos de uso
  - ✓ estrutura básica de um *applet*
  - ✓ diagramas de classes
- ✓ **desenvolvimento**
  - ✓ Java *Card Software Development Kit - SDK*
  - ✓ *Jcop Tools*
  - ✓ *hardware*
  - ✓ operacionalidade da implementação
- ✓ **considerações finais**
  - ✓ conclusões
  - ✓ extensões

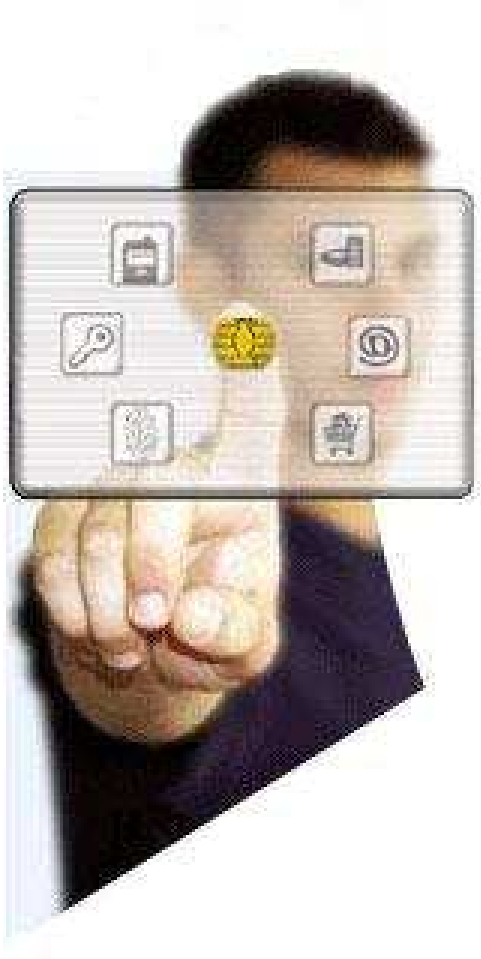
Introdução

- ✓ **antes do *smart card***
  - ✓ deve-se portar uma série de documentos:
    - ✓ CPF
    - ✓ Registro Geral
    - ✓ Título de Eleitor
    - ✓ CNH
    - ✓ etc, etc, etc...
    - ✓ dinheiro (cédulas e moedas)
- ✓ **depois do *smart card***
  - ✓ tudo em um só cartão: documentos e dinheiro
  - ✓ padronização

Objetivo principal

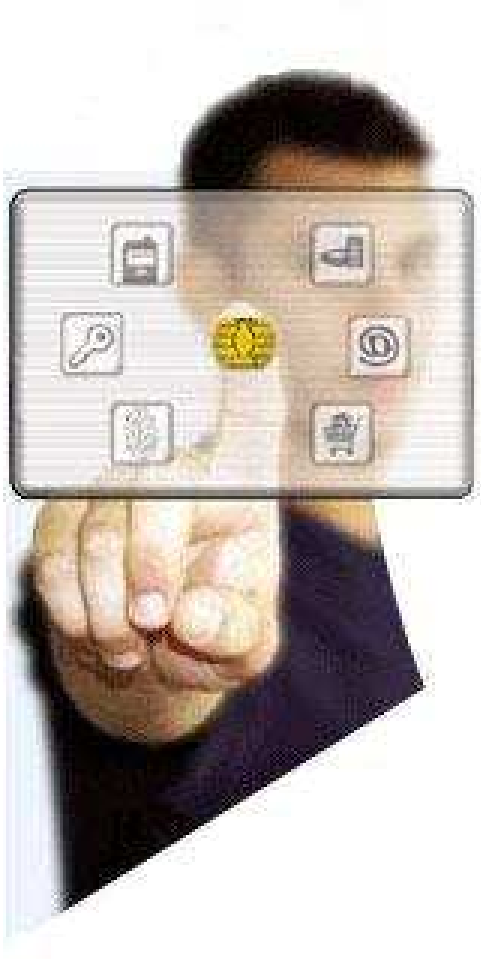
Desenvolvimento de *applets*, onde serão possíveis a utilização de dinheiro eletrônico e documentos pessoais, que poderão ser instalados e utilizados em *smart cards*

Objetivos específicos



- ✓ utilizar a tecnologia Java *card*
- ✓ documentos utilizados: Cadastro de Pessoa Física (CPF), Registro Geral (RG) e Título de Eleitor
- ✓ permitir débitos e créditos com relação ao dinheiro eletrônico
- ✓ permitir o armazenamento de um par de chaves assimétricas e um certificado digital

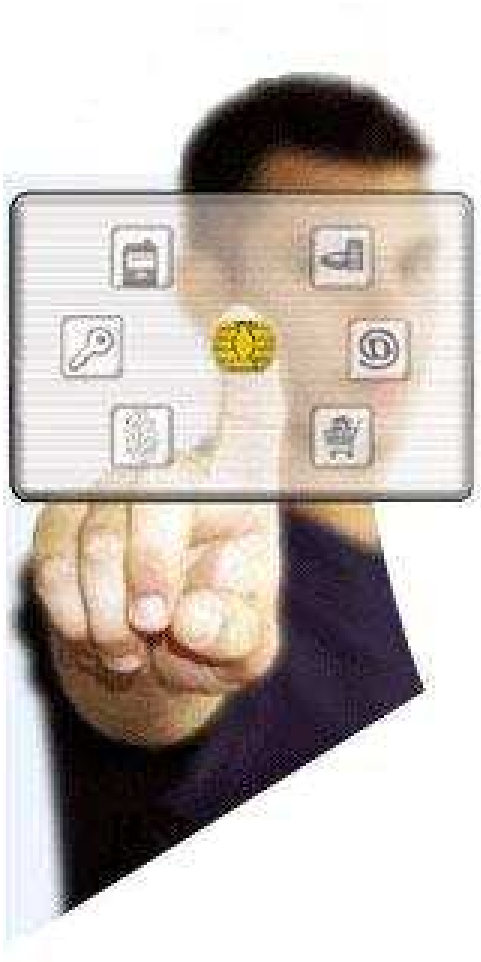
Relevância do Trabalho



- ✓ poder computacional
- ✓ dinâmico: novos *applets* podem ser instalados e registrados no *smart card* (Paludo. 2003, p. 85)
- ✓ flexibilidade: permite compartilhamento de produtos e serviços no mesmo *smart card* (Buse. 1998, p iv)
- ✓ exemplo para futuros trabalhos

DOCUMENTOS E DINHEIRO ELETRÔNICO COM *SMART CARDS* UTILIZANDO A TECNOLOGIA JAVA *CARD*

Roteiro



- ✓ **introdução**
  - ✓ objetivos
  - ✓ relevância
- ✓ **fundamentação teórica**
  - ✓ *smart cards*
  - ✓ tecnologia Java *card*
  - ✓ protocolo APDU
  - ✓ trabalhos correlatos
- ✓ **especificação**
  - ✓ requisitos do problema a ser trabalhado
  - ✓ técnicas e ferramentas utilizadas
  - ✓ diagramas de casos de uso
  - ✓ estrutura básica de um *applet*
  - ✓ diagramas de classes
- ✓ **desenvolvimento**
  - ✓ Java *Card Software Development Kit - SDK*
  - ✓ *Jcop Tools*
  - ✓ *hardware*
  - ✓ operacionalidade da implementação
- ✓ **considerações finais**
  - ✓ conclusões
  - ✓ extensões

Smart cards

- ✓ semelhante a cartões de crédito comum
- ✓ diferencial: *chip* com capacidade de armazenamento e processamento
- ✓ possui memórias:
  - ✓ ROM (*Read Only Memory*)
  - ✓ RAM (*Random Access Memory*)
  - ✓ EEPROM (*Erasable Eletrically Programable ROM*)
- ✓ opcional: co-processador(es) para funções de criptografia
- ✓ padronização: norma ISO 7816

Tecnologia Java *Card*

- ✓ Subconjunto da linguagem Java
  - ✓ principais limitações:
    - ✓ carregamento dinâmico de classes
    - ✓ *threads*
    - ✓ *char*, *double*, *float*, *long*, *arrays* bidimensionais
    - ✓ algumas classes do *package System*

Tecnologia Java *Card*

- ✓ Java Card Virtual Machine - JCVM
  - ✓ Porção *off-card* (computador)
    - ✓ pré-processamento gerando o arquivo Converted Applet (CAP)
  - ✓ Porção *on-card* (*smart card*)
    - ✓ instalação e registro de *applets*
    - ✓ execução das instruções em *byte-code*

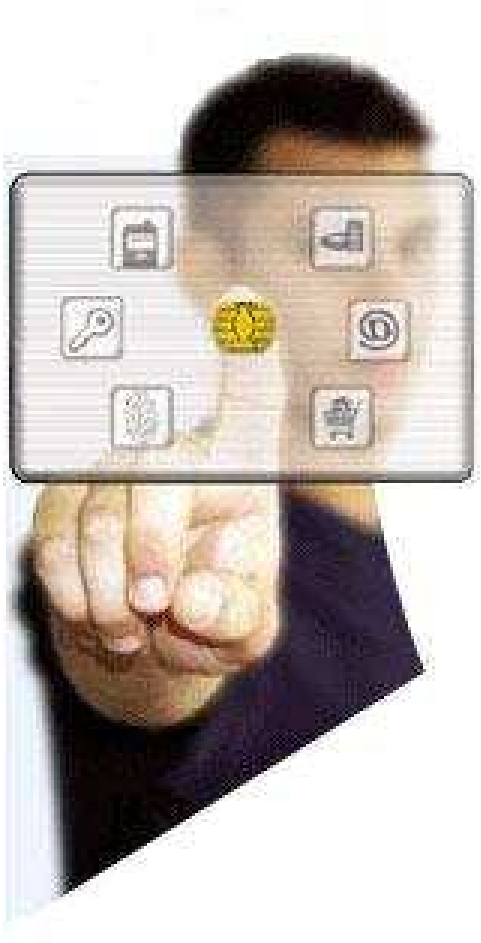
Tecnologia Java *Card*

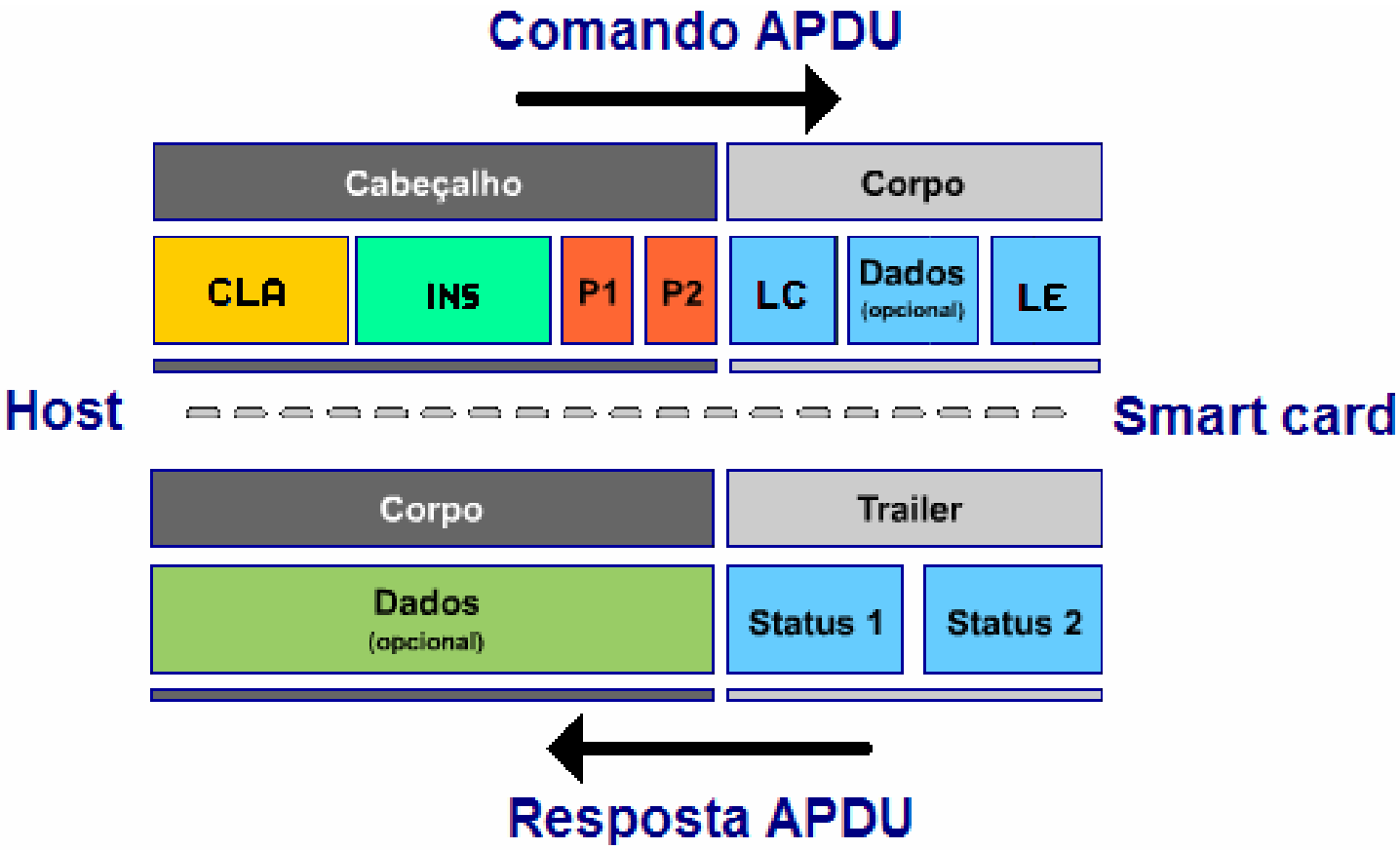
- ✓ Java *Card Runtime Enviroment* - JCRE
  - ✓ gerenciamento de recursos durante as sessões
  - ✓ manter objetos persistentes
  - ✓ operações atômicas e transações
  - ✓ *applet firewall*
  - ✓ compartilhamento de *applets*

Protocolo *Application Protocol Data Units* - APDU

- ✓ utilizado entre *host* e *smart* card para troca de mensagens
- ✓ Dividido em:
  - ✓Comando APDU
  - ✓Resposta APDU

Protocolo APDU





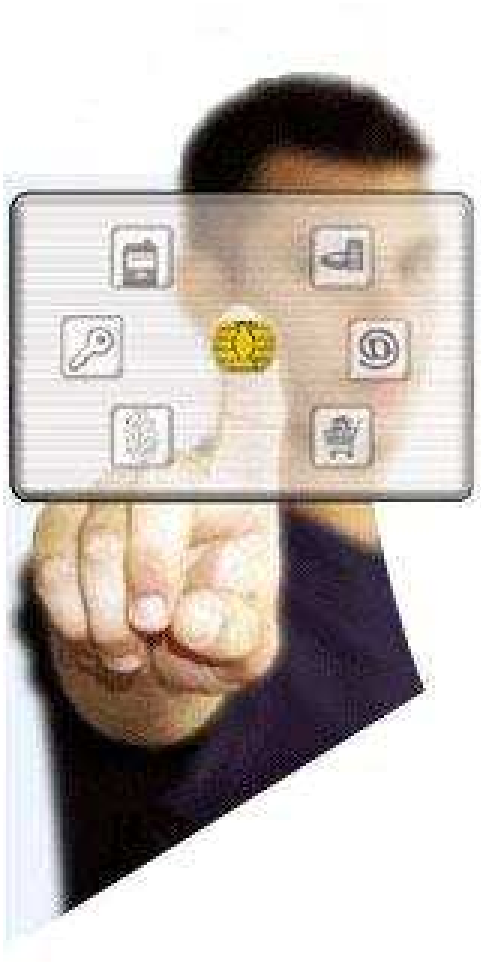
Adaptado de Alonso e Medeiros (2005)

Trabalhos correlatos

- ✓ cenário para aplicação em cooperativas médicas (Buse, 1998)
- ✓ tecnologias para aplicações móveis (Paludo, 2003)
- ✓ cenário para aplicação *e-commerce* (Hong e Chun, 2001)

DOCUMENTOS E DINHEIRO ELETRÔNICO COM *SMART CARDS* UTILIZANDO A TECNOLOGIA JAVA *CARD*

Roteiro



- ✓ **introdução**
  - ✓ objetivos
  - ✓ relevância
- ✓ **fundamentação teórica**
  - ✓ *smart cards*
  - ✓ tecnologia Java *card*
  - ✓ protocolo APDU
  - ✓ trabalhos correlatos
- ✓ **especificação**
  - ✓ requisitos do problema a ser trabalhado
  - ✓ técnicas e ferramentas utilizadas
  - ✓ diagramas de casos de uso
  - ✓ estrutura básica de um *applet*
  - ✓ diagramas de classes
- ✓ **desenvolvimento**
  - ✓ Java *Card Software Development Kit - SDK*
  - ✓ *Jcop Tools*
  - ✓ *hardware*
  - ✓ operacionalidade da implementação
- ✓ **considerações finais**
  - ✓ conclusões
  - ✓ extensões

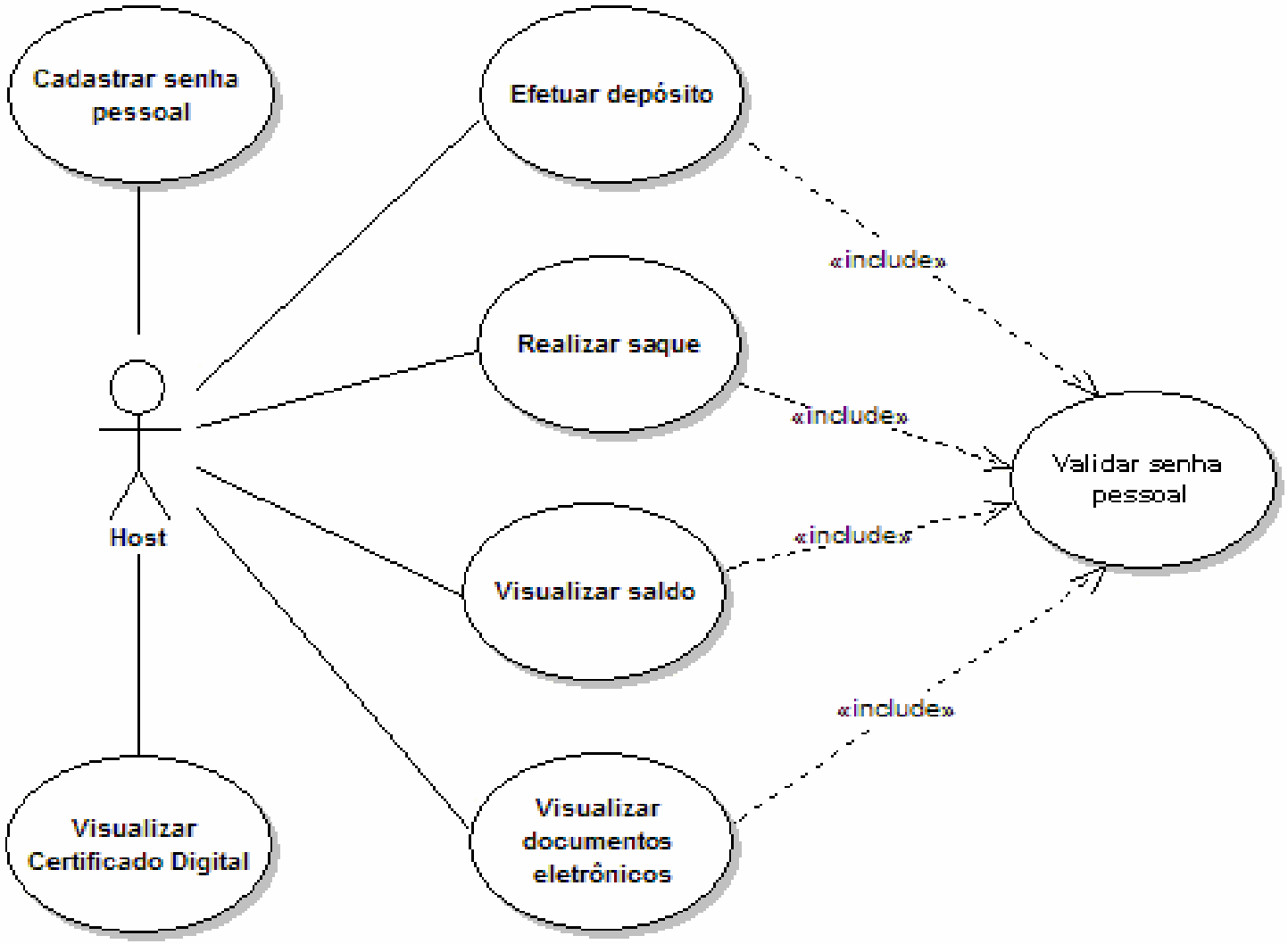
Requisitos do problema a ser trabalhado

- ✓ permitir o armazenamento e leitura de documentos eletrônicos (RF)
- ✓ permitir o controle de débitos e créditos com relação ao dinheiro eletrônico (RF)
- ✓ permitir o acesso às informações mediante uso de senha pessoal (RF)
- ✓ utilizar a tecnologia Java *card* (RNF - implementação)
- ✓ permitir o armazenamento de um par de chaves e certificado digital (RNF - segurança)

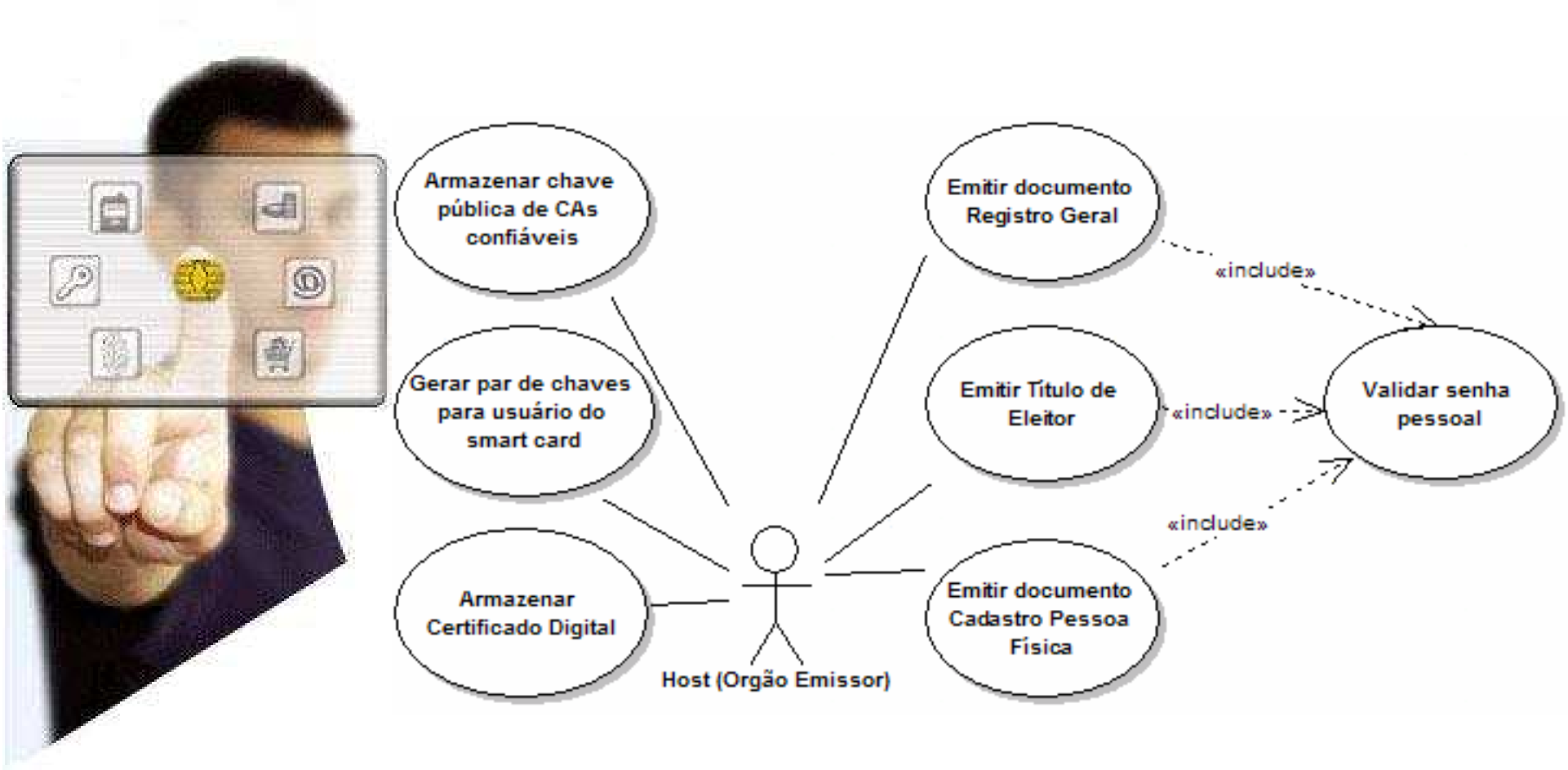
Técnicas e ferramentas utilizadas

- ✓ orientação a objetos
- ✓ *Unified moddeling language* (UML)
- ✓ *Enterprise Architect* (*Sparx Systems*)

Diagramas de Casos de Uso



Diagramas de Casos de Uso



Estrutura básica de um *applet*

- ✓ *applet* Java card extende da classe *Applet* do *package javacard.framework:*
  - ✓ *install()*
  - ✓ *select()*
  - ✓ *deselect()*
  - ✓ *process()*

Diagrama de classes (*package* senha)

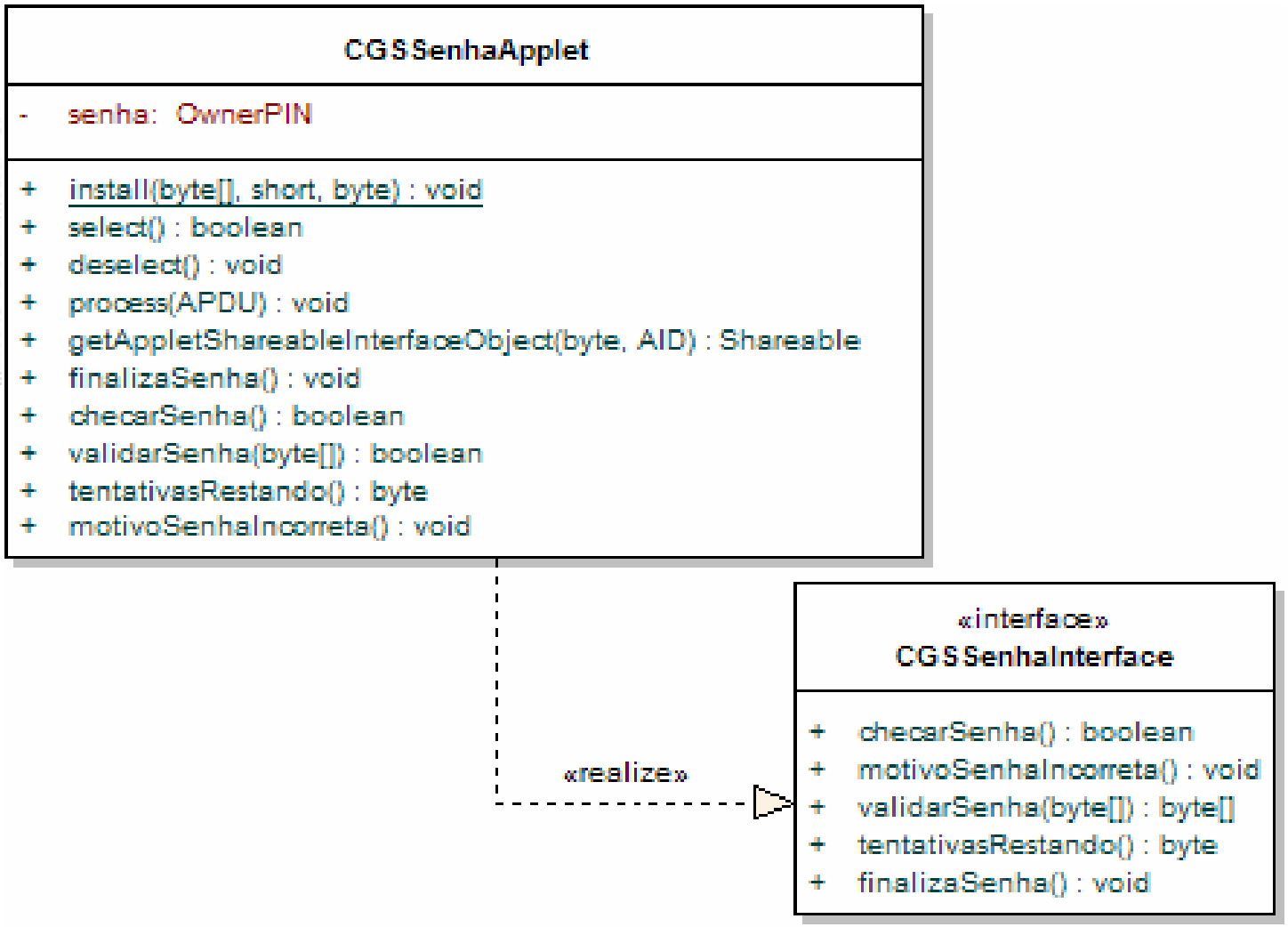
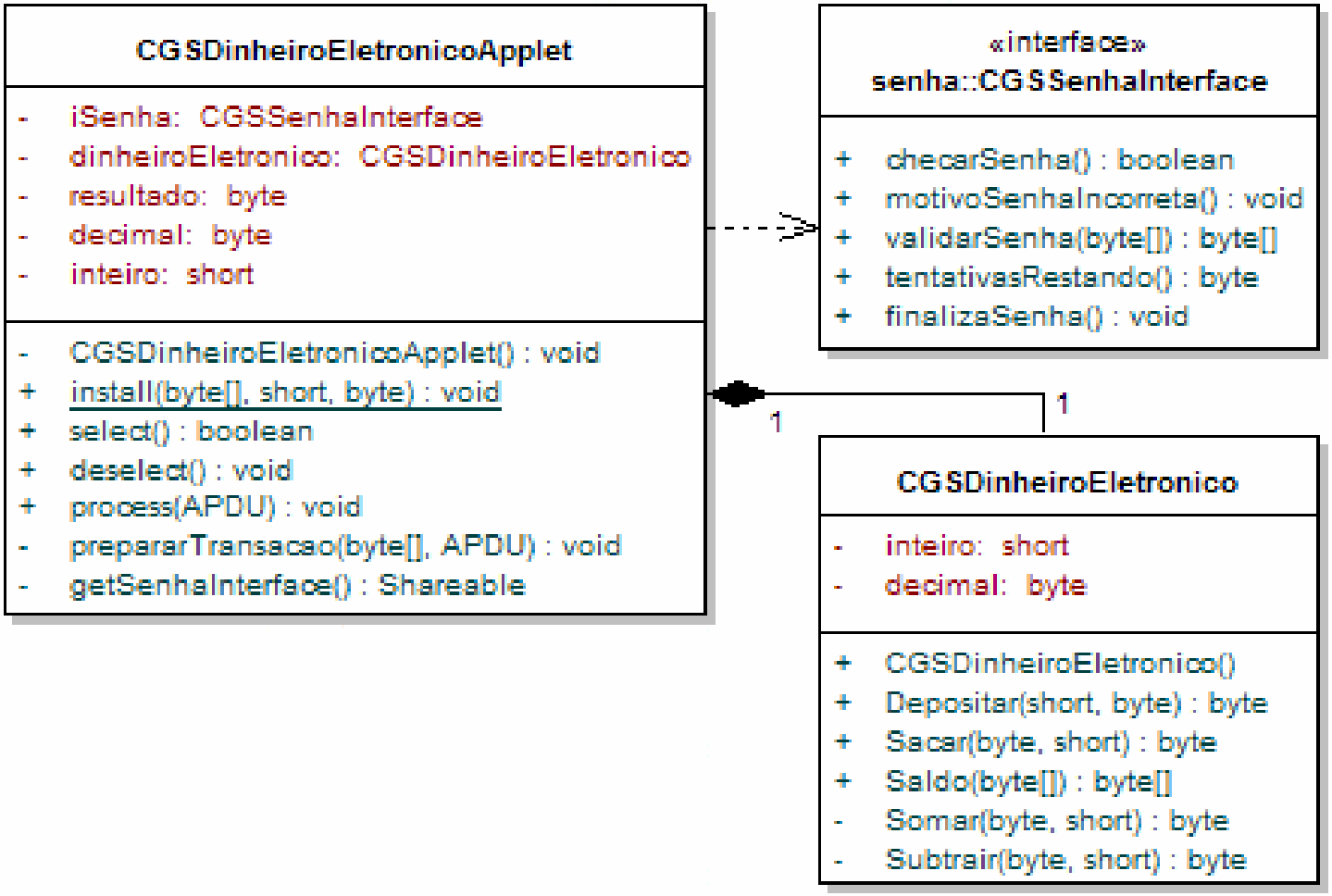
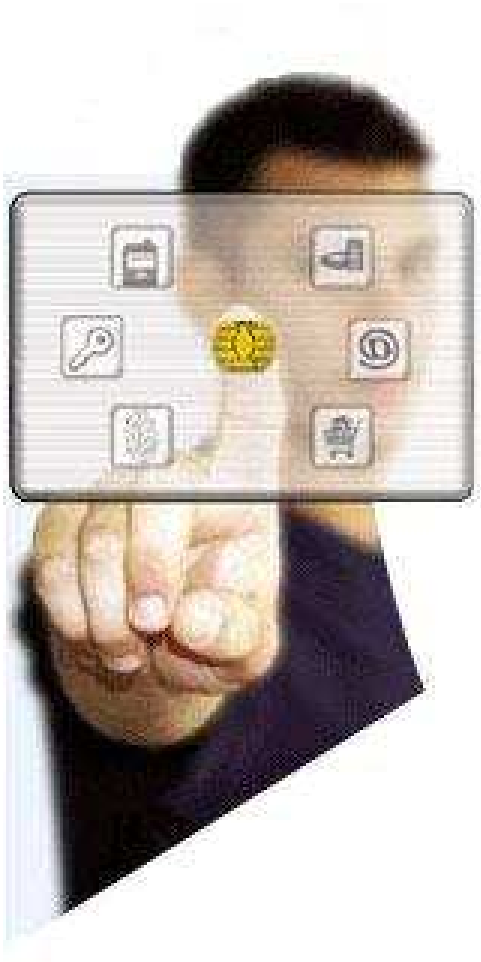


Diagrama de classes (*package* dinheiroEletronico)



DOCUMENTOS E DINHEIRO ELETRÔNICO COM *SMART CARDS* UTILIZANDO A TECNOLOGIA JAVA *CARD*

Roteiro



- ✓ **introdução**
  - ✓ objetivos
  - ✓ relevância
- ✓ **fundamentação teórica**
  - ✓ *smart cards*
  - ✓ tecnologia Java *card*
  - ✓ protocolo APDU
  - ✓ trabalhos correlatos
- ✓ **especificação**
  - ✓ requisitos do problema a ser trabalhado
  - ✓ técnicas e ferramentas utilizadas
  - ✓ diagramas de casos de uso
  - ✓ estrutura básica de um *applet*
  - ✓ diagramas de classes
- ✓ **desenvolvimento**
  - ✓ Java *Card Software Development Kit - SDK*
  - ✓ *Jcop Tools*
  - ✓ *hardware*
  - ✓ operacionalidade da implementação
- ✓ **considerações finais**
  - ✓ conclusões
  - ✓ extensões

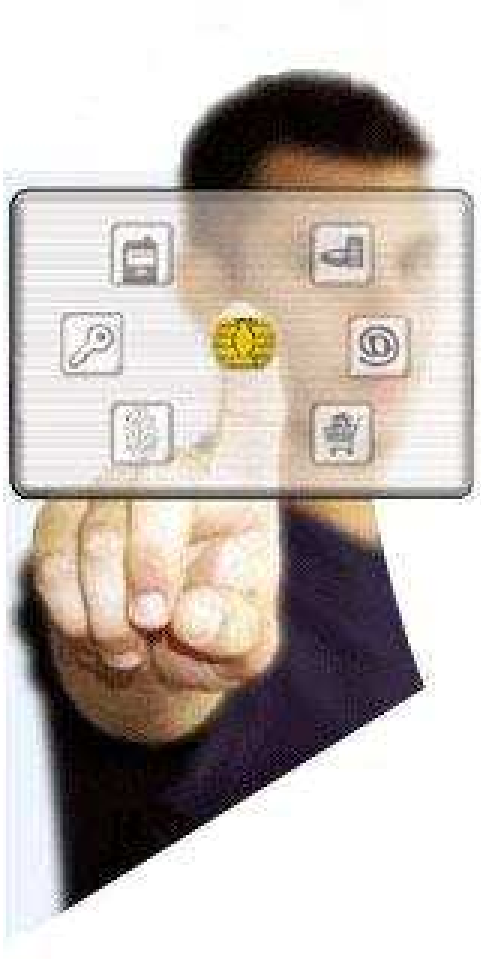
Java *Card* SDK – *Software Development Kit*

- ✓ documentação
- ✓ ferramentas para testes em ambiente simulado
- ✓ limitações:
  - ✓ instalação/exclusão de *applets*
  - ✓ persistência de dados
  - ✓ transações
  - ✓ compartilhamento de *applets*

JCOP *Tools*

- ✓ *plugin* para IDE Eclipse
- ✓ testes em ambiente real: *smart card* e leitor/gravador
- ✓ possui ferramenta de linha de comando para envio de comandos APDU (JCOP *Shell*)
- ✓ funções de *upload*, instalação e registro de *applets* no *smart card*
- ✓ *applet identifier* (AID)

Hardware



- ✓ leitor/gravador de *smart cards* (*Card Acceptance Device* - CAD)
- ✓ *smart card*
  - ✓72 *Kbytes* EEPROM
  - ✓160 *Kbytes* ROM
  - ✓4.5 *Kbytes* RAM
  - ✓Co-processadores
    - ✓RSA (Rivest-Shamir-Adleman)
    - ✓AES (*Advanced Encryption Standard*)
    - ✓3DES (*Triple Data Encryption Standard*)

Hardware – Smart card

Hardware – leitor/gravador de *smart card*

Operacionalidade da Implementação

JCOP Shell | Java Card Memory | CAP File Properties | Java Card Bytecode | Console

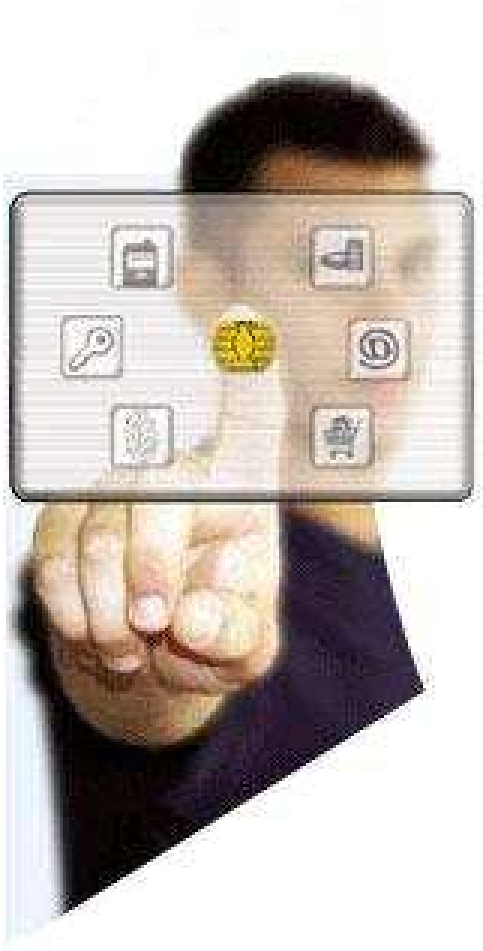
```
cm>  /select |documentosApplet
 => 00 A4 04 00 10 64 6F 63 75 6D 65 6E 74 6F 73 41    .....documentosA
    70 70 6C 65 74 00                                  pplet.
 (250 msec)
 <= 90 00                                              ..
Status: No Error
cm>  /send 0005000003313233
 => 00 05 00 00 03 31 32 33                            .....123
 (81 msec)
 <= 90 00                                              ..
Status: No Error
cm>  /send 000600001F436C656265722047696F76616E6E69205375617669003136303331393832 00
 => 00 06 00 00 1F 43 6C 65 62 65 72 20 47 69 6F 76    .....Cleber Giov
    61 6E 6E 69 20 53 75 61 76 69 00 31 36 30 33 31    anni Suavi.16031
    39 38 32 00                                        982.
 (221 msec)
 <= 90 00                                              ..
Status: No Error
cm>  /send 0001000000
 => 00 01 00 00 00                                     .....
 (311 msec)
 <= 43 6C 65 62 65 72 20 47 69 6F 76 61 6E 6E 69 20    Cleber Giovanni
    53 75 61 76 69 00 31 36 30 33 31 39 38 32 00 90    Suavi.16031982..
    00                                                 .
Status: No Error
```

Autenticação com Senha

Gravação de Informações

Consulta de Informações

Operacionalidade da Implementação



```
cm>  /send 0005000003313233
 => 00 05 00 00 03 31 32 33
 (81 msec)
 <= 90 00
```

dados

LC

parâmetro 2

parâmetro 1

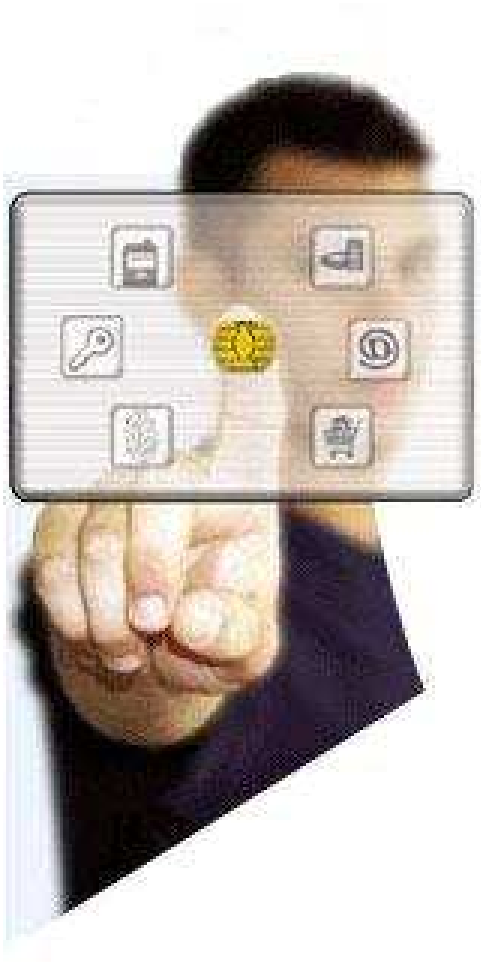
instrução

classe

Cabeçalho				Corpo		
CLA	INS	P1	P2	LC	Dados (opcional)	LE

DOCUMENTOS E DINHEIRO ELETRÔNICO COM *SMART CARDS* UTILIZANDO A TECNOLOGIA JAVA *CARD*

Roteiro



- ✓ **introdução**
  - ✓ objetivos
  - ✓ relevância
- ✓ **fundamentação teórica**
  - ✓ *smart cards*
  - ✓ tecnologia Java *card*
  - ✓ protocolo APDU
  - ✓ trabalhos correlatos
- ✓ **especificação**
  - ✓ requisitos do problema a ser trabalhado
  - ✓ técnicas e ferramentas utilizadas
  - ✓ diagramas de casos de uso
  - ✓ estrutura básica de um *applet*
  - ✓ diagramas de classes
- ✓ **desenvolvimento**
  - ✓ Java *Card Software Development Kit - SDK*
  - ✓ *Jcop Tools*
  - ✓ *hardware*
  - ✓ operacionalidade da implementação
- ✓ **considerações finais**
  - ✓ conclusões
  - ✓ extensões

Conclusões

- ✓ objetivo principal alcançado
- ✓ Java *card* não possui classes para manipulação de certificados digitais
- ✓ Kit completo de desenvolvimento : *smart card* + leitor/gravador + *plugin* JCOP *Tools*
- ✓ Escreve-se código para um chip em alto nível

Extensões

- ✓ desenvolvimento do software no *host* faria o envio de comandos APDU ao *smart card*
- ✓ mecanismos de segurança de modo que o *smart card* seja capaz de autenticar o *host*

DOCUMENTOS E DINHEIRO ELETRÔNICO COM *SMART CARDS* UTILIZANDO A TECNOLOGIA JAVA *CARD*

Referências bibliográficas

- ✓ ALONSO, Edson E.; MEDEIROS, Igor. **Explorando pequenos grandes mundos com Java card**. Mundo Java, Curitiba, n. 12, p. 52-61, 2005.
- ✓ BUSE, Alibert. **Tecnologia do smart card aplicada em cooperativas médicas.** 1998. 66 f. Monografia (Especialização em Tecnologias em Desenvolvimento de Sistemas) – Universidade Regional de Blumenau, Blumenau.
- ✓ CHEN, Ziqun. **Java card technology for smart cards**: architecture and programmer's guide. Massachusetts: Addison Wesley, 2000.
- ✓ HONG, Insuk; CHUN, Ingook. The implementation of electronic money for e-commerce using Java card. In: INTERNATIONAL SYMPOSIUM ON INDUSTRIAL ELECTRONICS, 2001, Pusan, Coréia. **Proceedings**... Pusan, Coréia: Information and Technology Department, Pusan National University, 2001. p. 1369-1372. Disponível em: <http://ieeexplore.ieee.org/iel5/7417/20158/00931681.pdf>. Acesso em: 23 mar. 2005.
- ✓ PALUDO, Lauriana. **Um estudo sobre as tecnologias Java de desenvolvimento de aplicações móveis**. 2003. 117 f. Monografia (Especialização em Ciência da Computação) – Departamento de Informática e Estatística, Universidade Federal de Santa Catarina, Florianópolis. Disponível em: <www.inf.ufsc.br/~leandro/ensino/esp/monografiaLaurianaPaludo.pdf>. Acesso em: 08 mar. 2005