

# Smart Cards

Uma tecnologia abrindo o seu  
caminho

# Sumário

- Visão geral - história
- Tecnologias
- Aplicações

# Historia dos cartões plásticos

- Inicialmente utilizados para identificação.
- Inicio uso para pagamentos em 1950 - Diners Club
- Segurança contra contrafações :
  - Caracteres em relevo e senha
  - Hologramas e micro impressão.
  - Desenhos invisíveis-fibras fluorescentes.
  - Assinatura
- Seguro, mas não a prova de estupidez.

# Cartões com tarja magnética

- Dados escritos eletronicamente.
- Trilhas com dados diferenciados.
- Inversões de fluxo correspondem a dados.
- Aproximadamente 140 bytes armazenados.
- Dados podem ser perdidos
- Segurança baixa

# O que são os Smart Cards?

Smart Cards são cartões, similares aos cartões de crédito, que contêm microprocessador e memória e atendem o padrão ISO 7816

Pequenos computadores em uma tira de plástico



# Tipos

- **Smart Card com contato**
  - Cartões de memória
  - Cartões microprocessados
- **Smart Card sem contato (*Contactless*)**
  - Armazenamento seguro de dados
  - Capacidade aritmética
- **Smart Card *COMBI***
  - Integração dos dois formatos
  - Único processador
  - Tarja magnética



# Historia dos Smart Cards

- 1974 : Primeira patente - Roland Moreno
- 1981 : Bull e Philips produzem cartão que atende as normas ISO
- Início 80's : France Télécom usa cartão nos telefones públicos
- 1985 : Cartões bancários são usado na França
- Desde 98 mais de 1 bilhão de cartões / ano

# Smart cards

- Vantagens sobre os magnéticos
  - Maior espaço de memória
  - Armazena informações secretas
  - Inteligência própria
  - Elimina a necessidade de enviar dados confidenciais nas linhas de comunicação

# A tarja magnética

## Negativo

- Fragilidade
- Segurança
- Memória pequena
- Pode ser replicado
- Operação on-line

## Positivo

- Custo
- Tecnologia conhecida
- Novas tecnologias

# Magneprint

- **A tarja tem bilhões de partículas magnéticas**
  - Cada uma tem propriedades magnéticas
  - Distribuídas randomicamente e tamanhos variados
  - Cada uma apresenta ruído intrínseco
  - Pode ser construída uma assinatura



# Smart com contato x Magnético

## Negativo

- Maior custo
- Contatos elétricos
- Mais frágil

## Positivo

- Memória
- Inteligente
- Microprocessado
- Criptografia
- Senhas
- Um cartão para tudo

# Smart sem contato x com contato

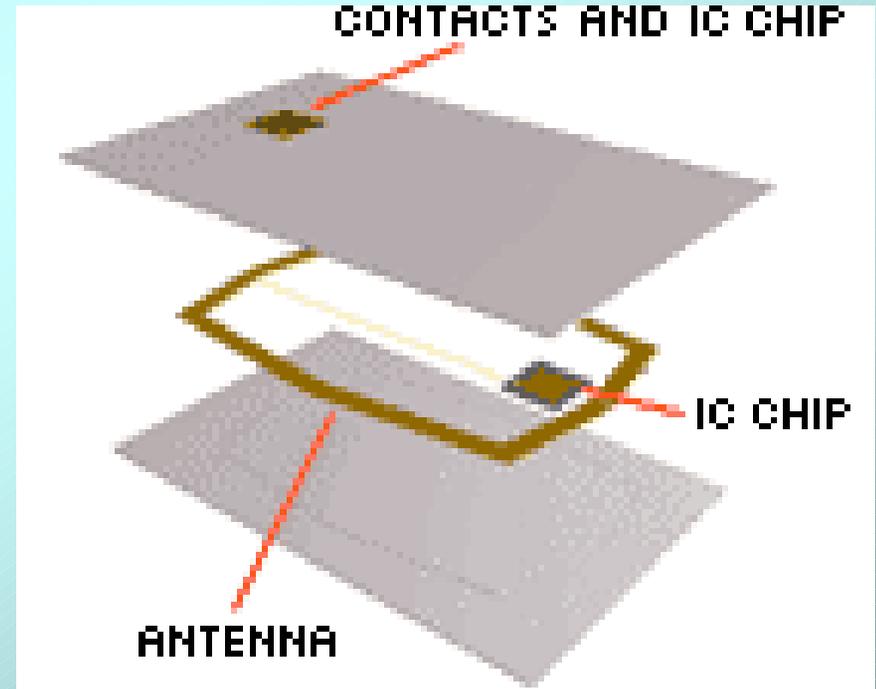
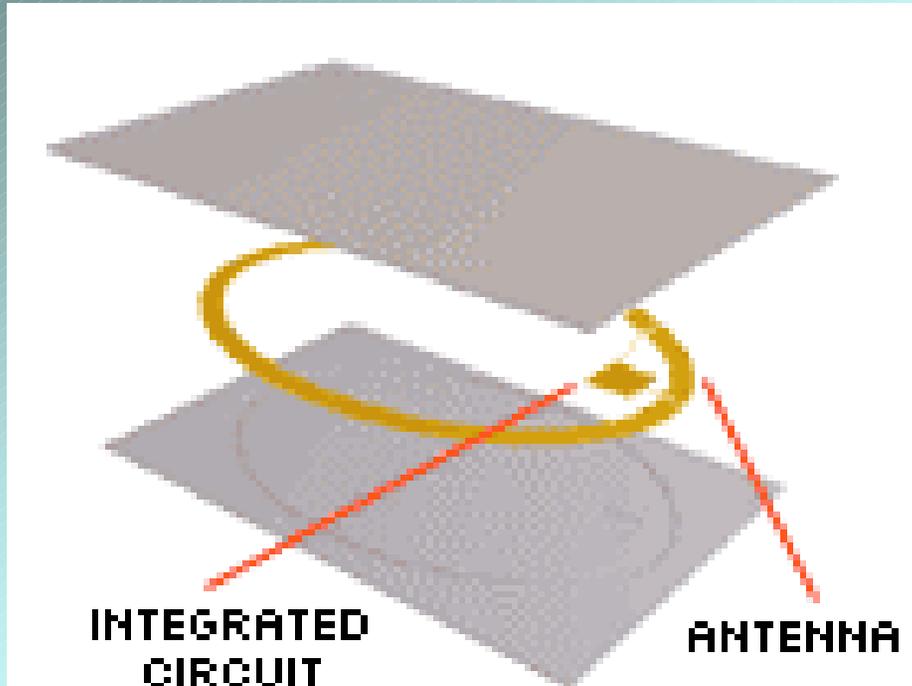
## Negativo

- Maior custo
- Circuito da antena
- Memória menor
- Mais frágil

## Positivo

- Uso mais fácil
- Uso por aproximação
- Transações rápidas
- Transações off-line

# O interior do cartão



# Cartões contactless

- Desvantagens
  - Caro: Pode custar \$ 1,2 em grandes quantidades.
  - Medo do usuário: a transação pode acontecer sem conhecimento.
  - Desaconselhável para grandes transferências de dinheiro. Rápido demais
- Uso:
  - Indústria do transporte
  - Controle de Acesso
  - Qualquer aplicação rápida.

# Cartões contactless

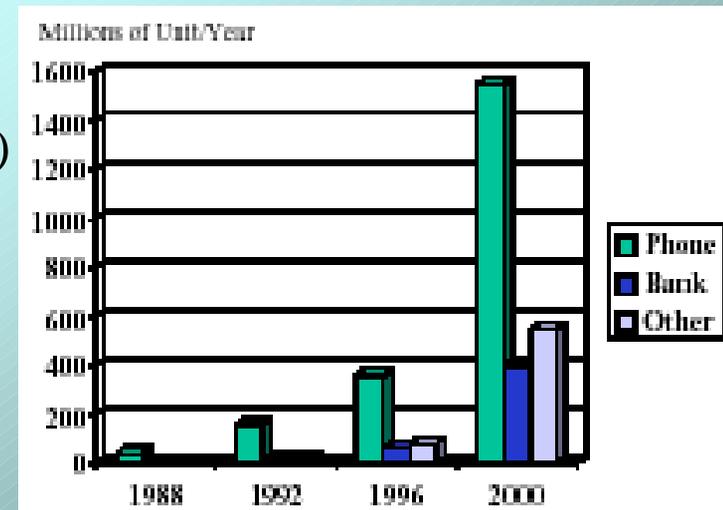
## Vantagens:

- Não é necessária a inserção.
- A alimentação é transmitida por rádio frequência via antena interna.
- Distância de leitura: de poucos cm até meio metro.
- Transação rápida.
- Maior confiabilidade por não ter contato mecânico.
- Vida maior por não ter desgaste mecânico

# Dados de mercado

## Smart Cards

- Divisão do mercado
  - Europa: **80%**
  - Ásia: 16%
  - América do Norte: 3%
- Mercado: Aprox. 2.5 Bilhões de cartões
- Distribuição por aplicação:
  - Telefonia: mais que 50% (em números)
  - Bancos: mais que 50% (em valor)



# Aplicações

- **Identificação:**

- ▶ Controle de acesso
- ▶ Controle de ponto
- ▶ Acesso à áreas restritas
- ▶ Compatibilidade com algumas técnicas de Biometria
- ▶ Mais de 1.000.000 de universitários no Estados Unidos

# Aplicações

## •Saúde:

- ▶ Alemanha: 80 milhões de cartões emitidos (todo cidadão tem direito)
- ▶ França: projeto *Sésam Vitale* espera emitir 10 milhões de cartões
- ▶ Comitê Europeu de Padronização de informações de saúde

# Aplicações

## Financeiras:

- **Débito - crédito:** aumento de segurança, oferta de novos serviços
  - ▶ *AMEX Blue Card:* início em Set / 99. Gasto estimado em marketing: U\$ 45 milhões. Estimativa de novas contas: 2 milhões
  - ▶ *UK Chip Card* 12 milhões de cartões sendo convertidos
  - ▶ *Deutsch GeldKarte* - mais de 40 milhões de cartões emitidos
  - ▶ *France GIE Carte Bancaire:* reduzir fraudes. 25 milhões de cartões de débito bandeira Visa.

# Aplicações

## •Telefonia:

- GSM – Cartão SIM, permite transferir dados nos telefones, armazenar agendas, mensagens créditos etc.
  - ▶ Cartão pré-pago, facilita a operação eliminando o troco

# Aplicações

## **Fidelidade:**

### Shoppings Centers

- ▶ Conveniências
- ▶ Farmácias, cinemas, restaurantes, hotéis ...
- ▶ Experiências nos Estados Unidos
  - ▶ Boots Advantage Card
  - ▶ Shell Smart Card
  - ▶ Rite Aid

**Marketing, incremento de vendas, incremento no *market share*.**

# Aplicações

- **Trânsito:**

- ▶ Transporte público (ônibus, metrô, trem, etc). Integração de modais
- ▶ Pagamento de pedágio
- ▶ Estacionamento
- ▶ Carteira de habilitação
- ▶ Projeto Smart Card em Washington DC
- ▶ US DOT Smart Fare Tech Brief
- ▶ Concord Conference Paper on Transportation
- ▶ The Intelligent Transportation Society of America
- ▶ **O projeto de transporte público de São Paulo**

# Smart Cards

na bilhetagem eletrônica de São Paulo

- 12.000 ônibus
- 60 garagens
- 3,5 milhões de cartões distribuídos
- 2 Milhões de transações por dia
- 200.000 recargas por dia em 800 lotéricas
- 3 novas redes começando a comercialização
- 26 lojas próprias da São Paulo Transportes

# Smart Cards

na bilhetagem eletrônica de São Paulo

- 800.000 cartões Vale Transporte
- 700.000 cartões estudantes
- 1 Milhão cartões usuários pagantes
- 700.000 cartões idosos
- 200.000 cartões operacionais

# Bilhetagem Eletrônica

digicon



Nome: Fulano

Número: 12345

Tipo: Comum

• *Carteira Especial*

• *Carteira Comum*

• *Carteira Dinheiro*

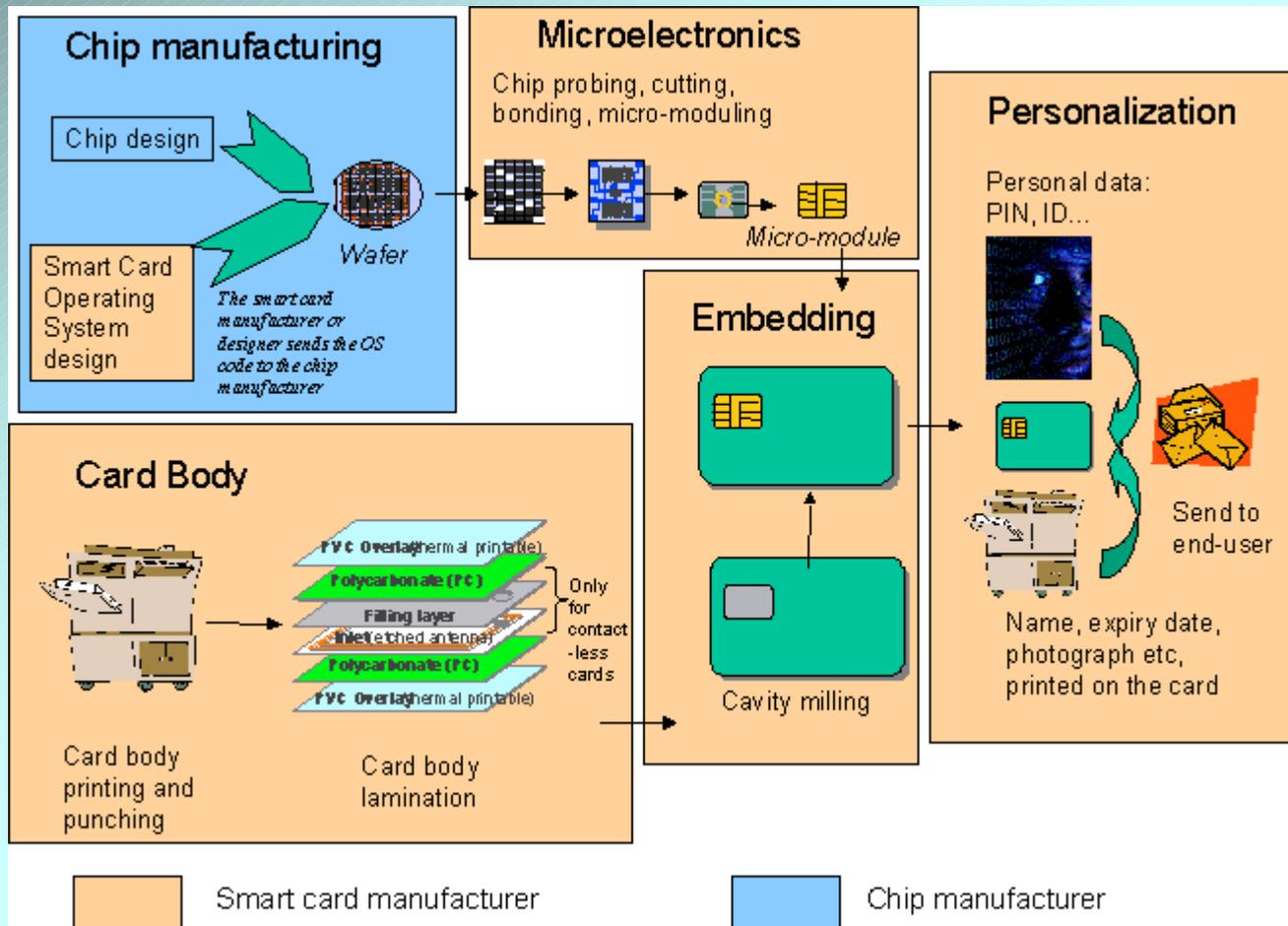
- **Smart Card com contato: valores**
- **Smart Card sem contato: para usuário**
- **Leitores para cartões**
- **SAM e SIM's para gerar assinaturas**
- **Dispositivos somente de leitura**
- **Multi - aplicação independente**
- **Garantia de segurança em todas etapas da comunicação**
- **Possibilidade de restrições**
- **Possibilidade de benefícios**
- **Automatização de processos**
- **Dados estatísticos**
- **Maior controle da operação**

fim

Corrado Lacchini

[clacchini@digicon.com.br](mailto:clacchini@digicon.com.br)

# Processo



# Tecnologia

## • Físico:

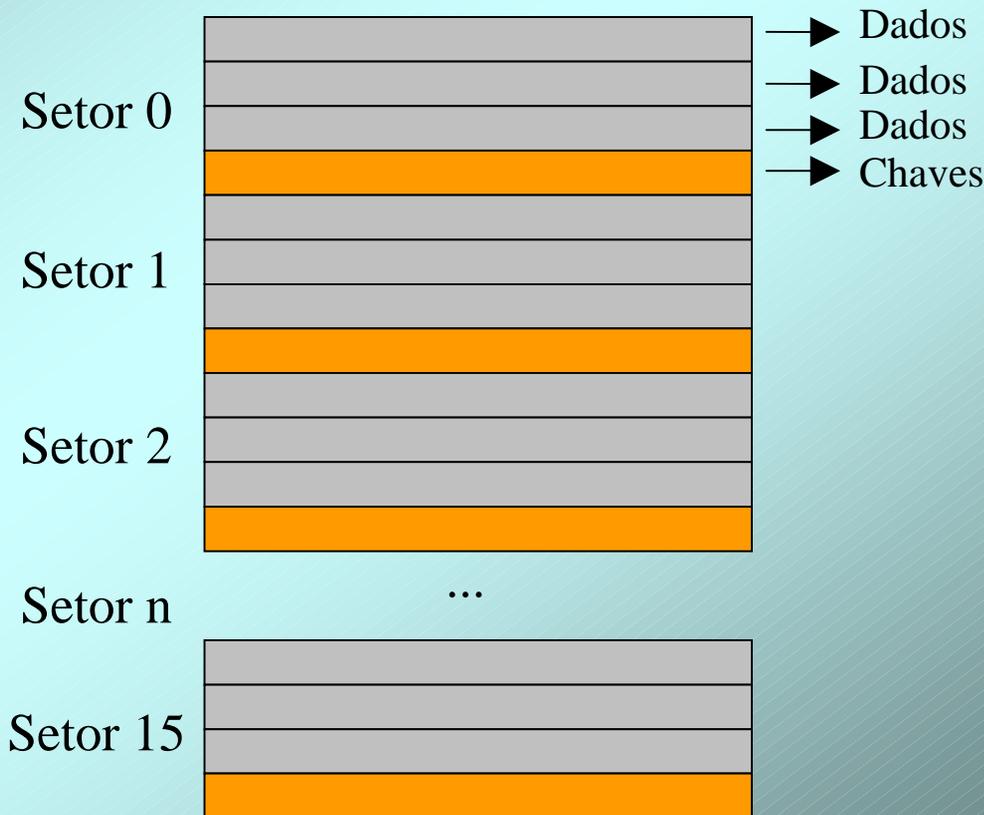
- ▶ Número de série irrepetível
- ▶ Capacidade: 1024 bits
- ▶ 16 setores
- ▶ Cada setor com 4 blocos
- ▶ Cada bloco com 16 bytes
- ▶ Cada setor com segurança
- ▶ 2 chaves e *Access Conditions*

Chave A    ACC    Chave B

6 bytes	4 bytes	6 bytes
---------	---------	---------

## Força Bruta

Caracteres	Possibilidades
1	256
2	65.536
3	16.777.216
4	4.294.967.296
5	1.099.511.627.776
6	281.474.976.710.656



- 30 ataques/s
- 297.517 anos

Digicon



Chaves diversificadas