SMART CARDS

Gustavo Bahnert (gustavo.bahnert@gmail.com)
Jean Rafael Sahlberg (jrsahlberg@gmail.com)
PUCRS, Porto Alegre, RS
Professor: Eduardo Augusto Bezerra (bezerra@inf.pucrs.br)

História dos smart cards

Em 1968 um inventor alemão, Jurgen Dethloff, patenteou o uso de cartões plásticos para carregar microchips. Em 1970, um inventor japonês chamado Kunitake Arimura patenteou algo semelhante e os Smart Cards foram introduzidos no Japão no mesmo ano. Em 1974 o francês Roland Moreno registrou o seu invento na França.

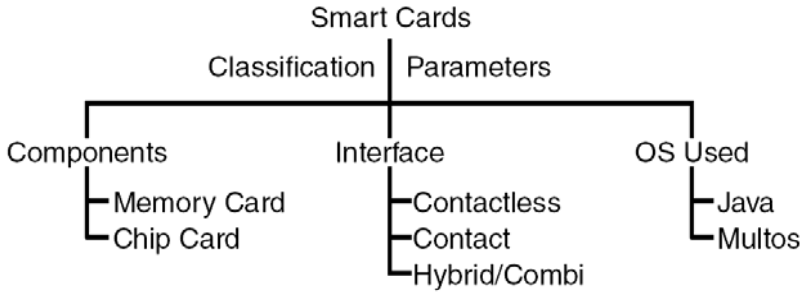
A maioria das pesquisas sobre Smart Cards aconteceram na Europa, por essa razão 80% desse mercado encontra-se nessa região. Smart Cards já estão sendo usados no mundo há vários anos para diversas aplicações e no futuro acredita-se que eles irão ser ainda mais pervasivos.

Classificação dos Smart Cards

Um Smart Card é definido como:

"Um cartão plástico, usualmente semelhante no tamanho e formato de um cartão de crédito, contendo um microprocessador e memória (a qual permite que se armazenem e processem dados) e que respeite os padrões ISO 7816."

Eles podem ser classificados em várias categorias como mostra a figura abaixo:



Componentes

Existem dois tipos de Smart Cards nessa categoria. Um são os *Memory Cards* (cartões de memória) e os que possuem um processador, chamados de *Chip Cards* ou *Microprocessor Cards*.

Memory Cards: São o tipo mais comum e de mais baixo custo. Eles possuem:

EEPROM: Onde todos os dados da aplicação são escritos. Seu tamanho varia de entre 2 kB e 8 kB. As informações armazenadas variam com o tempo e podem ser protegidas através de um PIN.

ROM: Armazena dados que não mudam. Normalmente armazena informações como número do cartão, nome do proprietário do cartão, etc.

Um esquema lógico de segurança limita o acesso de leitura e escrita de certas regiões da memória, apenas informando um código secreto o acesso dessas regiões é liberado.

A tecnologia simples empregada nesses cartões permite que sua construção seja muito barata e ao mesmo tempo robusto o suficiente para diversas aplicações por ser possível armazenar de alguma centena de bits até 8 kB de dados. Esse tipo de cartão tem uma aceitação alta no mercado de telefones pré-pagos pela sua simplicidade. Outras aplicações possíveis são em transporte publico, esquema de estacionamento pré-pago, cartões de programa de fidelidade, etc.

Microprocessor/Chip Cards: Esse tipo de cartão incorpora um microprocessador e são os que tecnicamente podem ser chamados de Smart Cards. Os principais componentes desse cartão são:

ROM: Armazena o sistema operacional e é escrito uma única vez (normalmente na produção do cartão). O tamanho da ROM varia de alguns *kilobytes* até 32 kB, dependendo do sistema operacional usado. Uma vez escritas essas informações não podem ser alteradas.

EEPROM: A EEMPROM guarda os programas e os dados do cartão. Não é uma memória permanente e é frequentemente escrita e apagada. Seu tamanho varia de 2 kB à 32 kB.

RAM: Memória volátil, usada pelo processador para executar as funções desejadas. É apagada toda vez que se desligada o cartão. Seu tamanho médio é de 256 bytes.

CPU: Usualmente é um microprocessador de 8 bits baseado na arquitetura CISC com um *clock* médio de 5 MHz. Lentamente está sendo substituído por microprocessadores de 32 bits, graças aos cartões Java.

Esses são cartões mais caros que os *memory cards* mas podem suportar diversos tipos de aplicações e disponibilizam uma forte segurança dos dados. Pode ser usado para controle de acesso, cartão de crédito, cartão para transações financeiras, passaporte ou outros tipos de aplicações que necessitem forte segurança.

Classificação por tipo de interface

Smart Cards podem ser classificados pelo método que utilizam para se comunicar e transferir dados para o leitor. Baseado nesse critério, eles podem ser classificados como *contact cards*, *contactless cards* ou *combi cards*.

Contact Cards: Esse tipo de cartão necessita ser inserido em um leitor para ser alimentado. Ele possui de seis a oito pinos dourados que devem ser conectados fisicamente ao leitor. Com o tempo os contatos podem acabar de desgastando ou a eletricidade estática pode danificar os circuitos do cartão.

Contactless Cards: Não necessitam serem inseridos em um leitor, trabalham por radio freqüência, apenas necessitando serem aproximados de uma antena. A distancia de leitura pode variar de alguns centímetros a até 50 cm. Esse tipo de cartão normalmente é usado em situações que a transação precisa ser rápida.

Combi ou Hybrid Cards: É a combinação dos dois tipos anteriores. Possuem tanto a interface física como a por radio freqüência. Possibilitando, dessa forma, que seja utilizado do jeito mais adequada para cada tipo de transação. No caso de operações que necessitem ser rápidas e não muito seguras utiliza-se o modo sem contato físico, já transações que necessitem de maior segurança utiliza-se o contato físico.

Sistema operacional

Smart Cards também são classificados quanto ao sistema operacional, existem diversos sistemas operacionais disponíveis no mercado, os principais são:

- MultOS
- JavaCard
- Cyberflex
- StarCOS
- MFC

O sistema operacional dos smart cards (chamados normalmente de SCOS – Smart Card Operational System) é colocado na memória ROM e costumam ocupar menos de 16 kB. Eles controlam os arquivos, gerenciamento de memória e os protocolos de transmissão.

Aplicações Smart Card

Cartões de telefones públicos pré-pagos aparecem em primeiro lugar como aplicação mais utilizada por Smart Cards. Como é possível recarregar o cartão, o seu valor pode ser repassado para o consumidor no momento da venda. O mesmo ocorre com telefones celulares, o *SIM Card* nada mais é do que um Smart Card.

Smart Cards permite que os bancos substituam seus cartões magnéticos que não oferecem quase nenhuma segurança e necessitam que as transações sejam efetuadas *online*, para autenticar a operação. Com Smart Cards isso não é necessário, uma vez que esses cartões possuem lógicas de segurança e podem armazenar informações como saldo disponível e dados pessoais do cliente.

Existem infinidade de possíveis aplicações, como por exemplo: cartões de estacionamento pré-pago, identificação (ID Cards), transporte publico, programa de fidelidade, etc.

Referências

1. Smart Card Handbook, by W. Ra nkl and W. E ffing.
2. Smart Card Security and Applications, by Mike Hendry.
3. Smart Cards Case Study, IBM Redbook.
4. ISO 7816 specifications.
5. EMV 2000 specifications.