Arquitetura de Sistemas de Segurança baseado em Smart Card

Isabelli Sade Ladeira[1], Emerson Rodrigo Alves Tavares[1]

[1]Ciência da Computação – Universidade Presidente Antonio Carlos (UNIPAC)
Rua Monsenhor José Augusto, 203 – 36205-018 – Barbacena – MG – Brasil

isalad@hotmail.com, emersontavares@unipac.br

Resumo. *A capacidade de gravação e proteção das informações contra a manipulação e o acesso não autorizado, fazem dos cartões inteligentes sistemas de segurança muito eficientes na atualidade. Este artigo pretende mostrar a utilização de sistemas Smart Card, fazendo um comparativo entre os tipos de arquiteturas, demonstrando sua implementação em uma aplicação para a autenticação de motoristas de uma empresa.*

Palavras-chave: Smart Card, segurança, autenticação**.**

1. Introdução

Com o crescimento no volume das transações eletrônicas, compras e serviços pela Internet e demais meios digitais, surgiu também a necessidade da utilização de mecanismos de segurança para proteção e sigilo das informações, tanto dos consumidores como das empresas [1].

O problema no controle das informações faz com que, cada vez mais, seja necessário adotar sistemas que mantenham a integridade e privacidade dos dados. Assim, os *Smart Cards* surgem, com uma arquitetura elaborada e portátil, para garantir a proteção e autenticação da informação em suas diversas aplicações. Pode-se encontrar S*mart Cards* sendo utilizados como cartão de crédito, dinheiro eletrônico, soluções de identificação, armazenamento de certificados digitais entre outros usos [2].

Com o objetivo de mostrar a eficiência do *Smart Card* como sistema de segurança na identificação de usuários e autenticação de informações, este artigo apresenta um estudo sobre as arquiteturas dos mesmos, ressaltando suas principais características e funcionalidades, bem como sua relação de custo/benefício.

O corpo do artigo está organizado em seções distribuídas da seguinte forma: a seção 2 apresenta o conceito de sistemas de segurança, sua importância na atualidade e os tipos existentes. A seção 3 conceitua o sistema de *Smart Card*. Na seção 4 são apresentadas as arquiteturas de *Smart Cards*. A seção 5 propõe uma aplicação de exemplo. A seção 6 demonstra como a modelagem desta aplicação foi desenvolvida bem como os diagramas utilizados e o banco de dados. Na seção 7 é descrita a fase de prototipação e desenvolvimento da aplicação. Já na seção 8 estão as considerações finais, com conclusões e sugestões para trabalhos futuros. E, na seção 9, encontram-se as referências bibliográfics utilizadas para o desenvolvimento deste artigo.

2. Sistemas de Segurança

A preocupação com a segurança das informações de um modo geral se faz desde o início das civilizações; porém, somente com o surgimento dos computadores, deu-se uma maior atenção aos sistemas de segurança.

Informação é um bem valioso e deve ser guardada de forma cuidadosa, protegida por algum tipo de segurança [3]. Com o avanço tecnológico, os mecanismos de segurança foram informatizados tentando minimizar os problemas com autenticação de usuários e garantir um maior controle na manipulação dos dados.

No intuito de entender às necessidades de proteção da informação e priorizar aspectos básicos como confidencialidade, integridade e disponibilidade da informação nos dias atuais, foram estabelecidos padrões de implementação e gestão da segurança da informação pela ISO (*International Organization for Standardization*) [4].

A cada dia novas técnicas surgem para combater o problema crônico da falta de segurança nos ambientes de tecnologia de informação e o comportamento inadequado dos usuários. Dentre os sistemas de segurança mais utilizados, destacam-se:

- Radiofreqüência – consiste em um crachá impresso diretamente ou montado em PVC (policloreto de vinila) com etiqueta descartável e é utilizado para aplicações de baixa e/ou alta segurança.
- Código de Barras - utilizados em aplicações comerciais. Exige o emprego de filme de infravermelho sobre o código ou fundo escuro. É a tecnologia mais frágil em termos de segurança.
- Tarja Magnética – utilizada, principalmente, em segmentos bancários. As tarjas são impressas diretamente no PVC e possuem um baixo custo.
- *Smart Card* – a impressão do cartão é feita de forma direta, não permitindo seu reaproveitamento. Difícil falsificação, baixa incidência de falhas na versão sem contato e média na versão com contato.
- *Tag* - tecnologia que permite a leitura à distância e em movimento, apresentando uma incidência quase nula de falhas.
- Leitura Biométrica da Mão - permite o acesso através das características corporais e geométricas da mão do indivíduo. Tecnologia restrita a aplicações de alto nível.
- Leitura Digital - utiliza a impressão digital como parâmetro de liberação de acesso.
- Leitura de Íris - sistema que identifica as pessoas por meio dos padrões apresentados pela íris do olho humano. Tecnologia muito utilizada em áreas do governo, instituições financeiras, órgãos de saúde, internet e comércio exterior. [3]

Metodologias, práticas, instrumentos e produtos guardam analogia entre segurança empresarial e de informática. Porém a forma, intensidade e prioridades podem ser tratadas de maneiras distintas, em face às diferenças, particularmente, quanto aos riscos, contemplados pela tecnologia dos sistemas de informática [3].

3. *Smart Card*

"Por volta de 1970 surgiram pesquisas em diversos países como Alemanha, França e Japão, originando os primeiros sistemas de *Smart Card*. O primeiro progresso real no desenvolvimento dos *Smart Cards* se deu na França, em 1974, através da patente registrada por Roland Moreno" [1].

O termo ainda é ambíguo e utilizado de várias formas, porém *Smart Card*, cartão de circuito integrado ou cartão inteligente, é um cartão de plástico (PVC) contendo um microchip embutido em sua superfície, semelhante a um cartão de crédito em sua forma

e tamanho. Ele é responsável pela proteção e armazenamento de certificados digitais, utilizando sua capacidade de processamento e memória neste sistema.

Os *Smart Cards* constituem uma plataforma segura para guardar informações sensíveis, como chaves privadas, e pode ser utilizado em sistemas bancários, identificação pessoal, celulares GSM, comunicação sem fio, entre outras aplicações. Em sua arquitetura existe uma CPU de 8 bits e 4 MHz, 16 Kb de ROM, 4 Kb de EEPROM, 512 bytes de RAM e um canal de comunicação com o leitor de 9600 bps [5].

Para uma maior segurança na autenticação de usuários, o cartão é inserido em uma leitora que faz parte de um terminal ou de um computador. Em seguida, o usuário digita uma senha, a fim de impedir que outra pessoa use um cartão perdido ou roubado. “O desenvolvimento dos *Smart Cards* combinado com a expansão dos sistemas de processamento de dados eletrônicos, criou possibilidades completamente novas para planejar tais soluções” [2].

Figura 1. Leitora de Smart Card e cartão

Um dispositivo leitor de *Smart Card*, como mostra a Figura 1, é projetado para conectar um cartão inteligente a um computador, seja através de uma porta serial ou USB, ou ainda através de uma interface para o leitor de cartão de memória, quando este é on-board. Após a inserção do cartão na leitora, ela se encarregará de fazer a interface com o cartão, enquanto o computador suporta e gerencia as aplicações.

Um software de baixo nível é que suporta o canal de entrada e saída dedicado, através do qual é feita a conexão da leitora ao computador e, a partir daí, prover acesso às funcionalidades especificas da mesma.

3.1. Exemplos de Aplicações

Os *Smart Cards* são divididos em duas categorias: os cartões de memória (M*emory Cards)* e os cartões micropocessados (*Microprocessor Cards*) [2].

Os cartões de memória, *Memory Cards*, foram os primeiros a serem utilizados em larga escala pelo sistema de telefonia.Os cartões eram preparados com seus valores inseridos e armazenados eletronicamente em um *chip* que, automaticamente, iam sendo diminuído à medida em que o cartão fosse utilizado. Este tipo de cartão pode ser utilizado como moeda em transporte público, vendas de equipamentos variados, cafeterias, lojas, etc., ou seja, tinha grande utilização como “dinheiro eletrônico”. [1]

Nos cartões de memória, as informações podem ser apagadas e reescritas infinitas vezes, tornando este tipo de cartão um bem "reciclável" quando comparados aos cartões magnéticos. Seu espaço de endereçamento da memória é linear, com possíveis faixas para uso relacionado à segurança, como ilustrado na Figura 2, ficando a área de segurança responsável pelo armazenamento dos dados a serem acessados, a área

de aplicação responsável pela gravação e leitura dos dados e a área do fabricante responsável pela gravação do modo operacional do cartão, predeterminada pelo próprio fabricante.

Figura 2. Endereçamento do Smart Card lógico

Devido à sua arquitetura frágil, os cartões de memória são de fácil falsificação e, por isso vem sendo substituídos pelos cartões microprocessados, *Microprocessor Cards*, (*Smart Cards)* que devido à sua lógica de segurança, impossibilita que se apague uma pilha de memória já escrita uma vez.

Com as novas gerações de circuitos integrados, os *Smart Cards* vão evoluindo cada vez mais, dependo da arquitetura e tecnologia utilizada para sua construção. Assim, eles permitem uma maior segurança nas informações e expandem sua utilização no mercado atual, sendo utilizados não somente em sistemas bancários ou de telefonia móvel, mas em qualquer situação onde precisa-se de privacidade e praticidade no controle das informações.

4. Arquitetura de um *Smart Card*

O padrão ISO 7816 e suas derivações definem as características dos cartões de circuitos integrados, no intuito de padronizá-los internacionalmente quanto às suas características físicas, dimensão e localização dos contatos, transmissão, protocolos e sinais elétricos, formato dos comandos, registro e identificação da aplicação, robustez e funcionalidade do cartão [4].

O *chip*, principal componente do S*mart Card*, é responsável por iniciar, controlar e monitorar todas as atividades do cartão, fazendo com que o mesmo tenha relação com o mundo exterior. Isto é conseguido devido às funcionalidades de seu processador, endereçamento de dados e memórias, além de um contato I/O.

O sistema de memórias de um *Smart Card* é dividido em: ROM (*Read-Only Memory*), onde o sistema operacional é armazenado; EEPROM (*Electrically Erasable Programmable Read-Only Memory*), onde são armazenados os dados da aplicação e uma pequena quantidade de RAM (*Random Access Memory*), utilizada tanto pela aplicação quanto pelas rotinas operacionais.

A Figura 3 mostra os principais elementos da arquitetura de um *Smart Card.* São eles: unidade central de processamento (CPU), memória, entrada e saída de dados (I/O), dispositivos de interfaces (*Interface Devices – IFDs*), sistema operacional, sistema de arquivos, software e a linguagem de programação utilizada, dependendo da arquitetura

escolhida [6]. Também são apresentados os terminais de *reset* (RST), *clock* (CLK), tensão de voltagem (VCC) e aterramento (GND) que serão descritas posteriormente.

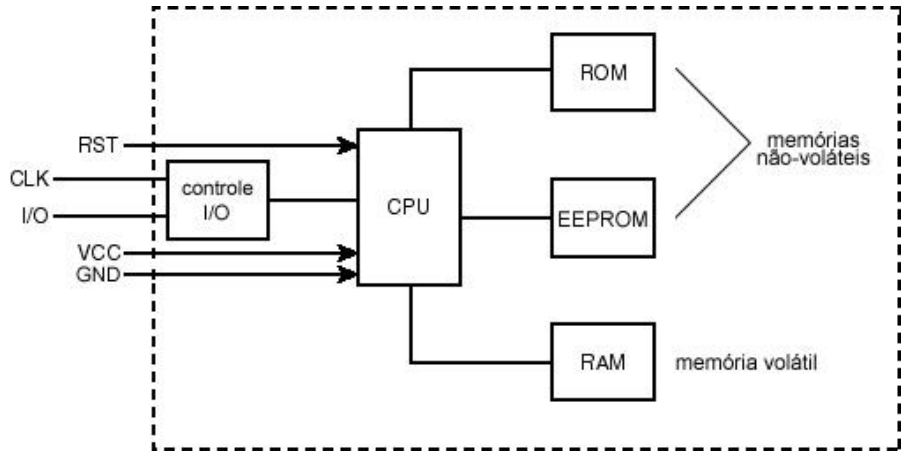

Figura 3. Elementos do Smart Card

Os processadores dos *Smart Cards* (CPU) devem ser de extrema confiança, e geralmente possuem uma arquitetura CISC (C*omplex-Instruction-Set Computer*) que significa a necessidade de vários ciclos de pulso de disparo para executar as instruções de máquina. [2]. Estes processadores têm a capacidade variando entre 6Kb a 64Kb e 8 *bits* a 32 *bits* em sua maioria [2].

Type of component or memory	**Surface area**
CPU and NPU	20%
ROM	10 %
EEPROM	45 %
RAM	15 %
Miscellaneous	10 %

Figura 4. Área de distribuição de um chip de Smart Card

As capacidades de RAM variam de 76 a 512 bytes. A Figura 4 mostra a distribuição do espaço de memória em um *Smart Card.* Uma pilha de RAM ocupa aproximadamente quatro vezes mais espaço que uma pilha de EEPROM, que, por sua vez, ocupa três vezes menos espaço que uma pilha de ROM.

A ROM de um *Smart Card*, contem a maioria das rotinas do sistema operacional, bem como as várias funções de teste e diagnóstico do mesmo. Estes programas são inseridos no *chip* pelo fabricante como uma máscara da ROM, utilizando o código do programa e processos litográficos[1]. Desta forma, os dados, que são os mesmo para todos os *chips* de determinada produção, só podem ser incorporados na ROM uma única vez, durante o processo de fabricação [2].

[1] Processos litográficos são passos da litografia, que consiste em uma técnica de gravura envolvendo a criação de marcas (desenhos) em uma matriz, com um lápis gorduroso. Esses processos utilizados são: limpeza, desenho, entintagem e impressão. [8]

EEPROM é memória permanente que permite que os dados sejam escritos e lidos sob o controle de um programa, dando a cada *chip* uma identidade original. Funcionalmente, corresponde ao disco rígido (HD) de um PC *(Personal Computer)*, uma vez que retém dados na ausência de energia e estes dados podem ser alterados como necessário.

Devido à EEPROM, os *chips* da maioria dos fabricantes são "uma vez programável", ou seja, não são regraváveis; porém, suas pilhas de memória, geralmente, são capazes de se ajustarem ao estado final da gravação. Assim, se houver uma alteração nos bits gravados, o usuário pode estar sujeito a uma violação da segurança [7].

A RAM dá forma ao espaço de funcionamento da memória a ser usado pelo processador para executar os programas. Deste modo, o processador tem o controle de leitura e gravação total da RAM [7].

4.1. Tipos de Arquiteturas

A característica de ter um circuito integrado encaixado no cartão, permitindo a transmissão, armazenamento e processamento dos dados nele contidos, faz com que estes dados sejam transmitidos usando contatos na superfície do cartão ou campos eletromagnéticos, sem nenhum contato [2].

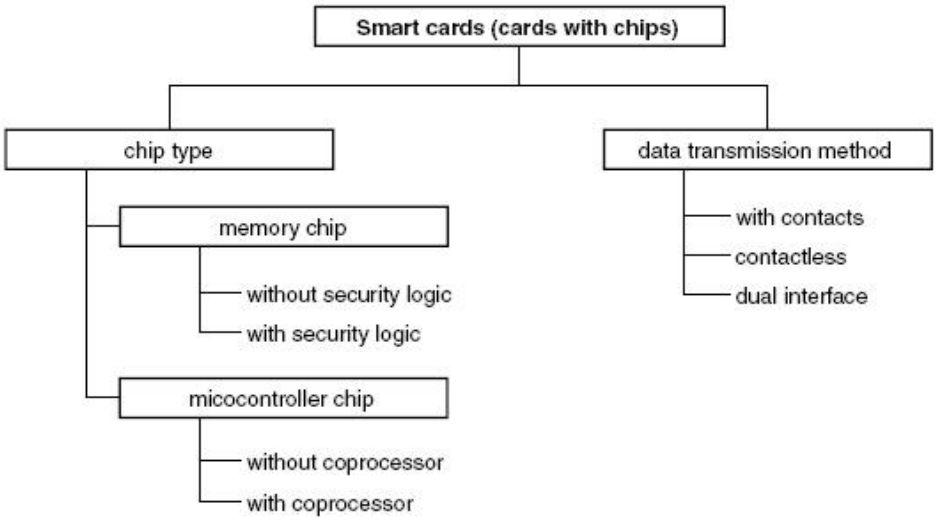

Figura 5. Classificação dos cartões quanto ao chip e meio de transmissão de dados

Assim, os *Smart Cards* são classificados quanto a sua funcionalidade e quanto à forma de conexão com a leitora, como mostra a Figura 5; podendo ser com ou sem contato físico.

4.1.1. Com contato físico

Os *Smart Cards* com contato possuem um *chip* de aproximadamente 1,27cm de diâmetro na sua parte posterior, o que faz com que seus conectores elétricos se encostem, quando inseridos numa leitora. Deste modo, as informações são lidas e

gravadas no *chip*. Estes cartões não possuem bateria, utilizando, assim, a energia fornecida pela leitora.

De acordo com o padrão ISO 7816, estes cartões possuem 8 contatos (Figura 6), mas somente 6 deles são conectados ao *chip*, localizado, geralmente, no canto superior esquerdo do cartão. Estes contatos são atribuídos às fontes de alimentação e programação (Vcc e Vpp), à terra, ao pulso de disparo, à restauração (linha de sinal inicial), e a uma ligação de comunicação I/O [9].

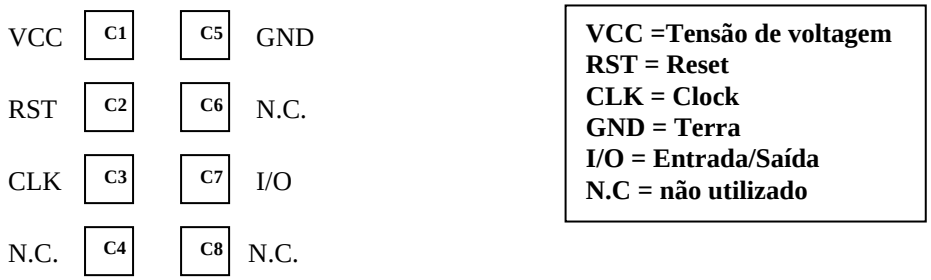

Figura 6. Contatos do cartão

Card Contact	Symbol	Function
C1	VCC	Supply Voltage
C2	RST	Reset
C3	CLK	Clock input
C4	N.C.	Not connected
C5	GND	Ground
C6	N.C.	Not connected
C7	I/O	Bidirectional data line (open drain)
C8	N.C.	Not connected

Figura 7. Descrição dos contatos, seus símbolos e funções

Como observado na Figura 6, os contatos C4 e C8 não são utilizados ultimamente, ficando reservados como contatos auxiliares, podendo ser utilizados posteriormente para relações tais como USB (*Universal Serial Bus)* [2]. O contato C6 (Vpp) também não é muito utilizado já que ele é reservado para apagar a EEPROM, submetido a uma tensão externa ao programa, o que à partir dos anos 90 passou a ser desnecessário devido à esta tensão ser aplicada diretamente no *chip* através de uma bomba de carga [7]. A Figura 7 descreve os contatos com suas respectivas funções e símbolos, para melhor entendimento.

A tensão da fonte de alimentação (Vcc), deve funcionar entre 4.75V e 5.25V com um consumo atual máximo de 200mA, geralmente variando de 3V a 5V para não ocasionar danos [7].

O sinal do pulso de disparo (CLK) oferece a velocidade das comunicações de I/O (entrada e saída) e, segundo a ISO 7816, deve variar entre 3,5MHz e 5MHz, sendo a freqüência selecionada por um protocolo específico [4].

O sinal de *reset* (RST) é utilizado para iniciar o programa contido na ROM do cartão. Este sinal controla a transferência dos endereços de entrada do cartão, quando submetido à alta tensão, com uma seqüência definida para ativá-lo e desativá-lo, minimizando, assim, a probabilidade de danos no mesmo [7].

Serial de entrada e saída (I/O) define uma única linha para a comunicação entre o cartão e a leitora. Na prática, esta linha opera no modo *half-duplex*, ficando a cargo de um protocolo de transmissão, "examinar" a necessidade do usuário [7].

4.1.2. Sem contato físico (*Contactless*)

Os *Smart Cards* sem contato físico possuem um *chip* que se comunica com a leitora através de radiofreqüência – RFID (*Radio-Frequency Identification*), variando as taxas de transmissão de 106 à 848 Kbps [7], ou utilizando uma conexão óptica. Tais cartões precisam estar próximos a uma antena para a transferência dos dados e possuem sua própria bateria. Eles não são introduzidos em um entalhe, mas sim colocados em uma posição marcada na superfície do leitor de cartão.

Além da radiofreqüência e da transmissão óptica, existem outras técnicas, também, para transmissão de dados e energias neste tipo de cartão; tais como microondas e acoplamentos capacitativo e indutivo (mais utilizados em cartões sem fonte de alimentação interna) [2].

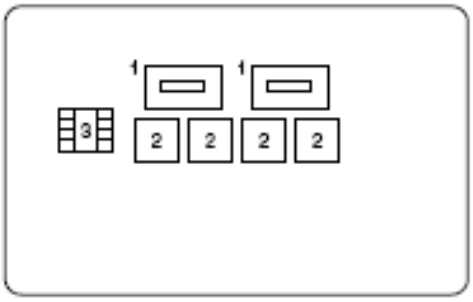

Figura 8. Componentes de um cartão *contactless*

Como não era possível concordar os padrões de acoplamentos capacitativo e indutivo, atualmente eles são definidos de maneira que ambos possam ser executados em um único cartão ou terminal, diferenciando apenas na distância entre o cartão e a leitora. Os componentes de sua arquitetura são mostrados na Figura 8 e descritos como: (1) acoplamentos (indutivo) dos componentes do cartão e (2) acoplamento capacitativo do cartão e (3) contatos do *chip* [2].

A comunicação entre o cartão e o leitor (que também serve como gravador do cartão) se faz com as seguintes funções: transferência de energia, sinal do pulso de disparo e transferência dos dados. Seu baixo consumo de energia e memória, restringem também a distância entre o cartão e o terminal.

A energia é transferida, passivamente, por um campo magnético com uma freqüência de 4.9152MHz, passando através das superfícies do acoplamento indutivo. A tensão induzida no cartão é proporcional ao sinal de pulso de disparo [2]. Esta energia é utilizada pelo *chip* para a transferência de dados.

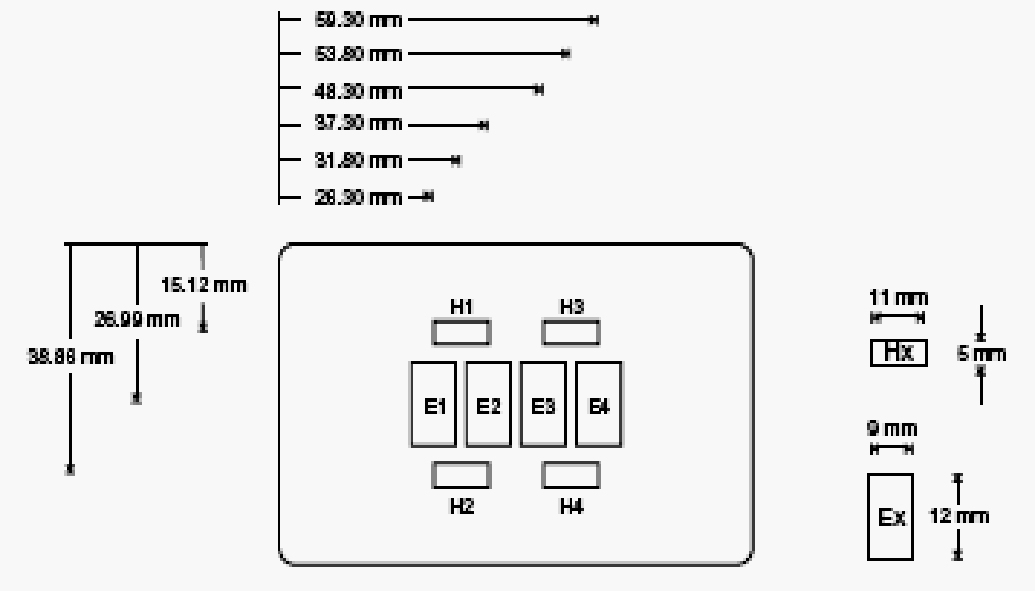

Figura 9. Localização dos acoplamentos no terminal

Tipos diferentes de modulação são usados para a transmissão de dados nos dois sentidos cartão-terminal. Para a transmissão de dados do cartão ao terminal, um carreador, usa uma modulação de carga com uma variação de pelo menos 10% (ver figura 10). A modulação dos dados é conseguida comutando a fase do carreador e produzindo estados bifásicos que podem ser interpretados como a lógica 0 e 1. O estado inicial, depois que o campo magnético foi estabelecido, é definido como 1 e permanece estável por um tempo determinado. Após este estado inicial, cada deslocamento de fase do carreador representa a reversão do estado da lógica para 0 [2].

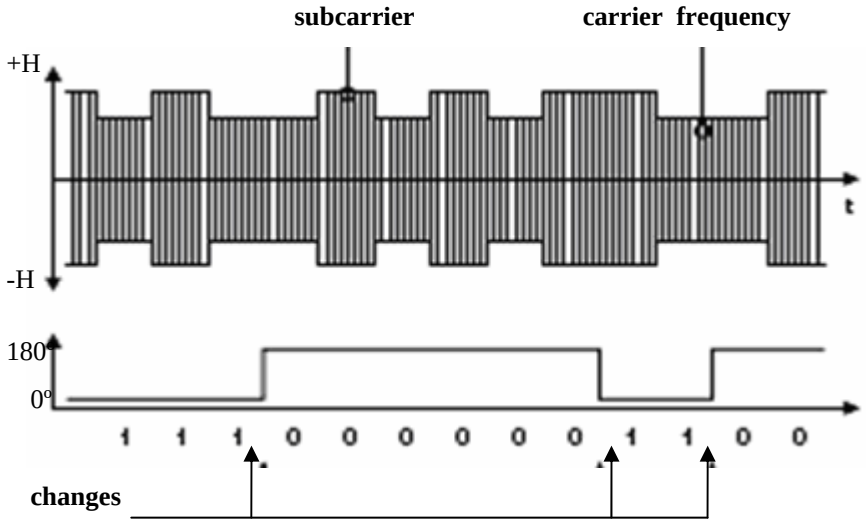

Figura 10. Princípios de modulação da transmissão de dados

A transmissão de dados do terminal para o cartão se faz alternando os campos magnéticos que passam através das superfícies H1 do acoplamento com H4 (ver Figura 9), usando uma fase de modulação e produzindo estados bifásicos. Desde que o cartão trabalhe em todas as quatro orientações ao terminal, o estado inicial é interpretado como a lógica 1, passando para 0, posteriormente [2].

Para a transmissão capacitativa de dados do cartão ao terminal, um par de superfícies do acoplamento é usado para um sentido e outro par pode ser usado para a transmissão de dados no sentido oposto. A diferença de potencial máxima entre um par de superfícies do acoplamento é limitada a 10V [2]. Se o cartão emitir um sinal de resposta à restauração, o terminal é capaz de reconhecer a orientação relativa do cartão.

A complexidade estrutural do cartão sem contato físico, resulta em seu custo elevado, tornando-o pouco competitivo no mercado atual; porém, a liberdade do usuário e redução das limitações simplifica o uso destes cartões e aumenta a sua aceitação.

4.2. Comparativo entre Arquiteturas

As diversas arquiteturas, muito utilizadas ultimamente pela tecnologia S*mart Card* sofrem distinções entre si, o que faz com que cada uma seja mais eficiente para determinada aplicação (ver Figura 11).

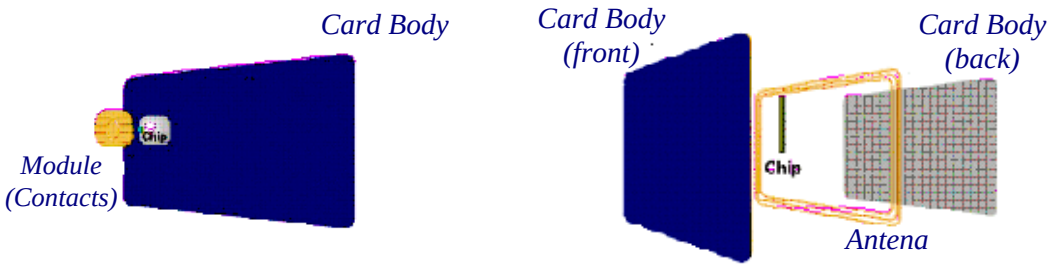

Figura 11. Arquitetura com contato *versus* sem contato

"Os *Memory Cards* tem suas funcionalidades limitadas. Mas sua capacidade de prover a segurança lógica das informações é suficiente para protegê-las de acessos e manipulações não autorizadas" [1]. Eles são uma ótima solução em relação à segurança e baixo custo; porém suas funcionalidades, personalizadas para cada aplicação, restringem sua flexibilidade.

O *Smart Card* microprocessado, ou "programável", com contato, tem suas funcionalidades restritas apenas ao espaço de armazenamento e capacidade do processador, tornando somente tecnológicos os limites impostos à implementação dos sistemas. Sendo assim, as vantagens são grandes, destacando-se uma maior capacidade de armazenamento e segurança dos dados, devido à utilização de criptografia, e a possibilidade de execução de várias aplicações em um mesmo cartão, de acordo com sua programação.

Pode-se comparar a estrutura de um *Smart Card* com contato com a estrutura lógica de funcionamento de um computador, devido aos componentes utilizados, mas com recursos muito limitados [1]. Isto, além do baixo custo, faz com que seja, cada vez mais crescente, a sua utilização e potencializa a tecnologia destes cartões.

Como os S*mart Cards* sem contato, ou sem fio, possuem internamente a mesma estrutura lógica de funcionamento de um *Smart Card* com contato ou um *Memory Card*,a diferença está em uma interface física, adicionada à sua estrutura, que faz com que haja comunicação através de radiofreqüência (RF), não necessitando de qualquer contato físico entre o cartão e a leitora para a transmissão de dados e energia.

Estes *Smart Cards* sem contato, que possuem um circuito complexo, necessitam de mais irradiação do sinal para o seu funcionamento. Já os *Memory Cards* e os *Smart Cards* com contato, operam a uma distância de alguns centímetros, devido a menor complexidade do circuito e a baixa intensidade do sinal necessária para sua operação. Assim, as aplicações que utilizam o *Smart Card* a uma longa distância, como os *Smart Cards* sem contato físico, podem ocasionar problemas, como o acesso indevido, facilitado por interferências durante a transmissão dos dados.

Como estes cartões podem ser utilizados a uma grande distância, não sendo necessário segura-lo nas mãos para sua utilização, sua segurança fica abalada, causando falhas na autenticação, pois um outro usuário pode manipula-lo sem o conhecimento do possuidor do cartão. Neste sentido, o cartão com contato será sempre mais confiável, tornando uma exceção o desgaste anormal do *chip*.

Uma vantagem significativa dos cartões sem contato em relação aos cartões de contato é o fato de ele sofrer menos degradação e falhas na comunicação devido a mau contato, uso excessivo ou exposição ao ambiente. Outra vantagem é o aspecto visual, tornando sua utilização uma solução muito elegante, já que nenhum componente é visível no cartão, como os contatos elétricos [1].

Em ambos os casos, com ou sem contato, o desempenho está relacionado à transferência dos dados e velocidade do pulso de disparo [2]. Contudo, a complexidade do sistema sem contato, aumenta significativamente os custos do próprio cartão e dos leitores, que precisam reconhecer os diferentes padrões utilizados por sua comunicação.

5. Aplicação Proposta

A aplicação proposta tem como objetivo exemplificar a utilização do *Smart Card*, com contato físico, na identificação e autenticação de usuários.

5.1. Arquitetura Escolhida

"A segurança dos *Smart Cards* depende muito de microcontroladores especiais e algoritmos inclusos nos sistemas operacionais" [1].

Assim que os *Smart Cards* são fabricados e seus *chips* inseridos neles, são instalados também, algum programa ou arquivo, antes de serem comercializados. Já em posse do usuário, eles passam pelo processo de personalização e impressão do cartão.

Durante a personalização, que envolve a manipulação física do cartão, ocorre o processo de gravação dos dados que serão validados por ele, bem como sua identificação na memória. Após este procedimento, se dá a impressão gráfica e textual do cartão para depois serem executados os programas que irão rodar no cartão e ele estar disponível ao usuário final [10].

Todos estes procedimentos fazem o *Smart Card* ser de grande utilidade, processamento e segurança das informações. Sua confiabilidade, durabilidade e baixo custo, popularizam ainda mais sua utilização. A facilidade com que os cartões são gravados, dependendo somente da leitora, e a baixa interferência na transmissão dos dados também são fatores que contribuíram com a escolha da arquitetura com contato físico.

5.2. Aplicação de Exemplo

Como a segurança da informação é um problema atual em diversos setores, garantir sua autenticidade e controle tornou-se difícil para várias empresas. Como exemplo, pretende-se demonstrar que, em uma empresa onde trabalham motoristas, precisa-se

garantir que estes motoristas estejam realmente habilitados para dirigir veículos específicos, bem como o horário em que entram e saem do veículo, a trajetória que percorrem, etc.

Um cadastro de todos os dados dos motoristas como nome, código dentro da empresa, endereço, telefone, data de admissão, RG, CPF, número da carteira de habilitação com categoria permitida e data de validade, é necessário para garantir que determinado motorista seja responsável por cada veículo específico. Com isto, será implementado um sistema de segurança que identifique estes motoristas e seus respectivos veículos.

Quando o motorista entrar no veículo, ele terá que "inserir" seu cartão no tacógrafo digital existente no veículo, certificando, assim, todas as suas informações através dos dados gravados no *Smart Card*, inclusive se sua carteira tem permissão para dirigir o veículo desejado, identificando se as categorias de ambos são compatíveis e se a habilitação do condutor não se encontra vencida. Ele deverá ainda informar sua senha de acesso, garantindo assim que um motorista não utilize o cartão de outro facilmente.

A partir daí é dada a partida no veículo, responsabilizando totalmente o motorista por quaisquer atividades ou eventualidades com o mesmo e minimizando a possibilidade de furto do veículo, já que este só será ligado a partir do momento que um *Smart Card* tiver sido validado.

Com esta aplicação de exemplo, pretende-se mostrar que os *Smart Card* com sua arquitetura bem elaborada e portabilidade são dispositivos seguros, com um custo relativamente baixo, e podem ser usados para qualquer tipo de certificação digital, das mais complexas às mais simples.

6. Modelagem da Aplicação

A fase de engenharia de software serve para introduzir as metodologias aplicadas ao desenvolvimento do software com o objetivo de reduzir custo e tempo de desenvolvimento, possibilitar melhor gerência do processo de desenvolvimento, facilitar o trabalho em equipe e aumentar a qualidade do software. Assim, para desenvolver um software de qualidade, seguro, que satisfaça ao propósito pretendido de forma rápida, eficiente e efetiva, é de fundamental importância a sua modelagem.

A UML (*Unified Modeling Language)*, ou Linguagem Unificada de Modelagem, é uma linguagem gráfica para visualização, especificação, construção e documentação de artefatos de sistemas complexos de software [11]. Ela padroniza a arquitetura de projetos de sistemas como processos de negócios e funções do sistema, bem como as classes escritas em determinada linguagem de programação, banco de dados e os componentes de softwares reutilizáveis.

Entretanto, devido à simplicidade do código e implementação do sistema proposto, não é necessário desenvolver todas as fases de modelagem da engenharia de software. Estão registradas, porém, as de maior relevância como o diagrama de caso de uso e sua descrição, assim como o diagrama de implantação e de componentes.

De acordo com o levantamento de requisitos, o sistema deverá cadastrar empresa, motoristas e veículos, bem como permitir a gravação e leitura dos *smart cards*, com validação dos dados e autenticação do usuário através de uma senha de acesso. Tudo isto com uma boa velocidade de processamento para uma resposta rápida de interação com o usuário.

Nos diagramas de implantação e componentes, são abordados os hardwares utilizados (leitora/gravadora, *Smart Card*, tacógrafo digital e computador) e suas relações físicas e lógicas, como mostra a Figura 12.

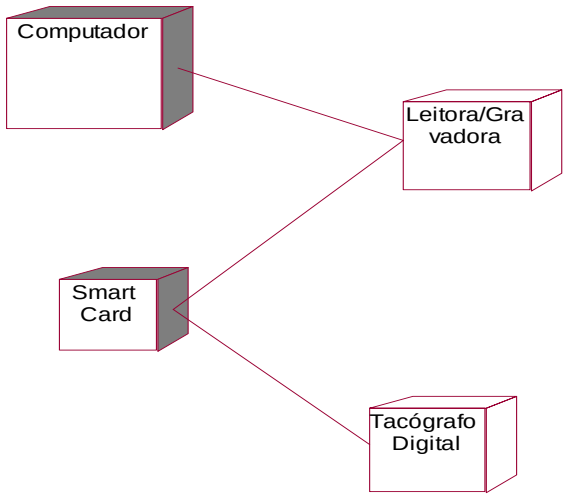

Figura 12. Diagrama de Implantação

Para complementar, também está documentada a modelagem conceitual (Figura 13) e lógica do banco de dados a ser implementado, contendo três tabelas como as que seguem na Tabela 1.

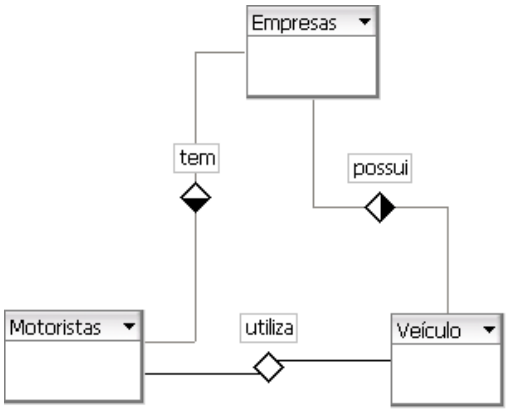

Figura 13. DER do Banco de Dados

Tabela 1. Modelo Lógico do Banco de Dados

Empresas (@codempresas, nome, razaosocial, endereço, bairro, cidade, estado, cep, cnpj, ie, email, homepage, telefone, responsável)
Motoristas (@codmotorista, codempresas, nome, endereço, bairro, cidade, estado, dep, rg, cpf, email, telefone, dat_nasc, dat_admissao, numerocnh, tipocnh, validadecnh, senha)
Veículo (@placa, codempresas, modelo, marca, cnhpermitida, senha)

7. Prototipação e Desenvolvimento da Aplicação

A fase de prototipação documenta toda a estruturação dos dados, atributos e construção dos algoritmos utilizados no desenvolvimento da aplicação, além da fase de testes, com alguns cadastros.

Para a criação do Banco de Dados foi utilizada a ferramenta Firebird 1.5, que é um completo SGDB (Sistema de Gerenciamento de Banco de Dados), permitindo criar, recuperar, executar comandos e *scripts* SQL, efetuar *backups* e *restores*, etc. [12]

Depois de criadas as tabelas e relacionamentos do Banco de Dados, deu-se prosseguimento à implementação da aplicação, utilizando o *Delphi* como linguagem de programação. Nele foram feitas as interfaces de cadastro dos dados da empresa, motoristas e veículos, bem como a interface de leitura e gravação do cartão e a interface de testes e validação do cartão.

Após a criação do código da aplicação, este será transferido, *byte* a *byte*, para a leitora/ gravadora, através de uma porta que conecta o computador diretamente a ela. Desta forma, as informações serão retransmitidas ao cartão, através de gravação, por contato físico, ao processador do *Smart Card*, que armazenará todos os dados a serem validados pelo tacógrafo.

O processo de testes e validação consiste no reconhecimento dos dados armazenados no cartão, através de uma senha de acesso, pelo tacógrafo digital. Este já vem gravado de fábrica, não tendo qualquer ligação com a aplicação desenvolvida.

Com a inserção do cartão no tacógrafo digital, será requisitada a digitação da senha que, se confirmada e validada, liberará o veículo para utilização do usuário. Caso contrário, o veículo não dá a partida e impede o usuário de guiá-lo.

8. Conclusões e Trabalhos Futuros

De acordo com a pesquisa bibliográfica e os testes da aplicação, conclui-se que os *Smart Card* são viáveis para utilização em sistemas de validação e autenticação do usuário, principalmente os com contato físico, uma vez que sofrem menos interferências e possuem um custo mais acessível às empresas.

No caso de empresas que querem controlar seus motoristas através dos cartões processados, sua utilização é bem eficaz pois além de identificar quem estará utilizando o veículo, o cartão juntamente com o tacógrafo digital, consegue armazenar o consumo de combustível, mostrando qual motorista é mais econômico, controla o excesso de velocidade do veículo e as rotações por minuto, auxiliando na manutenção. Tudo isto sem levar em conta que o uso do tacógrafo nessas empresas é obrigatório.

Os *Smart Cards* também são bem eficientes como sistemas de segurança em outras aplicações que exigem portabilidade, sendo uma opção aos cartões magnéticos e outros sistemas de segurança.

Com o constante crescimento da linguagem *Java*, outra opção seria o *Java Card*, onde podem ser executados *applets* desenvolvidos numa versão limitada do *Java.* As especificações da SUN para esta tecnologia, defininem um subconjunto de comandos e uma maquina virtual para *Java Cards*, o funcionamento dos cartões em tempo de execução e a estrutura principal das extensões, classes e *packages* para este tipo de aplicação.[13] Assim, fica como sugestão para trabalho futuro o aprimoramento desta aplicação utilizando *Java Card.*

9. Referencias Bibliográficas

[1] LORENZONI, A. F.. *Smart card – Java card.* 2006. 87p. Monografia (Bacharelado em Ciência da Computação). Instituto de Ciências Exatas e Tecnológicas. Centro Universitário Feevale.

[2] WOLFGANG, R.; WOLFGANG, E.. ***Smart card handbook***. 3 ed. Munich: Carl Hanser Verlag, 2002.

[3] GIL, A. de L.. ***Segurança em informática***. 2 ed. São Paulo: Atlas, 1998.

[4] CARDWERK S. M.. The ISO 7816 Smart Card Standard: Overview. Disponível em http://www.cardwerk.com/smartcards/smartcard_standard_ISO7816.aspx. Acesso em 25 de abr. 2007.

[5] TANENBAUM, A. S.. ***Sistemas operacionais modernos***. 2 ed. São Paulo: Prentice Hall, 2003.

[6] HOWSTUFFWORKS. What is a "smart card"? Disponível em http://computer.howstuffworks.com/question332.htm. Acesso em 02 de mai. 2007.

[7] SMART CARD TUTORIAL. Introduction to smart cards. Disponível em http://www.smartcard.co.uk/tutorials/sct-itsc.pdf. Acesso em 12 de mai 2007.

[8] WIKIPEDIA. Litografia. Disponível em http://pt.wikipedia.org/wiki/Litografia. Acesso em 22 de jul 2007.

[9] NACCACHE, D.; M'RAIHI, D.. *Cryptographic smart cards*. 1996. 14p. Artigo Cryptography Department. Gemplus PSI.

[10] GTA - UFRJ. Smart Card e E-Tag. Disponível em http://www.gta.ufrj.br/grad/04_2/smartcard. Acesso em 20 de mai. 2007.

[11] BOOCH, Grady; RUMBAUGH, James; JACOBSON, Ivar. **UML guia do usuário.** 2 ed. Rio de Janeiro: Elsevier, 2005.

[12] CANTU, Carlos H. Conheça o Firebird. Disponível em http://www.firebirdnews.org/docs/fb2min_ptbr.html . Acesso em 10 de set. 2007.

[13] ARIZA, César. *JavaCards*. 2005. 16p. Dissertação (Mestrado em Sistemas de Informação). Departamento de Sistemas de Informação. Universidade do Minho.