UNIVERSIDADE REGIONAL DE BLUMENAU

CENTRO DE CIÊNCIAS EXATAS E NATURAIS

CURSO DE SISTEMAS DE INFORMAÇÃO – BACHARELADO

PROTÓTIPO DE UM SISTEMA ÚNICO DE IDENTIFICAÇÃO PESSOAL BASEADO EM TECNOLOGIA RFID

MARLEI RUTE GRUCHINSKI

BLUMENAU
2007

2007/I-14

MARLEI RUTE GRUCHINSKI

PROTÓTIPO DE UM SISTEMA ÚNICO DE IDENTIFICAÇÃO PESSOAL BASEADO EM TECNOLOGIA RFID

Trabalho de Conclusão de Curso submetido à Universidade Regional de Blumenau para a obtenção dos créditos na disciplina Trabalho de Conclusão de Curso II do curso de Sistemas de Informação - Bacharelado.

Prof. Francisco Adell Péricas, Mestre - Orientador

BLUMENAU
2007

2007/1-14

PROTÓTIPO DE UM SISTEMA ÚNICO DE IDENTIFICAÇÃO PESSOAL BASEADO EM TECNOLOGIA RFID

Por

MARLEI RUTE GRUCHINSKI

Trabalho aprovado para obtenção dos créditos na disciplina de Trabalho de Conclusão de Curso II, pela banca examinadora formada por:

Presidente:	Prof. Francisco Adell Péricas, Mestre – Orientador, FURB
Membro:	Prof. Miguel Alexandre Wisintainer, Mestre – FURB
Membro:	Prof. Oscar Dalfovo, Doutor – FURB

Blumenau, Junho 2007

Dedico este trabalho as familiares pelo apoio e confiança que depositaram em mim, aos amigos que me apoiaram não só durante o desenvolvimento deste trabalho, mas durante todo o período acadêmico, especialmente aqueles que me ajudaram diretamente na realização deste.

AGRADECIMENTOS

Meu primeiro e mais importante agradecimento, é a Deus por ter me dado a oportunidade de estar aqui.

Agradeço aos meus pais, Anna e Egon e ao meu irmão Daniel, que mesmo estando distantes, sempre estiveram do meu lado me apoiando não só na execução deste trabalho mas em todos os momentos necessários.

Ao meu namorado Gilbran pela compreensão dos momentos em que estive ausente para a realização deste trabalho e por me ouvir nas situações de desespero.

Aos meus amigos Jefferson, Ieda, Odair, Rubens, Rodrigo S., Roger e Thaiana pelos empurrões e cobranças, e por serem amigos que ficarão para a vida toda.

As pessoas que me ajudaram a tornar este trabalho uma realidade, Denis, Omar, Rodrigo D. e Sr. Werner Keske cada uma com os seus conhecimentos.

A empresa WK Sistemas pelo empréstimo dos equipamentos nos instantes finais.

Ao meu orientador, Francisco Adell Péricas por ter acreditado neste trabalho mesmo quando tudo parecia perdido.

Ao meu Tio Vilson e minha Tia Rosemeri, que me deram casa e uma segunda família, apoio nos momentos de dificuldade e o principal empurrão para que eu estivesse aqui hoje.

Enfim, a todos aqueles que torceram e ainda torcem por mim.

Jamais esqueças que tua própria decisão de alcançar o sucesso é mais importante do que qualquer outra coisa.

Albert Einstein

RESUMO

Registro Geral, Cadastro Nacional de Pessoa Física, Carteira de Motorista, Título de Eleitor. estes são alguns dos documentos que qualquer cidadão precisa possuir para que possa ser identificado em qualquer situação. Isso implica em estar com todos eles ao alcance, ou seja, na carteira. O presente trabalho é o desenvolvimento de um sistema de documentação de informações pessoais utilizando RFID como um documento único. Em um único documento, ter todas estas informações, que hoje encontram-se em papel e sem vínculo algum. Este documento único é um cartão de *SmartCard*, que utiliza a tecnologia de Comunicação por Rádio Freqüência (RFID). Este cartão possui um código de identificação, e é esta seqüência de número que será a responsável por identificar cada pessoa, na base de dados onde estarão cadastrados todos os documentos e outras informações úteis.

Palavras-chave: Documentos. RFID. *SmartCard*.

ABSTRACT

Identity card, Security ID Number, Driver’s licence and Voter's card. These are some documents that any citizen needs to use to be identified in any situation. That implies in be with all of them in the hands, that is, in the wallet. The present work intends the development of a personal documentation information system using RFID as an only document. In an only document, have all these information that today are in paper, and without any link. This only document is a SmartCard, that uses the Radio Frequency IDentification (RFID). This card use an identification code, and this sequencial number will be the responsible for identifying each person, in the data base will be registered all the documents and other useful information.

Keywords: Documents, cards, RFID. SmartCard.

LISTA DE ILUSTRAÇÕES

LISTA DE SIGLAS

CNH – Carteira Nacional de Habilitação

CNPq – Conselho Nacional de Desenvolvimento Científico e Tecnológico

CPF – Cadastro Nacional de Pessoa Física

CRC – *Cyclic redundancy Check*

DLL – *Dynamic Link Library*

DoS – *Denial Of Service*

EAN Brasil – Associação Brasileira de Automação

EPC – Código Eletrônico de Produto

EPC – *Electronic Product Code*

FDA – *Food and Drug Administration*

FDX – *Full Duplex*

GPS – *Global Positioning System*

HDX – *Half Duplex*

ID – Identificador

IDC – Instituto de Desenvolvimento Cultural

InCor - Instituto do Coração

ISO – União Internacional das Instituições Nacionais de Padronizações

MIT – *Massachusetts Institute of Technology*

ODBC – *Open Data Base Connectivity*

ONS – *Object Naming Service*

PDA – *Personal Digital Assistant*

RAF – *Royal Air Force*

RFID - *Radio Frequency Identificantion*

RG – Registro Geral

SEQ – Comunicação Seqüencial

SUIP – Sistema Único de Identificação Pessoal

UML – *Unified Modeling Language*

USP – Universidade de São Paulo

SUMÁRIO

1 INTRODUÇÃO

Nada mais incômodo do que chegar a determinado local e ter que apresentar uma série de documentos, tirando da carteira um monte de papéis, número do Registro Geral (RG), número do Cadastro de Pessoa Física (CPF), número do Título de Eleitor, confirmação do voto nas últimas eleições, Carteira Nacional de Habilitação (CNH) e tudo isso só para comprovar que você é você mesmo. E ainda há outras informações, como tipo sangüíneo, pontuação da carteira de motorista que uma pessoa possui. Enfim, são muitos os registros e armazená-los todos na memória é extremamente complexo. Atualmente não existe nenhum tipo de integração entre estes documentos, o que causa muitas vezes duplicidade de dados.

Então surge uma questão: por quê não unir todos estes documentos pessoais em um único? Um documento único deveria, além de identificar o proprietário informando seu nome, data e local de nascimento, permitir o acesso a um detalhamento completo sobre a sua vida. Alguns exemplos seriam passagens pela polícia, pontuações na Carteira Nacional de Habilitação (CNH) com o histórico detalhado das infrações cometidas, algumas informações médicas, como possíveis doenças, tipagem sanguínea, uso de remédios controlados, enfim, um “mundo” de informações. Ou seja, criar uma base de dados que armazenaria todas estas informações e que seria alimentada por órgãos e instituições que de alguma forma fazem parte da vida das pessoas, como por exemplo a Secretaria da Receita Federal do Brasil com o CPF e o Tribunal Superior Eleitoral com o título de eleitor.

A idéia de armazenar informações pessoais em um banco de dados, já possui uma semente: o Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq) vem desenvolvendo juntamente com o Instituto do Coração (InCor) e a Universidade de São Paulo (USP) um projeto chamado MobMed, onde a idéia é, usando dispositivos móveis (*Personal Digital Assistants* - PDAs), permitir que um médico tenha acesso ao Prontuário Eletrônico do Paciente em qualquer lugar. O Prontuário Eletrônico seria, segundo MedAlliance (2002), um repositório de dados clínicos e demográficos que centraliza todas as informações sobre a saúde do paciente, com total segurança e sigilo em um banco de dados.

Com a proposta que está sendo apresentada, pretende-se a criação de um banco de dados que armazene todas as informações citadas até o presente momento. A forma de acesso a este banco se dará pelo uso de um cartão de *SmartCard* com a Tecnologia de *Radio Frequency Identificantion* - Identificação por Rádio Freqüência (RFID).

1.1 OBJETIVOS DO TRABALHO

O objetivo geral é o desenvolvimento de um sistema de documentação de informações pessoais utilizando a tecnologia de RFID, unificando informações constantes em documentos exigidos em nível nacional, incluindo também dados médicos e policiais.

Os objetivos específicos do trabalho são:

a) identificar as informações pessoais, medicas e policiais que serão armazenadas no banco de dados;
b) disponibilizar um sistema de gerenciamento das informações para acessar o banco de dados, restrito aos médicos o acesso ao prontuário médico e aos policiais acesso à ficha policial para auxilia-los as devidas investigações nas delegacias e nos postos policiais;
c) identificar as informações para o gerenciamento do acesso às informações, disponibilizando-os nos diferentes órgãos públicos e privados;
d) disponibilizar, através de um leitor de SmartCard baseado em RFID, o acesso ao conteúdo do documento. Através de um leitor de SmartCard baseado em RFID, possibilitar o acesso ao conteúdo que fica armazenado na base de dados informações médicas e informações policiais, observando para isso os direitos de acesso de cada usuário.

1.2 ESTRUTURA DO TRABALHO

No capítulo um é apresentada uma introdução ao tema abordado, bem como os objetivos que foram traçados para o trabalho.

No capítulo dois é mostrado um estudo sobre a tecnologia RFID, suas vantagens, desvantagens, segurança e equipamentos.

Já no capítulo três são mostrados os aspectos técnicos referentes ao desenvolvimento do trabalho, descrevendo a especificação e a implementação do aplicativo. Também são abordadas algumas características do software desenvolvido, baseadas nos conceitos já apresentados no capítulo dois.

No capítulo quatro são descritos os testes realizados com a aplicação.

Por fim, no capítulo cinco são descritas as conclusões e dificuldades encontradas na confecção do software, bem como sugestões para futuras pesquisas nesta área.

2 FUNDAMENTAÇÃO TEÓRICA

Este capítulo apresenta informações sobre a Tecnologia de RFID e sobre alguns trabalhos correlatos.

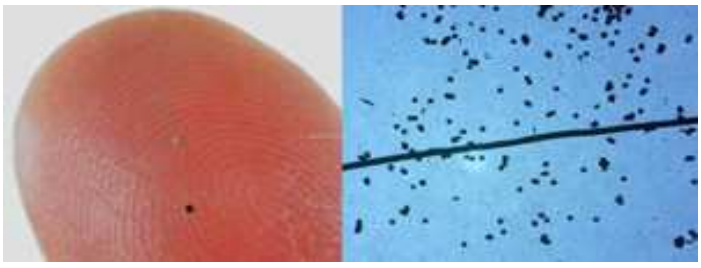
2.1 RADIO FREQUENCY IDENTIFICATION

Na década de 1980, o Massachusetts Institute of Technology (MIT), junto com outros centros, iniciou uma pesquisa sobre uma arquitetura que pudesse utilizar os recursos das tecnologias baseadas em radiofreqüência para servir de base para o desenvolvimento de novas tecnologias para rastrear e localizar produtos. Com isso nasceu o Código Eletrônico de Produtos - *Electronic Product Code* (EPC) que mais tarde recebeu o nome de *Radio Frequency Identification* (RFID) (PINHEIRO, 2004).

A solução é descendente da tecnologia dos *transponders* que foram utilizados pelos ingleses na 2º Guerra Mundial. Nesta ocasião, esta tecnologia identificava os aviões da *Royal Air Force* (RAF – Força Aérea Real). Assim, quando uma aeronave surgia no radar e não respondia com seu *transponder*, ela era identificada como inimiga e abatida (LOES, 2006).

Com o passar dos anos, a evolução tecnológica e os esforços de grupos de industriais geraram uma tecnologia capaz de gravar uma seqüência numérica de 96 bits – em breve, 128 bits – em um chip dez vezes menor que uma formiga. A dimensão atual permite que o componente seja inserido em etiquetas aplicadas a uma infinidade de produtos, dando origem ao termo ‘etiqueta inteligente’ (BRAUN, 2006).

Para uma idéia da atual dimensão dos chips, a Hitachi criou uma etiqueta que pode ser a menor do mundo. O dispositivo mede certa de 0,05 x 0,05 mm, sem antena.



Fonte: TechGuru

Figura 01: Etiqueta RFID.

Basicamente, a tecnologia do RFID consiste em uma comunicação por radiofreqüência, sem fios, que transmite dados de um dispositivo móvel para um leitor (SANTINI, 2006).

Várias empresas já aderiram ao uso da tecnologia RFID. A empresa *Delta Air Lines* está testando em alguns vôos *Tags* de RFID nas malas dos passageiros procurando reduzir as perdas e facilitar o itinerário das bagagens caso ocorram mudanças na rota de vôo. Outro exemplo são alguns pedágios dos Estados Unidos, onde foram implantados os chamados *EZpass*. Ao invés dos carros pararem, um cartão que está equipado com um *microchip* RFID recebe e responde a sinais de rádio das antenas ou leitores que estão colocados sobre as cabines, enviando seu número de identificação. Uma vez que o número é reconhecido, a passagem é liberada. As *Tags* são adquiridas mediante um depósito, e este valor é debitado toda vez que o carro passar por um pedágio (PORTAL AUTOMAÇÃO, 2004).

A área da Saúde também já está aderindo à tecnologia do RFID. Segundo Inovação Tecnológica (2004), o *Food and Drug Administration* (FDA), o Ministério da Saúde dos Estados Unidos, liberou a utilização de *microchips* implantáveis em seres humanos para fins médicos. Este *bio-chip* é um *microtransponder* baseado na tecnologia RFID. O sistema completo que foi apresentado inclui além do chip, um aplicador, responsável pela inserção do aparelho na pele do paciente, um leitor dos sinais emitidos pelo *bio-chip,* e uma base de dados segura para armazenar as informações médicas.

No início do ano de 2006, existiam no Brasil quarenta e duas famílias usando o chip subcutâneo. Estão na fila de espera onze mil famílias interessadas em colocar o chip. O motivo da procura é o medo da violência. Existem dois tipos de *chip* subcutâneos. O primeiro, conhecido como passivo, guarda informações e dados pessoais, normalmente usados para guardar dados médicos e para identificar, por exemplo, pacientes cardíacos e com Mal de Alzheimer assim que eles entram no hospital. Mas para isso, o hospital precisa estar equipado para realizar a leitura das informações destes *chips*. O segundo modelo é chamado ativo, e é usado para monitorar movimentos de pessoas. Neste caso, utiliza-se também a tecnologia de localização por satélite *Global Positioning System (*GPS) para fazer o rastreamento. No momento do implante, o usuário define uma região por onde pode circular, caso a pessoa saia desta região sem avisar à base de monitoramento ou os familiares, começa o processo de busca (SCHNOOR, 2006).

No Japão, o chip está sendo usado para substituir a velha lista de presença. Uma escola do ensino fundamental implantou no final de 2004 uma etiqueta eletrônica que utiliza RFID. Quando o aluno passa pelo portão da escola, um sensor detecta a entrada, identifica o aluno e

envia um e-mail para o celular dos pais avisando que o filho entrou na escola (SCHNOOR, 2006).

Portal da Automação (2004) também cita a idéia de colocar uma *Tag* RFID em todos os documentos importantes, ou seja, um chip na carteira de motorista, no passaporte, diplomas universitários, certidões de nascimento, etc. Diferentemente, a idéia aqui proposta sugere um único *transponder* unindo todos os documentos que são necessários para que uma pessoa possa ser reconhecida como cidadã.

2.2 COMO FUNCIONA O RFID

Diferente do feixe de luz utilizado no sistema de código de barras para captura de dados, esta tecnologia utiliza a freqüência de rádio.

Os equipamentos que compõem uma arquitetura de RFID são os seguintes: a antena e o *transceiver* que quando estão juntos, ou seja, no mesmo equipamento, recebem o nome de Leitor, e o *transponder* (também chamado de RF *Tag* ou somente *Tag*) que é composto pela antena e pelo *microchip*.

2.3 LEITORES

Segundo Pinheiro (2004), a antena é a responsável por ativar a *Tag* para que possa haver a troca/envio de informações, e para isso ela envia um sinal de rádio. São dos mais diversos formatos e tamanhos, cada uma com sua configuração e característica distinta para um determinado tipo de aplicação. Algumas antenas são acopladas ao *transceiver* e ao decodificador em um mesmo invólucro: neste caso recebem o nome de leitor.

O leitor (Figura 02), que nada mais é do que uma antena, por intermédio do *transponder*, emite as freqüências de rádio, podendo atingir alguns centímetros ou até metros, dependendo da potência de saída e da freqüência de rádio que está sendo utilizada. Este sinal enviado pela antena ativa o *Tag* realizando assim, a leitura ou a gravação dos dados na mesma (WIKIPEDIA, 2007).

Fonte: HidCorp

Figura 02: Leitor de RFID

Quanto à conexão e função em relação ao restante do sistema, o RFID não é muito diferente do leitor de código de barras. A diferença entre eles é que o leitor de RFID não precisa estar na frente do produto para que a leitura possa ser realizada, pois a leitura pode ser feita através de vários tipos de materiais, uma vez que as ondas emitidas pela antena se propagam em diversas direções e distâncias. Quando uma *Tag* passa pelo campo de cobertura da antena, o seu campo magnético é detectado e os dados que estão na *Tag* são decodificados e repassados para o computador fazer o processamento (PINHEIRO, 2005).

O tempo decorrido desta execução é inferior a um décimo de segundo, portanto o tempo de exposição necessário da *Tag* é bem pequeno. Resumindo, a única função da leitora é ler/gravar e decodificar os dados que estão em uma *Tag* que passa pela sua região de "abrangência" (Info-as, 2007).

2.4 TAGS

Os *transponders* (ou RF *Tag*s), Figura 03, estão disponíveis em diversos formatos, tais como cartões, pastilhas, argolas, e podem ser encapsulados em materiais como o plástico, vidro entre outros.

São hardwares que possuem uma antena e um chip, que respondem a sinais remotos de um leitor (SANTINI, 2006).

Fonte: Santini (2006)

Figura 03: *Tag* RFID

As *Tags* ainda podem ser de duas formas:

a) ativas: são alimentados por bateria interna, e permitem o processo de leitura e gravação;

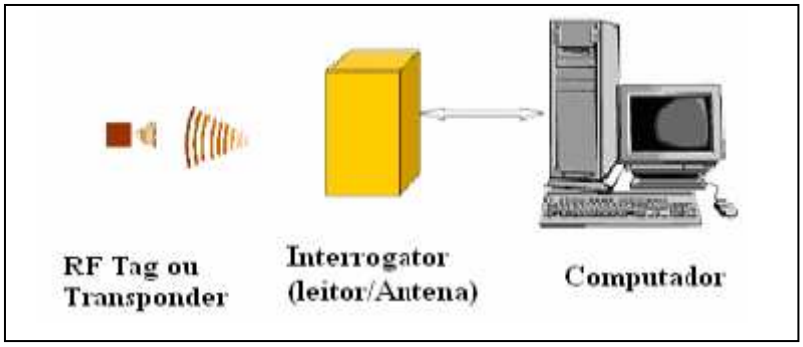
b) passivas: operam sem bateria e sua alimentação é feita pelas próprias ondas eletromagnéticas, geralmente só usadas para leitura com distâncias curtas.

Segundo Santini (2006), existe uma nova *Tag*, classificada como duas vias. São *Tags* ativas, possuem uma bateria interna que supre seu próprio consumo de energia, a grande diferença consiste em que este tipo de *transponder* não precisa ser necessariamente ativado por um leitor: as *tags* podem comunicar-se entre si.

Conforme Pinheiro (2004), a faixa de freqüência que as *Tags* atuam varia conforme classificação abaixo:

a) sistema de baixa freqüência (30 a 500 KHz): para curta distância de leitura e baixos custos. Utilizada para controle de acesso, rastreabilidade e identificação de animais. Esta freqüência mais baixa trabalha muito melhor perto da água ou dos seres humanos;

b) sistema de alta freqüência (850 a 950 MHz e 2.4 a 2.5 GHz): para leitura a médias e longas distâncias e a alta velocidade. Normalmente utilizado para leitura de *Tags* em veículos e coleta automática de dados.



Fonte: Hightechaid

Figura 04: Funcionamento do RFID

De uma forma resumida, o RFID funciona da seguinte forma (figura 04): A antena ou leitor envia um sinal, a *Tag* recebe o sinal, responde ao leitor enviando os dados que estão gravados nela, assim que a leitora recebe o sinal de volta, repassa as informações adiante, geralmente para um sistema que vai trabalhar com os dados enviados.

2.5 MEMÓRIA E PROCESSAMENTO

Segundo Glover (2006 apud SANTINI, 2006), as *Tags* também podem ser classificadas conforme sua memória e processamento.

2.5.1 1-bit Transponder

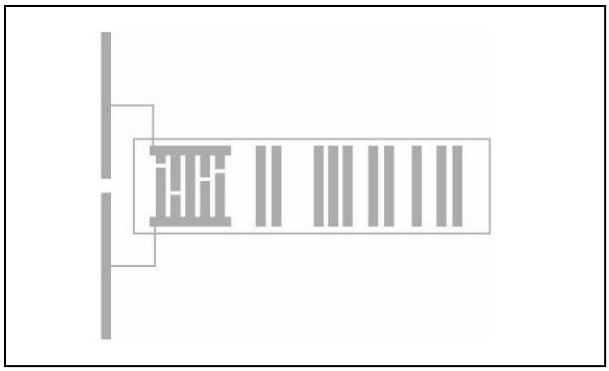
Recebem este nome porque conseguem comunicar somente 1 bit, extremamente pequeno, não possui nenhuma identificação própria pelo fato de não possuir uma memória interna. Seu funcionamento é simples, quando um leitor procura por *tags* em seu campo de atuação, elas simplesmente respondem sim ou não, “0” ou “1”, 1 presente, 0 ausente. Este tipo de *transponder* é usado em sistemas anti-roubo. As *tags* são colocadas nos produtos de tal forma que se forem retirados sem o uso da ferramenta correta, danificam o produto, inibindo assim o roubo. Muitas lojas usam esta tecnologia em suas mercadorias e na saída das mesmas, possuem enormes leitores que quando recebem um sinal positivo de uma *tag* acionam o

sistema de segurança.

2.5.2 Surface Acoustic Wave (SAW) Transponder

Diferentemente do 1-bit *Transponder*, elas já saem de fábrica com um número, um identificador único que não pode ser alterado. Por este motivo, este tipo de *transponder* não possui bateria nem processador ou *microchip*.

Segundo Bhatt et. al. (2006, apud SANTINI, 2006), as *tags* SAW possuem uma antena em uma das suas extremidades que recebe o sinal que por sua vez é passado para um bloco chamado transdutor interdigital. Este transdutor possui um cristal piezelétrico que vibra quando recebe o pulso criando uma onda acústica que percorre toda a *Tag* que possui linhas refletoras. Estas linhas são o ID da *Tag*. Estas linhas refletem de volta parte dos pulsos que fazem novamente vibrar os cristais. O número de linhas refletoras e os espaços entre elas é que forma o ID do *transponder*.



Fonte: Santini (2006)

Figura 05: *Transponder* SAW

2.5.3 n-bit Transponder

Usado quando existe a necessidade de armazenar n bits, como um identificador ou mais informações. Atualmente é quase impossível dizer a capacidade máxima de armazenamento em uma T*ag*, pois existem muitas pesquisas na área.

A melhor alternativa segundo Finkenzeller (2003, apud SANTINI, 2006), é armazenar a menor quantia possível de informações dentro da *Tag*, como um ID por exemplo, e o restante, num banco de dados. Isso faz com que as *Tags* tenham um menor custo e haja uma

maior segurança quanto às informações.

Quando a *Tag* armazena somente um ID, sua estrutura é bem simples. Conforme Glover (2006, apud SANTINI, 2006), a memória é divida em 3 partes. A primeira é o *Cyclic redundancy Check*, (CRC - Checagem de Redundância Cíclica) verifica se o bloco com as informações não esta corrompido; a segunda parte é o EPC que é a identificação da *Tag* e a última parte é o *Password*, senha usada para desativar a *Tag*.

As *Tags* usadas neste trabalho, gentilmente cedidas pela empresa WK Sistemas (www.wksistemas.com.br), na pessoa do Sr. Werner Keske, são do tipo RO (*Read Only*), somente leitura com o código atribuído pelo fabricante, a empresa Texas Instrument. Este código possui 64 bits. A freqüência operacional é de 134,2 KHz.

Já o leitor, que possui uma caixa e uma fonte de alimentação que foram montados pela WK Sistemas, assim como a antena, é um Micro-Reader TIRIS também da empresa Texas. Somente o módulo leitor é da Texas.

2.6 FORMAS DE COMUNICAÇÃO

Existem 3 tipos de comunicação entre o leitor e as *Tags*. Segundo Finkenzeller (2003, apud SANTINI, 2006), na comunicação FDX (*Full Duplex*) a *Tag* e o leitor podem falar ao mesmo tempo. Na comunicação HDX (*Half Duplex*) cada um tem sua vez de falar.

Nestes dois casos, é o leitor que fornece toda energia necessária para a comunicação. Já na comunicação seqüencial (SEQ), para que a comunicação seja realizada, um capacitor tem que armazenar a energia que será utilizada quando a transmissão do leitor terminar, pois a *Tag* transmite os dados em pausas, também chamadas de pulsos.

2.7 VANTAGENS E DESVANTAGENS DO USO DO RFID

Segundo Santana (2005), a principal vantagem do uso do RFID é realizar a leitura sem o contato e sem a necessidade de uma visualização direta do leitor com a *Tag*. É possível, por exemplo, colocar a *Tag* dentro de um produto e realizar a leitura sem ter que desempacotá-lo, ou ainda, aplicar a *Tag* em uma superfície que posteriormente será coberta por tinta. O tempo

de resposta é muito baixo, menos que 100 ms, e o custo dos equipamentos apresentaram uma significativa queda nos últimos anos.

Algumas das principais vantagens:

a) capacidade de armazenamento, leitura e envio de dados para etiquetas ativas;
b) detecção sem necessidade da proximidade da leitora para o reconhecimento dos dados;
c) durabilidade das etiquetas com possibilidade de reutilização;
d) contagens instantâneas de estoque, facilitando os sistemas empresariais de inventário;
e) precisão nas informações de armazenamento e velocidade na expedição;
f) localização dos itens ainda em processos de busca;
g) melhoria no reabastecimento com eliminação de itens faltantes e aqueles com validade vencida;
h) prevenção de roubos e falsificação de mercadorias;
i) coleta de dados de animais ainda no campo;
j) processamento de informações nos abatedouros (BORGES 2004, apud SANTANA, 2005).

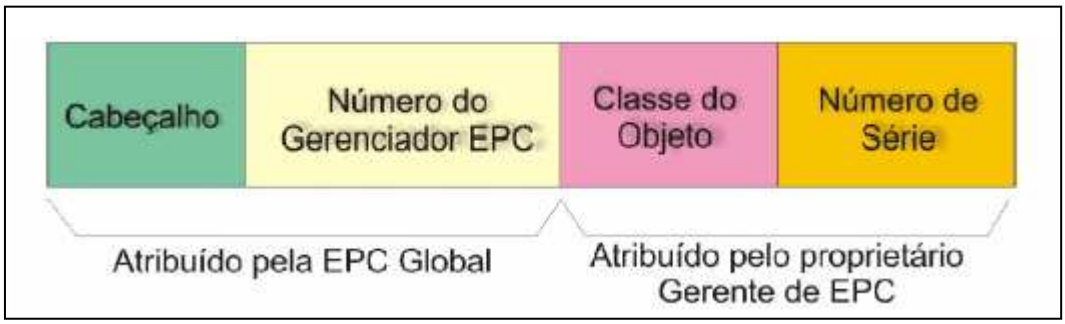
As desvantagens apresentadas são:

a) o custo elevado da tecnologia RFID em relação aos sistemas de códigos de barras é um dos principais obstáculos;
b) o preço final dos produtos, pois a tecnologia não se limita apenas ao *microchip* anexado ao produto. Temos ainda as antenas, os leitores, ferramentas de filtragem de informações e sistemas de comunicação;
c) o uso em materiais metálicos e condutivos pode afetar o alcance de transmissão das antenas. Como a operação é baseada em campos magnéticos, o metal pode interferir negativamente no desempenho. Entretanto, encapsulamentos especiais podem contornar esse problema.
d) a padronização das freqüências utilizadas para que os produtos possam ser lidos por toda a indústria, de maneira uniforme.
e) a invasão da privacidade dos consumidores por causa da monitoração das etiquetas colocadas nos produtos. Para estes casos existem técnicas, de custo ainda mais elevado, que bloqueiam a funcionalidade do RFID automaticamente quando o consumidor sair fisicamente da loja (BOSS, 2004 apud SANTANA, 2005).

2.8 PADRÕES

A questão da padronização é hoje a mais discutida na área de RFID.

Segundo a EAN Brasil, atualmente sendo chamada de GS1, (2007), a EPC Global é uma organização que esta engajada em encontrar um padrão para a comunicação entre sistemas RFID. Segundo esta organização, a estrutura básica de um número do Código Eletrônico de Produto (EPC), segue as regras conforme figura 06.



Fonte: Santini (2006).

Figura 06: Padrão de estrutura para um número EPC

O cabeçalho tem por finalidade identificar o comprimento, tipo, estrutura, versão e geração do EPC. O número do gerenciador é o identificador da entidade que é responsável por manter as partições que seguem. A classe do objeto identifica a qual classe ele pertence e o número de série identifica a instância a qual ele pertence. Segundo a GS1Brasil, todos os produtos que possuem algum tipo de identificação, RFID por exemplo, possuem uma etiqueta como a apresentada na figura 07 abaixo.

Fonte: EAN Brasil

Figura 07: Etiqueta de identificação

A ISO (União Internacional das Instituições Nacionais de Padronizações) segundo Klaus (2003, apud SANTINI, 2006), também possui em sua organização um comitê responsável por desenvolver um padrão para o RFID.

Estes padrões estão em constante mudança, pois ainda existem muitas pesquisas para descobrir a melhor forma de armazenar os dados nas *Tags*.

2.9 SEGURANÇA COM RFID

Há muito tempo que a segurança da informação é prioridade na questão de investimentos na área de tecnologia, e segundo o Instituto de Desenvolvimento Cultural (IDC), este cenário não tente a mudar tão cedo. Segundo pesquisa efetuada pelo Instituto e publicada pelo site IDG Now, em 2006 a segurança foi à segunda colocada em questão de prioridade de investimento nas empresas.

Qualquer empresário fica horrorizado só em pensar que as valiosas informações da sua empresa podem cair nas mãos de concorrentes ou até mesmo de pessoas mal intencionadas.

Para tentar evitar que isso ocorra, as empresas vêm investindo pesado conforme a pesquisa do IDC. Antivírus, servidores “super lacrados” para evitar a entrada de qualquer tipo de espião, treinamentos para que os funcionários possam ajudar a empresa a não cair na cilada da segurança.

Infelizmente não são somente estas ameaças a que as empresas estão expostas. A proliferação de vírus também preocupa e muito, pois uma vez que uma máquina da rede esta infectada, toda a rede da empresa esta ameaçada.

Mas será que com o RFID é diferente?

Infelizmente não. A tecnologia RFID não fica fora desta corrida. Apesar de a tecnologia RFID apresentar um grande avanço, ela pode trazer grandes problemas aos seus usuários.

O grande problema das etiquetas de RFID, segundo Wikipedia (2007), é que elas não possuem nenhuma rotina ou dispositivo para proteger seus dados, mesmo as *Tags* passivas que tem raio de atuação muito menor podem sofrer intervenções e extravio de suas informações, já com as ativas, o problema é muito maior. Se o RFID tomar as proporções que estão sendo almejadas, todas as pessoas possuirão T*ags* em seus objetos pessoais, assim, dados pessoais poderão ser obtidos por qualquer um que possuir uma leitora de RFID.

Mas, para que isso não ocorra várias alternativas já estão sendo estudadas, entre elas, a mais aceitável é a de não armazenar informações nas T*ags*, mas sim em bancos de dados ou nas leitoras.

Proprietários de carros que possuem em sua chave um mecanismo que destrava o carro com a aproximação da chave devem ter um cuidado redobrado. Os mecanismos usados para destravar o carro contém *chips* de RFID. Segundo Inovação Tecnológica (2005), um artigo científico publicado indica que a criptografia utilizada nos *chips* RFID das chaves de automóveis não são capazes de manter os ladrões à distância.

Segundo detalhes publicados no site Inovação Tecnológica (2005) sobre o artigo, os pesquisadores levaram menos de 15 minutos para quebrar a criptografia da chave secreta. A verificação de segurança da etiqueta inteligente ocorre por meio de pergunta e resposta, quando o chip se aproxima o leitor emite uma mensagem de 0 e 1, o *chip* processa e envia uma resposta, se ela for correta, o sistema libera o acesso. Para descobrir a chave secreta, o que o grupo de pesquisadores fez foi descobrir o processo matemático utilizado. Para isso, eles compraram um *microchip* disponível em lojas especializadas e o programaram para descobrir a chave secreta de um "chaveiro" de pagamento de propriedade de um dos pesquisadores. Da mesma forma conseguiram descriptografar a chave de um carro, conseguindo assim desarmar o sistema anti-roubo do carro sem a presença da chave original. Para resolver este problema, os cientistas deram à dica de usar um estojo metálico para guardar a chave enquanto ela não estiver em uso, que impede que os dados da chave sejam lidos por ondas de rádio.

Segundo Wikipedia (2007), os sistemas de RFID são divididos em 3 zonas de segurança, que precisam ser analisadas e protegidas:

a) a primeira zona compreende as próprias *Tags* RFID. A possibilidade de vulnerabilidade existente consiste em como os dados são armazenados na *Tag*. A grande maioria das empresas não tem por hábito encriptar os dados que estão gravados na *Tag* pelo simples motivo de espaço. Gravar os dados de forma simples, pode em alguns casos permitir que sejam gravadas mais informações na *Tag* que em alguns casos pode ser realmente útil;
b) a segunda zona está nas leitoras que geralmente estão conectadas a uma rede local, através de redes cabeadas ou *wireless*. Existem duas possibilidades, uma que o tráfego de dados entre a leitora e a *Tag* não é criptografado ou então os leitores que não possuem um sistema de autenticação das *Tags*. Neste caso, podem ocorrer ataques como o *spoofing* (*Tag* falsa) ou então por *Denial Of Service* (DoS, Negação de Serviço). Este DoS consiste em a *Tag* receber um sinal, considerá-lo válido, e quando tentar decodificar, verificar que o sinal é inválido, assim ela se reinicia para um estado de erro, o mesmo estado que ela se encontra quando é

ligada (COMPUTERWORLD, 2006). A grande ameaça neste caso consiste em qualquer pessoa que esteja por perto, equipada de um *sniffer* (ferramenta que busca por dispositivos conectados a rede) pode capturar as informações que estão sendo transmitidas;

c) Por último, são os serviços como ONS1, Gerenciador de Eventos, EPCIS2 e o servidor de integração.(ONS: *Object Naming Service*, Serviço de Nomeação de Objetos. É um serviço da EPC Global Inc que faz a tradução de um código para a informação de um produto. EPCIS: EPC *Information Service* é um repositório de eventos de RFID EPC. O *Security Working Group* da EPC é um grupo que trabalha na segurança dos sistemas RFID com a ajuda da VeriSign e ConnecTerra.)

Diante dos fatos apresentados, a Wikipedia (2007) conclui que para que possa haver uma maior confiança na utilização da tecnologia, seja usada criptografia, assim como é usada no envio e recebimento de e-mail que contenham informações confidenciais.

2.10 TRABALHOS CORRELATOS

Behnke (2004), em seu Trabalho de Graduação, propôs a criação de uma Carteira de Habilitação Digital. No trabalho, existe a união de um produto já existente no mercado com a CNH digitalizada. No momento que um agente de trânsito efetuar uma notificação, munido de um *Personal Digital Assistant* (PDA) com uma leitora de CNH digital embutida, teria ali, no PDA, todas as informações sobre o veículo, desde que ele esteja cadastrado no sistema, e também do condutor do mesmo, bastando para isso efetuar a leitura da CNH digitalizada. Além destas facilidades, Behnke (2004) também propõe que com esta CNH, as multas cometidas não precisariam mais ser enviadas via correio para o infrator, pois elas estariam gravadas no sistema e o mesmo poderia efetuar o pagamento em qualquer agência bancária, ou até mesmo pela internet, bastando para isso possuir uma leitora de CNH digital.

Durante as pesquisas foi encontrado também o Trabalho de Conclusão de Curso de Zeidin (2005), que também utiliza a tecnologia de RFID, mas propõem um sistema para controle do estoque, permitindo um controle total das mercadorias, demonstrando sua movimentação de entrada e saída.

Segundo o Serviço Federal de Processamento de Dados (2004), a intenção dos Estados

Unidos e outros 27 países é criar o passaporte digital, incluindo ali tanto os dados em formato de texto como também biométricos. Os dados biométricos incluem fotografia frontal do rosto, como já são usadas hoje, impressões digitais e a imagem da íris. Para guardar todas as informações, foi estimada aproximadamente a utilização de 32KB de memória, cujo conteúdo seria protegido pelo uso de uma assinatura digital. A tecnologia que está sendo estudada para esta digitalização é a RFID, justificando seu uso por ser mais robusto do que a leitura eletrônica, que requereria um bom contato elétrico. Com o RFID, a leitura do passaporte também poderia ser realizada estando a pessoa distante do leitor.

Aqui no Brasil, a MedAlliance, empresa que administra uma rede de tecnologia que tem por objetivo gerenciar o Prontuário Eletrônico e todas as informações que o compõem, composta por instituições de saúde, médicos e clínicas de todo país, tem em seu poder um banco de dados com todas as informações médicas dos seus pacientes, onde somente médicos autorizados pelo usuário podem ter acesso. Como um opcional, o paciente pode ter um cartão com tecnologia "*smart*" que vem com um *microchip* capaz de carregar informações sobre o prontuário do paciente.

Behnke (2004) sugere a digitalização de somente um documento, enquanto a presente proposta pretende unir todos os documentos de identificação. Zeidin (2005) utiliza em seu trabalho a tecnologia de RFID, que também será utilizada como forma de acesso ao banco de dados.

A idéia do Serviço Federal de Processamento de Dados vem ao encontro da presente proposta, pois estaria digitalizando um documento e utilizando para isso a tecnologia aqui proposta, o RFID.

Já a idéia do Prontuário Eletrônico Pessoal, tem em comum com a presente proposta o objetivo de disponibilizar em qualquer lugar que possua acesso a internet, as informações médicas. As informações que a MedAlliance armazena em seu banco de dados são praticamente as mesmas que aqui se pretende usar, como: antecedentes clínicos, os medicamentos consumidos e se possui alguma alergia a tipos específicos de remédios.

3 DESENVOLVIMENTO DO TRABALHO

Neste capítulo serão apresentados os aspectos técnicos referentes ao desenvolvimento do trabalho. O mesmo teve por objetivo desenvolver e criar um documento de identificação único, que armazene dados em um banco de dados, e utilizando um identificador de um *SmartCard* faça a pesquisa dos dados.

Para o detalhamento da implementação e das rotinas do software proposto são demonstrados os seus aspectos principais através dos diagramas de classes, caso de uso e atividades.

3.1 REQUISITOS PRINCIPAIS DO PROBLEMA A SER TRABALHADO

Conforme Lima (2005), um requisito é uma condição ou habilidade necessária para um sistema alcançar um determinado objetivo ou finalidade. O objetivo de todo sistema é atender a um conjunto de requisitos, as necessidades que o sistema deve satisfazer.

3.1.1 Requisitos funcionais

Requisitos funcionais, segundo Bezerra (2002), são responsáveis por definir as funcionalidades do sistema.

Lima (2005) afirma que os requisitos funcionais especificam ações que o sistema deve executar independente de exigências físicas ou tecnológicas, ou seja, é o conjunto das necessidades do cliente que devem ser satisfeitas para resolver um problema ou alcançar um objetivo em seu negócio.

O Quadro 01 lista os requisitos funcionais atendidos pelo sistema.

Código	**Descrição do Requisito**	**Caso de Uso**
RF01	O Sistema deve permitir o cadastramento de indivíduos e todos os seus dados pessoais de identificação.	UC04
RF02	O Sistema deve gravar os dados cadastrais em uma base de	UC06

	dados.	
RF03	O Sistema deve gravar os dados cadastrais básicos (nome, RG, CPF, naturalidade, nome dos pais, data de nascimento) nos cartões de SmartCard.	UC08
RF04	O Sistema deve interpretar os dados enviados pela leitora de RFID e apresentá-los em tela.	UC05
RF05	O Sistema deve pesquisar na base de dados, utilizando o CPF como identificador único, e apresentar os dados encontrados em tela.	UC05 e UC07
RF06	O Sistema deve permitir ao administrador cadastrar grupos de usuários, informar quais informações cada um poderá acessar e efetuar o devido controle de acesso .	UC01
RF07	O Sistema deve permitir ao administrador, após cadastrar os grupos de usuários, cadastrar os usuários associando-os a um grupo de acordo com as informações que está autorizado a consultar e/ou alterar.	UC02
RF08	O Sistema deve, assim que o usuário efetuar *login*, verificar quais as suas permissões de acesso.	UC3

Quadro 01: Requisitos Funcionais

3.1.2 Requisitos não funcionais

Para Lima (2005), requisitos não funcionais estão ligados, relacionados com as características do sistema ou do ambiente em que ele está inserido. Estética, interface amigável, segurança, desempenho são alguns requisitos classificados como não funcionais.

Bezerra (2002) resume em poucas palavras, requisitos não funcionais declaram as características de qualidade que o sistema deve possuir e que estão relacionadas às suas funcionalidades.

O quadro 02 lista os requisitos não funcionais atendidos pelo sistema.

Código	Descrição do Requisito
RNF01	Os dados gravados nos cartões de SmartCard deverão estar em conformidade, ou seja, deverão ser exatamente os mesmos que são apresentados hoje em documentos impressos (RG, CPF, Título de Eleitor e CNH).
RNF02	A interpretação e a apresentação dos dados em tela, enviados pela leitora de RFID, não podem ultrapassar o tempo de 5 segundos. A visualização dos dados resultantes da pesquisa deverá ser apresentada em uma única tela.
RNF03	Para a implantação do sistema deverá ser disponibilizado um leitor de RFID.
RNF04	O Sistema deverá ser implementado em Visual Studio C++.
RNF05	O sistema deverá utilizar banco de dados MYSQL.
RNF06	O Sistema não deverá permitir a alteração dos dados já gravados no SmartCards, somente dos dados que estão gravados na base de dados.
RNF07	As informações que serão gravadas no Cartão de SmartCard não podem ultrapassar a capacidade de 16 KBytes.

Quadro 02: Requisitos Não Funcionais

3.2 ESPECIFICAÇÃO

A especificação do aplicativo Sistema Único de Identificação Pessoal (SUIP) se dará através dos diagramas da *Unified Modeling Language* (UML):

a) diagrama de casos de uso;

b) diagrama de classes;

c) diagrama de atividades.

Para a construção dos diagramas foi utilizada a ferramenta Enterprise Architect.

3.2.1 Diagrama de caso de uso

Segundo Lima (2005), diagramas de caso de uso mostram conceitualmente o conjunto de funções que o sistema deve executar para atender aos requisitos do cliente, servindo também, como um contrato entre o cliente e o desenvolvedor. No caso de uso, o sistema é

visto com a perspectiva do usuário.

3.2.1.1 Cadastro de grupos e usuários

A figura 8 representa os casos de uso relacionados ao cadastro de grupos de usuários e usuários no sistema.

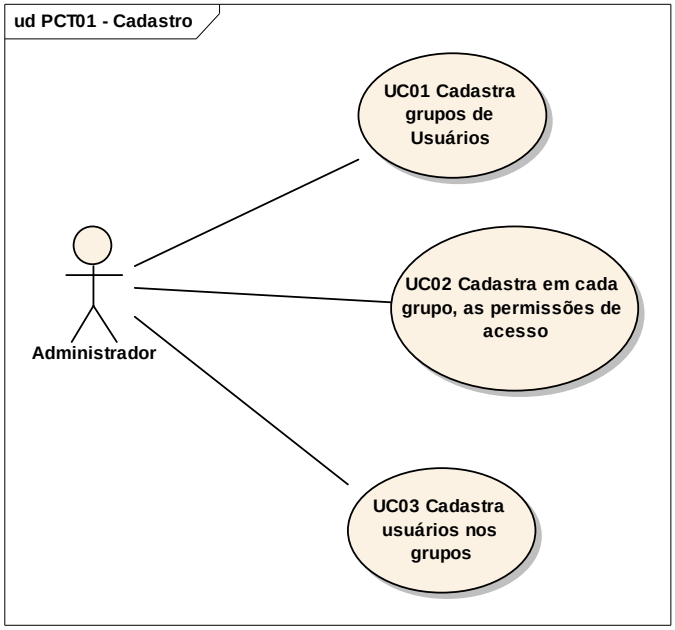


Figura 8 – Cadastro de Grupos e Usuários

O quadro 03 apresenta um detalhamento do caso de uso 01, apresentado na figura 8.

UC01: Cadastra grupos de usuário	
Resumo	Administrador cria diversos grupos.
Seqüência de ações	1. Administrador informa um código para o grupo. 2. Informa uma descrição para o grupo.

Quadro 03 – Detalhamento do caso de uso 01

O quadro 04 apresenta um detalhamento do caso de uso 02, apresentado na figura 8.

UC02: Cadastra em cada grupo, as permissões de acesso	
Resumo	Administrador atribui às permissões.
Seqüência de ações	1. Administrador seleciona quais informações o grupo poderá cadastrar ou consultar.

Quadro 04 – Detalhamento do caso de uso 02.

O quadro 05 apresenta um detalhamento do caso de uso 03, apresentado na figura 8.

UC03: Cadastra usuários	
Resumo	Administrador cadastra usuários.
Seqüência de ações	1. Administrador informa um código para o usuário. 2. Informa um apelido e senha para o usuário. 3. O sistema verifica se a senha e a confirmação da senha estão iguais. 4. Administrador escolhe a qual grupo este usuário estará ligado. 5. Se usuário também for administrador seleciona a opção de administrador.

Quadro 05 – Detalhamento do caso de uso 03.

3.2.1.2 Consulta dados e inclui dados

A figura 9 representa os casos de uso relacionados às ações de consulta de dados já gravados, inclusão de novos dados e indivíduos no sistema.

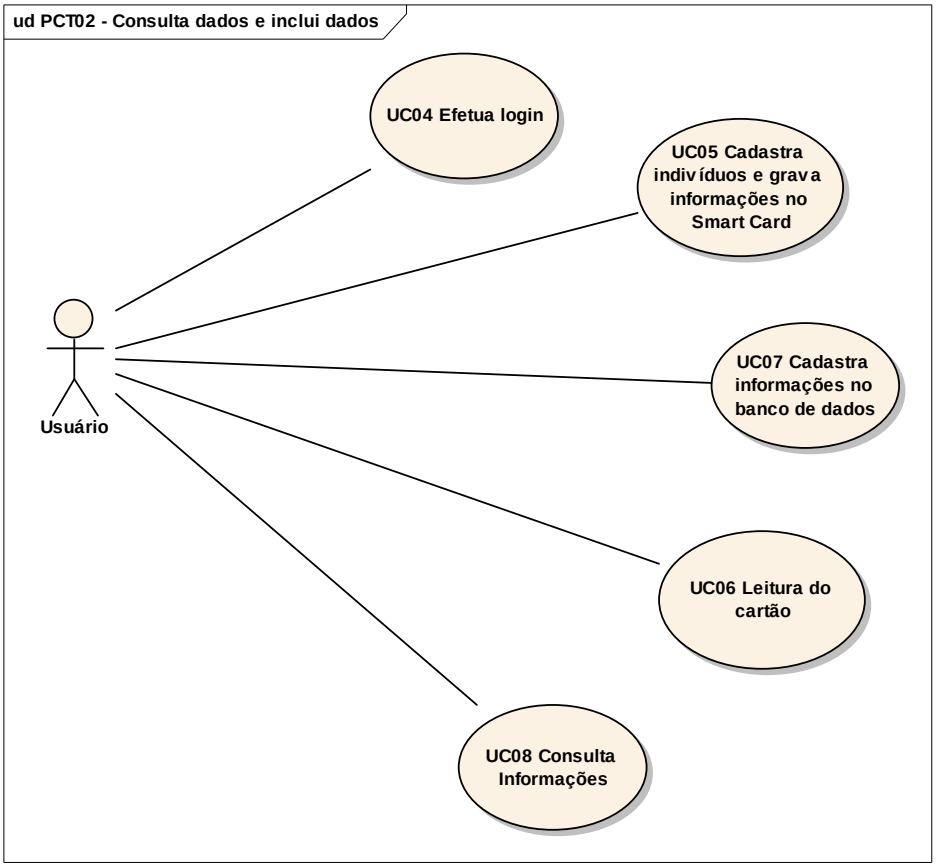


Figura 9 – Consulta dados e inclui dados

O quadro 06 apresenta um detalhamento do caso de uso 04, apresentado na figura 9.

UC04: Efetua login	
Resumo	Usuário se conecta no sistema.
Seqüência de ações	1. Usuário informa seu apelido e senha. 2. O sistema faz a verificação para saber quais as permissões deste usuário, habilitando assim somente as informações que ele pode ver ou alterar.
Exceção	No passo 1 o usuário não está cadastrado no sistema, ou o apelido e senha foram digitados de forma incorreta. O sistema apresenta uma mensagem “Usuário não cadastrado!” ou “Senha inválida”!.

Quadro 06 – Detalhamento do caso de uso 06.

O quadro 07 apresenta um detalhamento do caso de uso 05, apresentado na figura 9.

UC05: Cadastra indivíduos	
Resumo	Usuário cadastra novos indivíduos no banco de dados.
Seqüência de ações	1. Usuário informa todos os dados necessários para o cadastro. 2. Usuário aproxima cartão da leitora. 3. O sistema faz a gravação dos dados no banco de dados e armazena na tabela como chave primária o código encontrado no cartão.
Exceção	1. No passo 1 o usuário não tem permissão para efetuar cadastros. O menu com a opção de cadastro estará desabilitado.

Quadro 07 – Detalhamento do caso de uso 07.

O quadro 08 apresenta um detalhamento do caso de uso 06, apresentado na figura 9.

UC06: Leitura do cartão	
Resumo	Usuário aproxima o cartão do leitor para realizar a leitura dos dados.
Seqüência de ações	1. O leitor detecta a aproximação do cartão e faz a leitura dos dados. 2. Usando o código que foi encontrado no cartão, o sistema pesquisa na base de dados para encontrar os dados do indivíduo. 3. Após encontrar os dados o sistema os apresenta na tela.
Exceção	No passo 2, não existe dados informados para este código na base de dados. O Sistema apresenta a mensagem “CPF não cadastrado na base de dados!”.

Quadro 08 – Detalhamento do caso de uso 08.

3.2.2 Diagrama de classes

Para Lima (2005), um diagrama de classes mostra a estrutura estática do modelo, em que os elementos são representados por classes, com sua estrutura interna e seus relacionamentos.

A figura 10 apresenta as classes componentes da aplicação SUIP, proposta neste estudo.

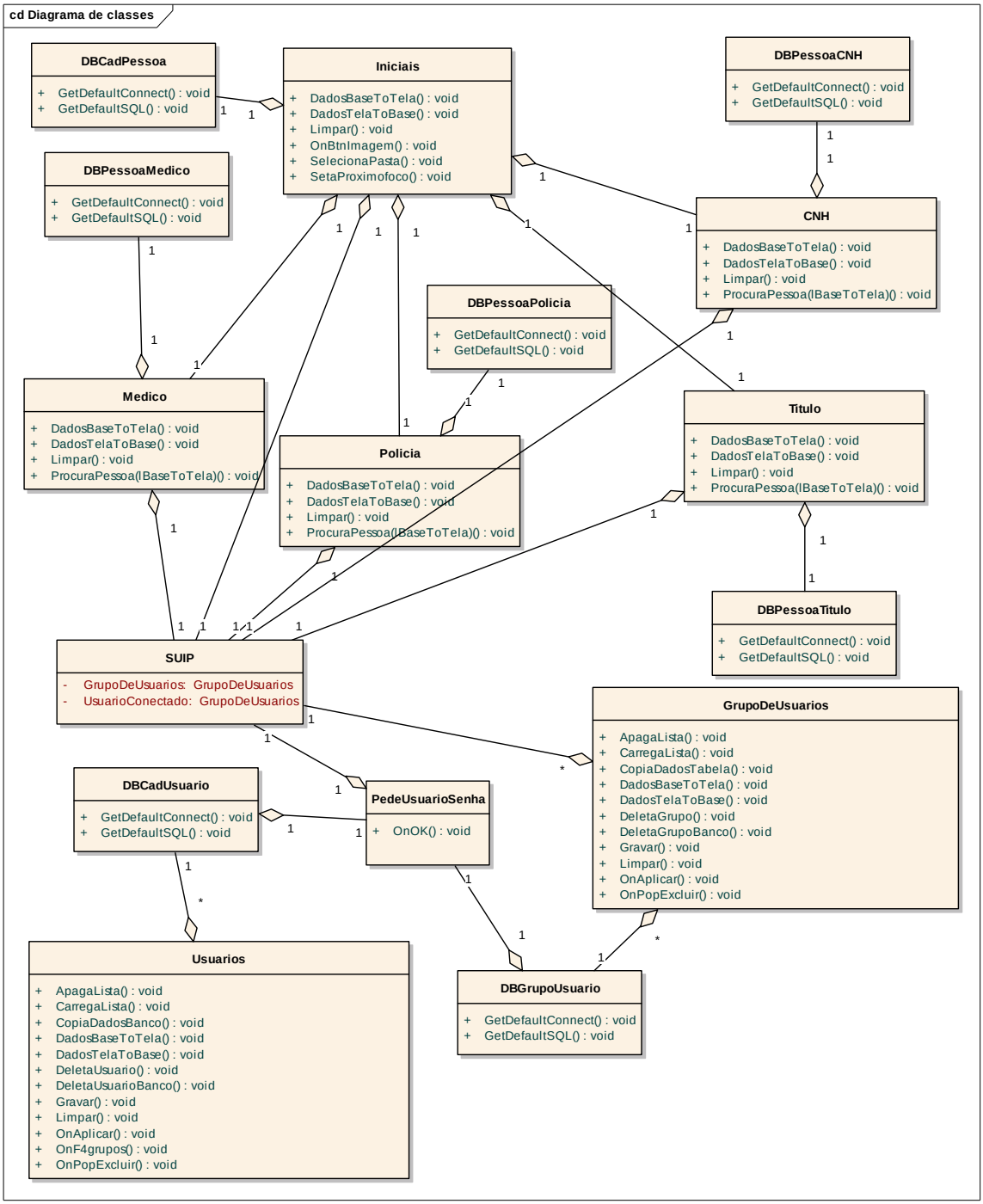


Figura 10 – Diagrama de classes

O quadro 09 apresenta uma descrição das funcionalidades de cada uma destas classes:

Classe	Descrição
SUIP	Esta classe é responsável por armazenar a tabela com as informações do usuário que está conectado, e também a tabela de grupos de usuários cadastrada no sistema.
Iniciais	Responsável por montar as telas de consulta e cadastro de dados. Controla todas as outras classes que seguem: CNH, Titulo, Policia e Medico.
GrupoDeUsuarios	Controla o cadastro de grupos de usuários.
Usuarios	Permite o cadastro dos usuários e a ligação com o grupo que cada um irá pertencer.
DBCadUsuario	Classe responsável por fazer a conexão com o banco de dados para a tabela de usuários.
DBGrupoUsuarios	Classe que faz a conexão com o banco de dados para a tabela de grupos.
DBCadPessoa	Faz a conexão com a base de dados para a tabela de pessoas.
DBPessoaCNH	Responsável pela conexão com a base de dados para a tabela de carteira nacional de habilitação.
DBPessoaTitulo	Conexão com a base de dados para obter as informações do título eleitoral.
DBPessoaPolicia	Classe responsável pela conexão com a tabela de informações policiais.
DBPessoaMedico	Classe usada para obter as informações da tabela de informações médicas.
PedeUsuarioSenha	Esta classe é responsável por verificar se o usuário e a senha informados para abrir o sistema existem e estão em conformidade com o cadastro. Também armazena em uma tabela todas as permissões de acesso que o usuário que esta conectando possui.

Quadro 09 – Detalhamento das funcionalidades das classes.

3.2.3 Diagrama de atividades

Segundo Bezerra (2002), diagrama de atividades é um tipo especial de diagrama de estados, onde são apresentados os estados de uma atividade, em vez dos estados de um objeto. Estes diagramas são orientados a fluxos de controle.

Lima (2005) resume dizendo que um diagrama de atividades permite modelar o comportamento do sistema, denotando os caminhos lógicos que um processo pode seguir.

3.2.3.1 Conectar

Na Figura 11 são demonstrados através de um diagrama de atividades todos os passos necessários para que um usuário possa se conectar ao sistema.

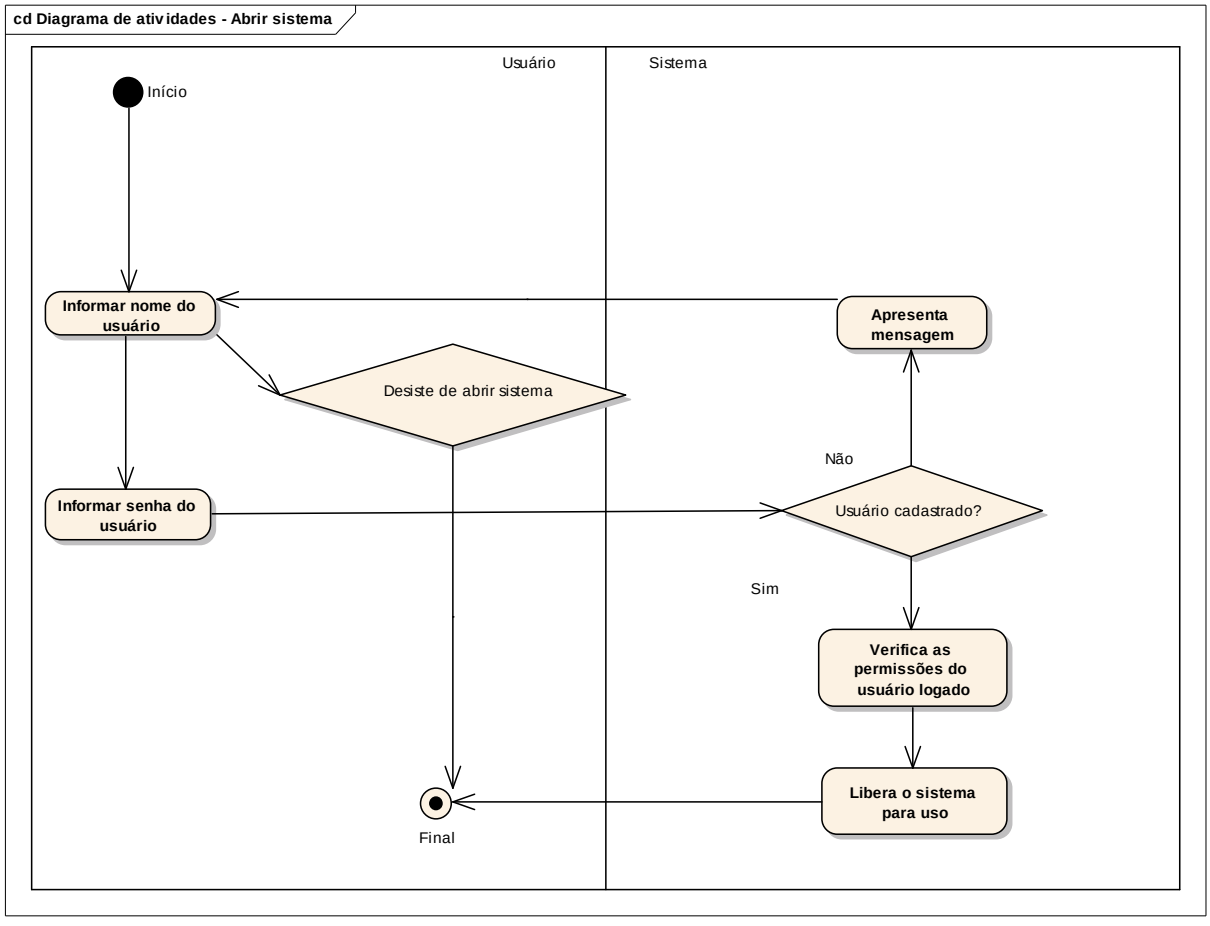


Figura 11 - Diagrama de atividades – Abrir sistema

Observa-se que após o usuário informar o nome e senha o sistema verifica se o mesmo está cadastrado, e a senha digitada confere com a que está no cadastro. Se tudo estiver correto,

o cadastro do grupo a que o usuário pertence é lido para que possam ser verificadas quais informações podem ser liberadas. E assim o sistema é liberado para o uso.

Caso a senha ou o apelido tenham sido digitados de forma diferente do que está no cadastro, o sistema assume como usuário não cadastrado e irá apresentar a mensagem “Usuário não cadastrado!”.

3.2.3.2 Efetuar leitura de dados

Na Figura 12 são demonstrados através de um diagrama de atividades todos os passos necessários para efetuar a leitura de dados a partir da leitura do cartão.

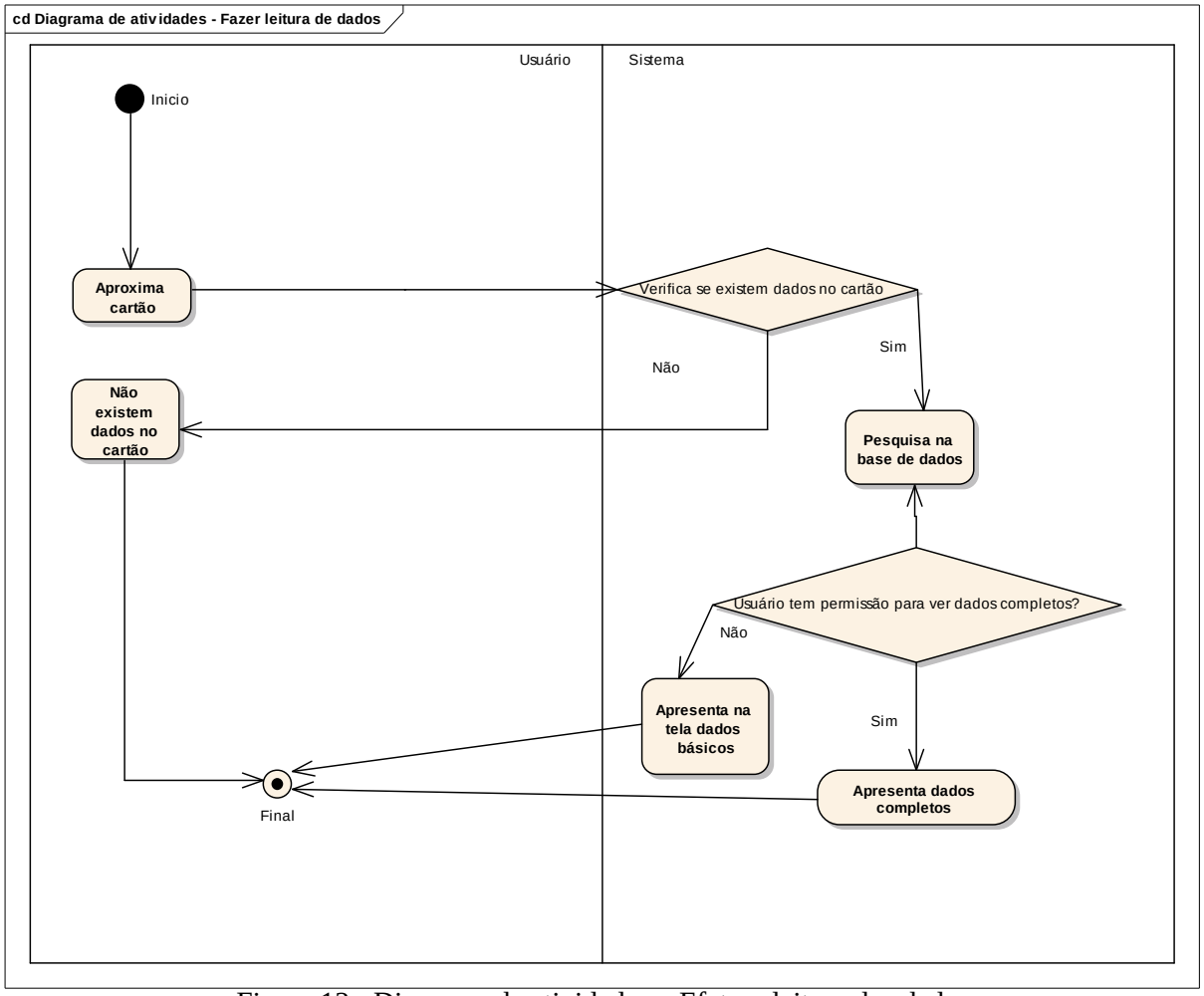


Figura 12 - Diagrama de atividades – Efetuar leitura dos dados

Observa-se, portanto, que o primeiro passo é aproximar o cartão da leitora para que ela possa capturar o código. Com esta identificação, o sistema irá buscar o cadastro da pessoa na base de dados, se encontrar irá verificar as permissões do usuário logado no sistema, caso ele possa ver todos os dados que estão gravados na base, ou for administrador, apresenta os

mesmos em tela. Caso o usuário não possa ver todos os dados da base, somente as informações básicas por exemplo, (CPF, identidade, local de nascimento, data de nascimento, nome dos pais e a foto) só estas serão mostradas em tela. Os dados apresentados variam de acordo com as permissões do usuário logado. Caso não existam dados gravados na base com este código, o sistema apresenta uma mensagem.

3.2.4 Modelo de banco de dados

Na figura 13, segue modelo de entidade relacionamento do banco de dados utilizado nesta proposta.

Como existem duas tabelas, que são usadas para o controle de acesso as informações no sistema, mas elas não estão sendo ligadas a nenhuma outra tabela, pode-se concluir que existem dois modelos de entidade de relacionamento, e dois banco de dados, mas, dentro de um só modelo.

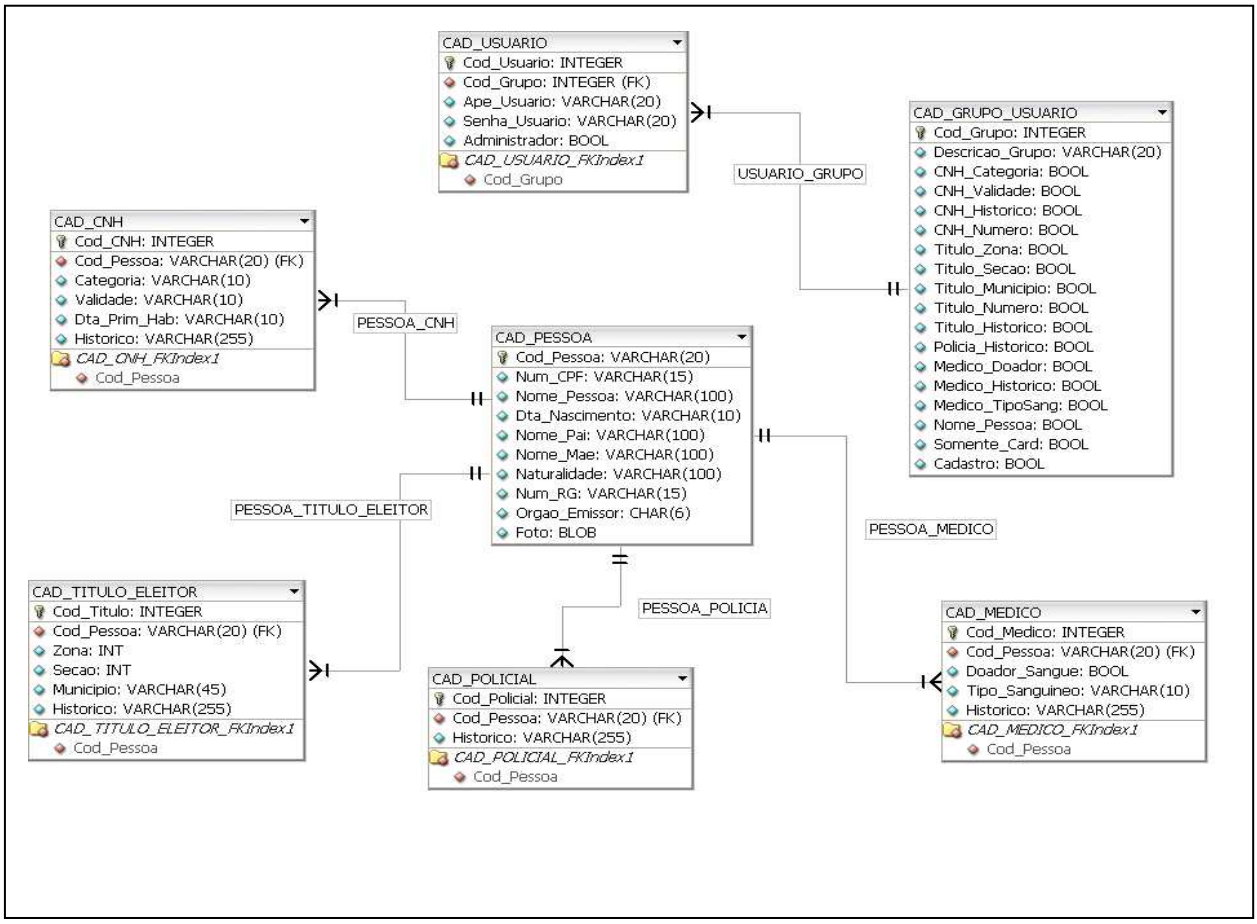


Figura 13 – Modelo de Entidade Relacionamento do banco de dados

3.3 IMPLEMENTAÇÃO

Neste capítulo são apresentadas as ferramentas utilizadas para o desenvolvimento deste trabalho e a operacionalidade do protótipo desenvolvido.

3.3.1 Técnicas e ferramentas utilizadas

Para o desenvolvimento do aplicativo SUIP, foi utilizada a ferramenta Microsoft Visual C++.

E para a criação do banco de dados a ferramenta utilizada foi o DBDesigner 4 juntamente com o MySQL – Front.

Para o desenvolvimento dos Diagramas e Casos de Uso, foi utilizada a ferramenta Enterprise Architect.

3.3.2 Operacionalidade da implementação

Nesta seção é apresentada a seqüência de telas e operações que um usuário deve fazer para que consiga usar o SUIP.

Primeiramente, para que o sistema consiga localizar a base de dados, é preciso estar com a ferramenta de gerenciamento MySQL (MySQL Front) instalada na máquina, e a base de dados dentro da pasta data que é criada após a instalação dentro da pasta *mysql* que ficará na raiz do diretório escolhido para instalação. Depois disso faz-se necessário que ela seja registrada com o seguinte nome “SUIP – Base de Dados” em Fonte de dados (ODBC), para isso deve ser instalado na máquina o *driver* do MySQL *ODBC*. Além dele, também é necessária a instalação do MySQL admin que deve estar com o serviço ativo para que a base possa ser encontrada. (Todos estes programas estão no CD que acompanha este trabalho.)

3.3.2.1 Logar no sistema

Na tela apresentada na Figura 14, é onde o operador do sistema informa seu nome de usuário e senha.

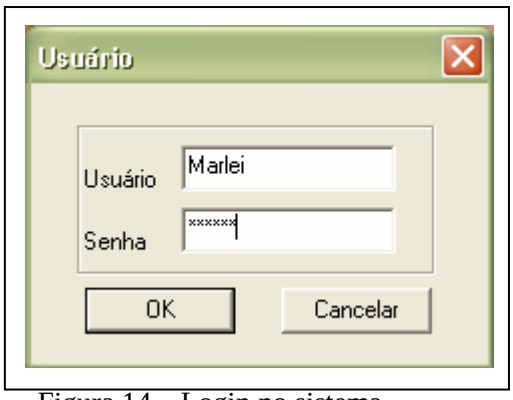


Figura 14 – Login no sistema.

Informado o nome de usuário e senha, o operador clica em OK. O sistema irá verificar se o usuário existe, caso não esteja cadastrado irá apresentar a mensagem como mostra a Figura 15. Ou então, se a senha informada estiver diferente da que consta no cadastro do usuário, será apresentada a mensagem de “Senha inválida!”.

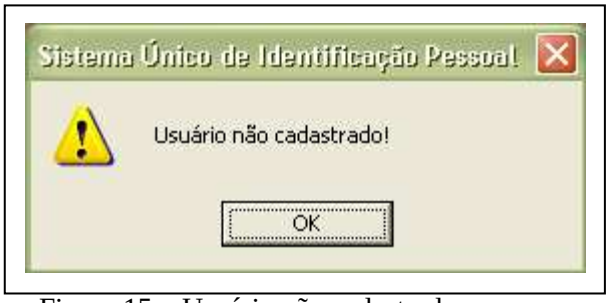


Figura 15 – Usuário não cadastrado.

Caso esteja cadastrado e a senha estiver correta, o sistema é liberado para o uso.

3.3.2.2 Usando o sistema

A seguir serão apresentados alguns procedimentos comuns ao uso do SUIP.

3.3.2.2.1 Cadastro de grupos

Caso esta seja a primeira vez que o sistema está sendo acessado, a primeira coisa a ser feita, é cadastrar os grupos de usuários conforme a Figura 16. Para acessar o sistema pela primeira vez, deve-se usar o usuário ADM e senha ADM, este usuário é administrador e por isso possui acesso para o cadastro de todas as informações que se fazem necessárias para o correto uso do sistema. Somente o Administrador do sistema pode efetuar cadastro de usuários e grupos. Para os demais usuários esta opção de menu estará desabilitada.

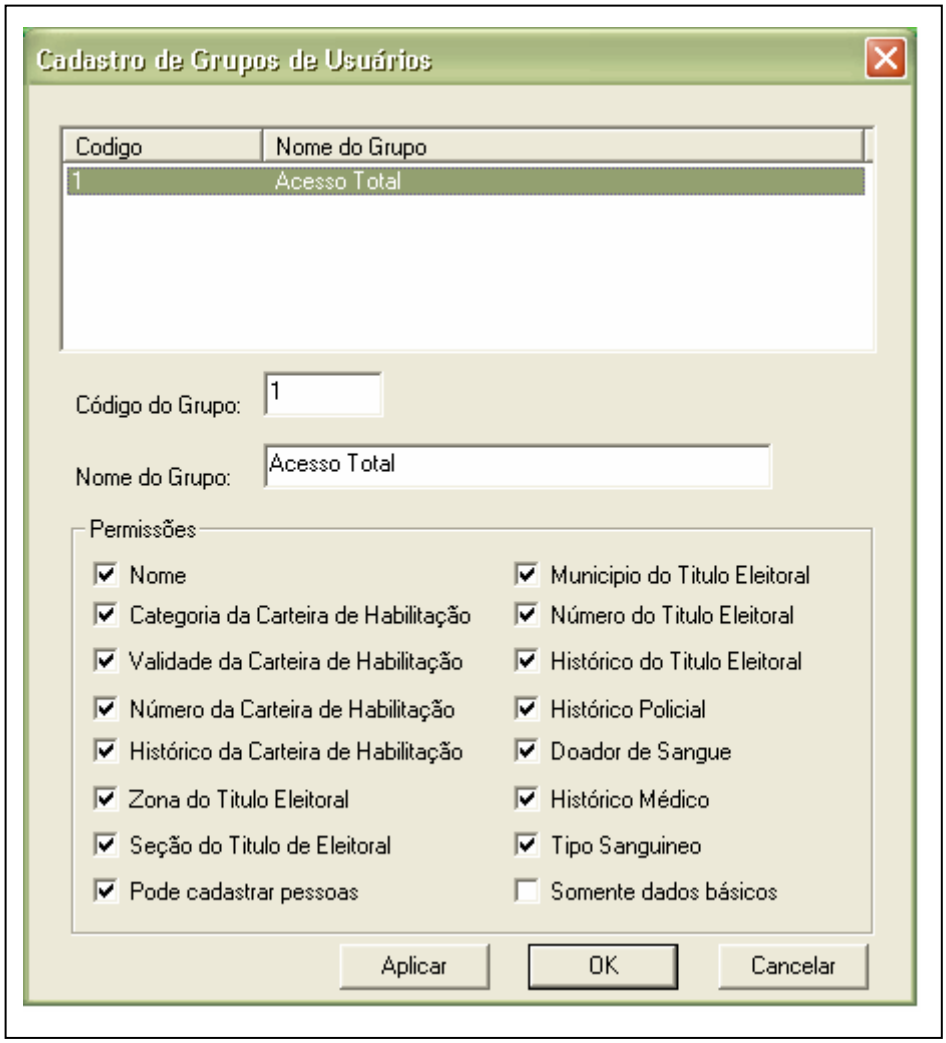


Figura 16 – Cadastro de grupos de usuários.

A quantidade de grupos para cadastro é ilimitada. São várias as opções de combinações. A única combinação que não pode ser feita é cadastrar no mesmo grupo a permissão de acesso para “Somente dados do Cartão” com mais alguma opção, pois, estas outras opções não serão habilitadas: somente os dados do cartão serão disponibilizados para visualização.

3.3.2.2.2 Cadastro de usuários

Depois de ter os grupos cadastrados, o próximo passo é cadastrar os usuários, conforme mostra a Figura 17.

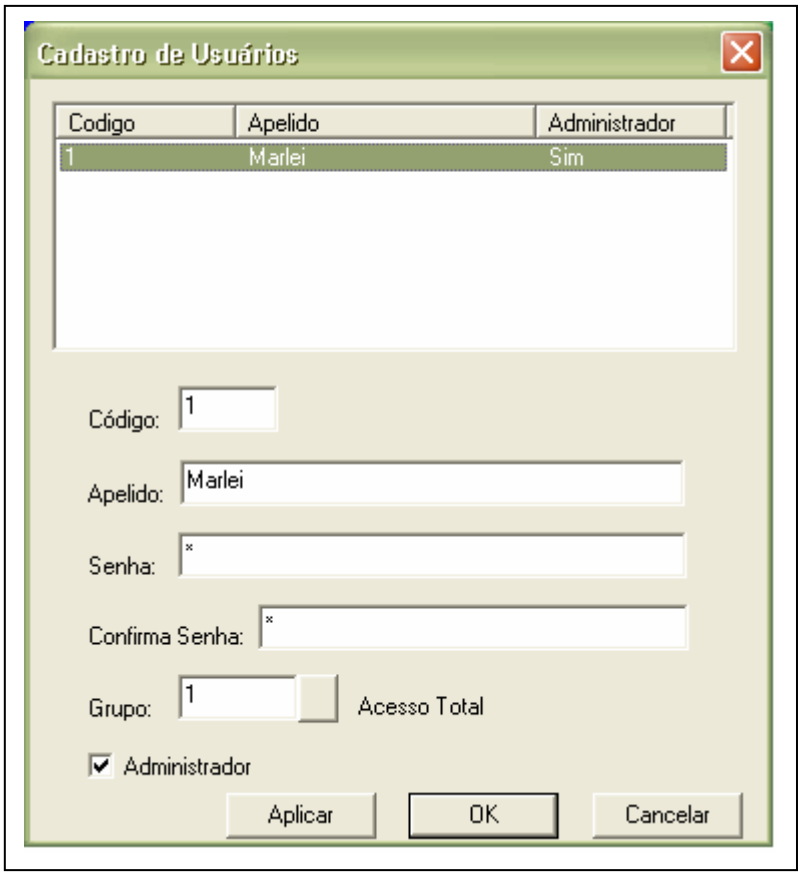


Figura 17 – Cadastro de usuários.

Quando o usuário for administrador, mesmo que esteja cadastrado em algum grupo que possua restrições, ele possui acesso a todas as informações.

Nas duas opções de cadastro, clicando com o botão direito do mouse sobre a lista, é habilitado um menu, com as opções de Exclusão do registro que esta selecionado, e de inclusão. Se selecionada opção de excluir, o registro será eliminado da base de dados. Já no incluir, irá limpar todos os campos para que possam ser digitadas novas informações. O sistema também verifica no momento da exclusão, se o usuário ou o grupo que está selecionado, é diferente do usuário e grupo que esta tentando fazer a exclusão, se for igual, a exclusão não é permitida e é apresentada uma mensagem em tela.

Com estes dois cadastros efetuados, o sistema está pronto para o uso. Lembrando que, se for efetuada alguma mudança de permissão no grupo do usuário que está conectado no

sistema, para que elas tenham efeito, é necessário efetuar um novo *login* no sistema.

3.3.2.2.3 Cadastro de indivíduos

Para que este menu seja habilitado, Figura 18, o usuário deve ser um administrador ou possuir a permissão de cadastro do grupo ao que ele pertence. Caso contrário, não poderá cadastrar indivíduos no sistema.

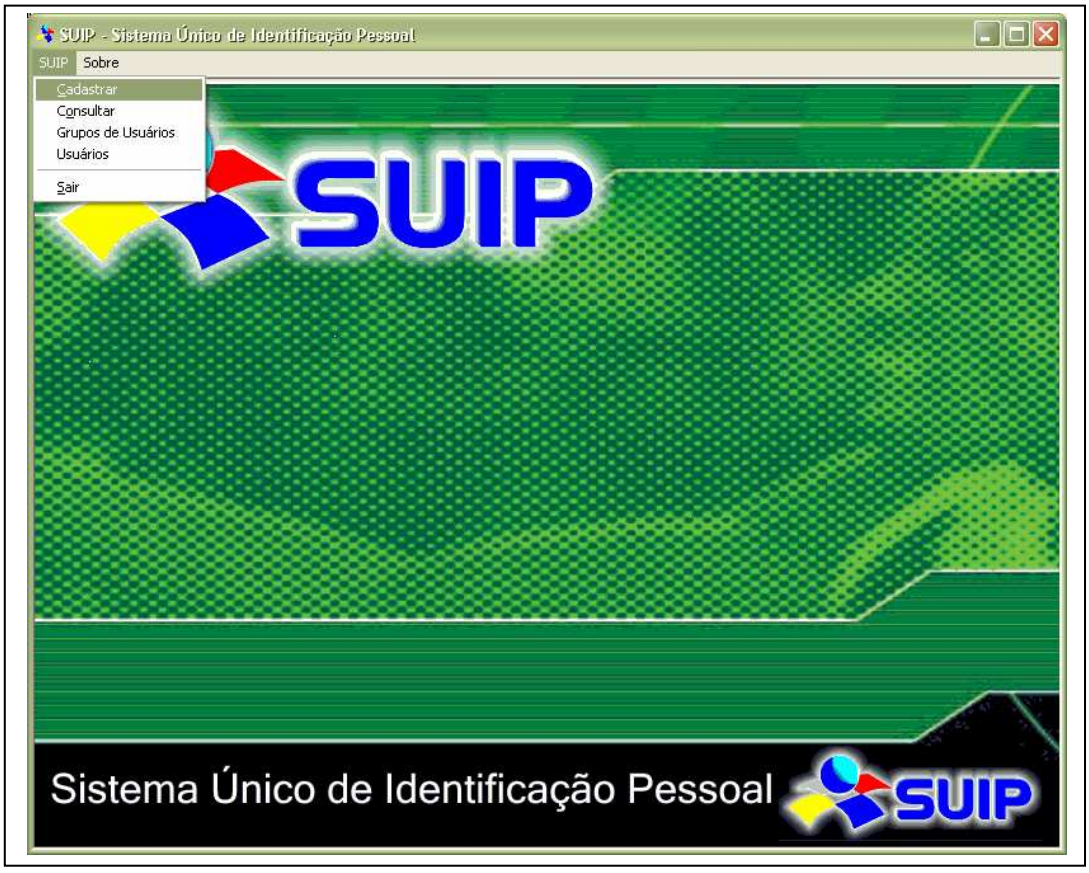


Figura 18 – Menu para cadastro de Pessoas.

Na tela de cadastro de pessoas, deve-se informar todos os dados necessários, incluindo informações de carteira de habilitação, conforme demonstrado na Figura 19.

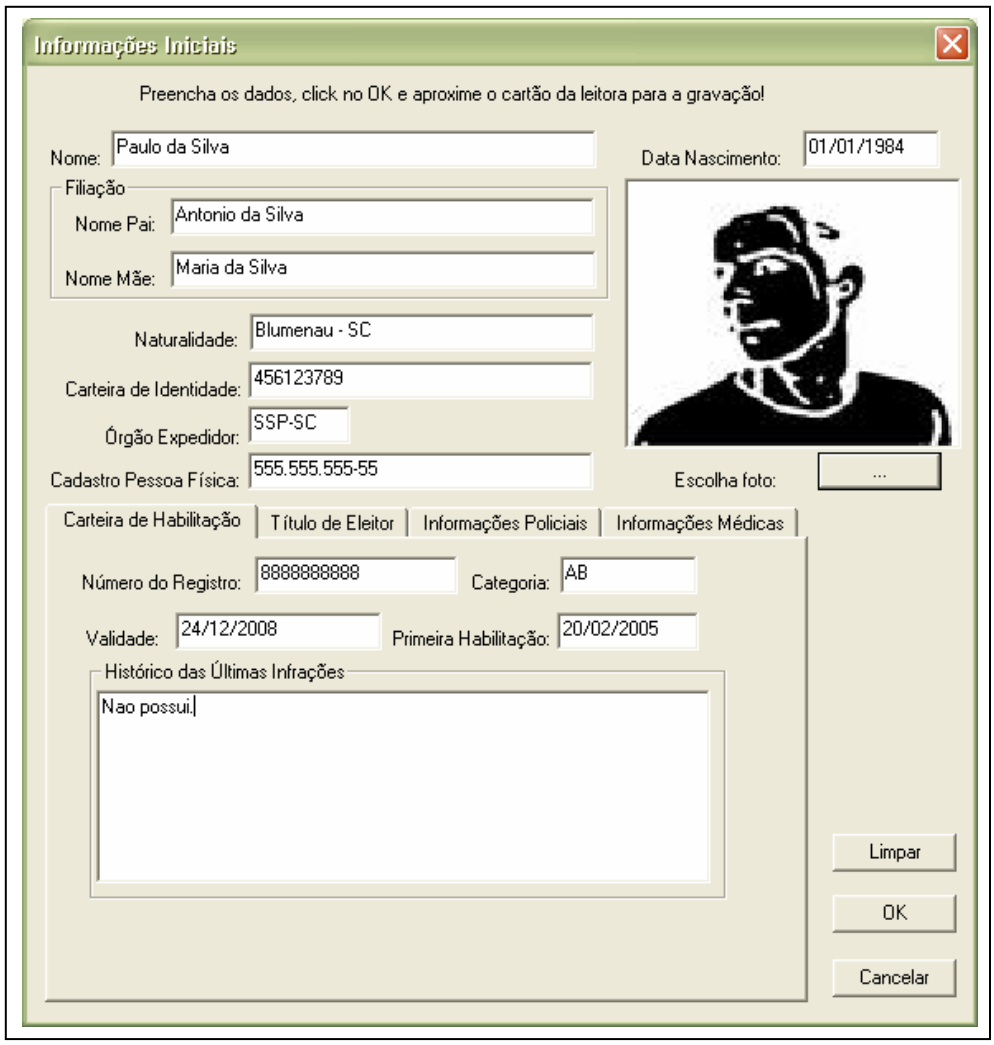


Figura 19 – Cadastro de pessoa.

Na próxima *tab*, Figura 20 encontra-se as informações que dizem respeito ao Título de Eleitor e ao comprovante de votação na última eleição.

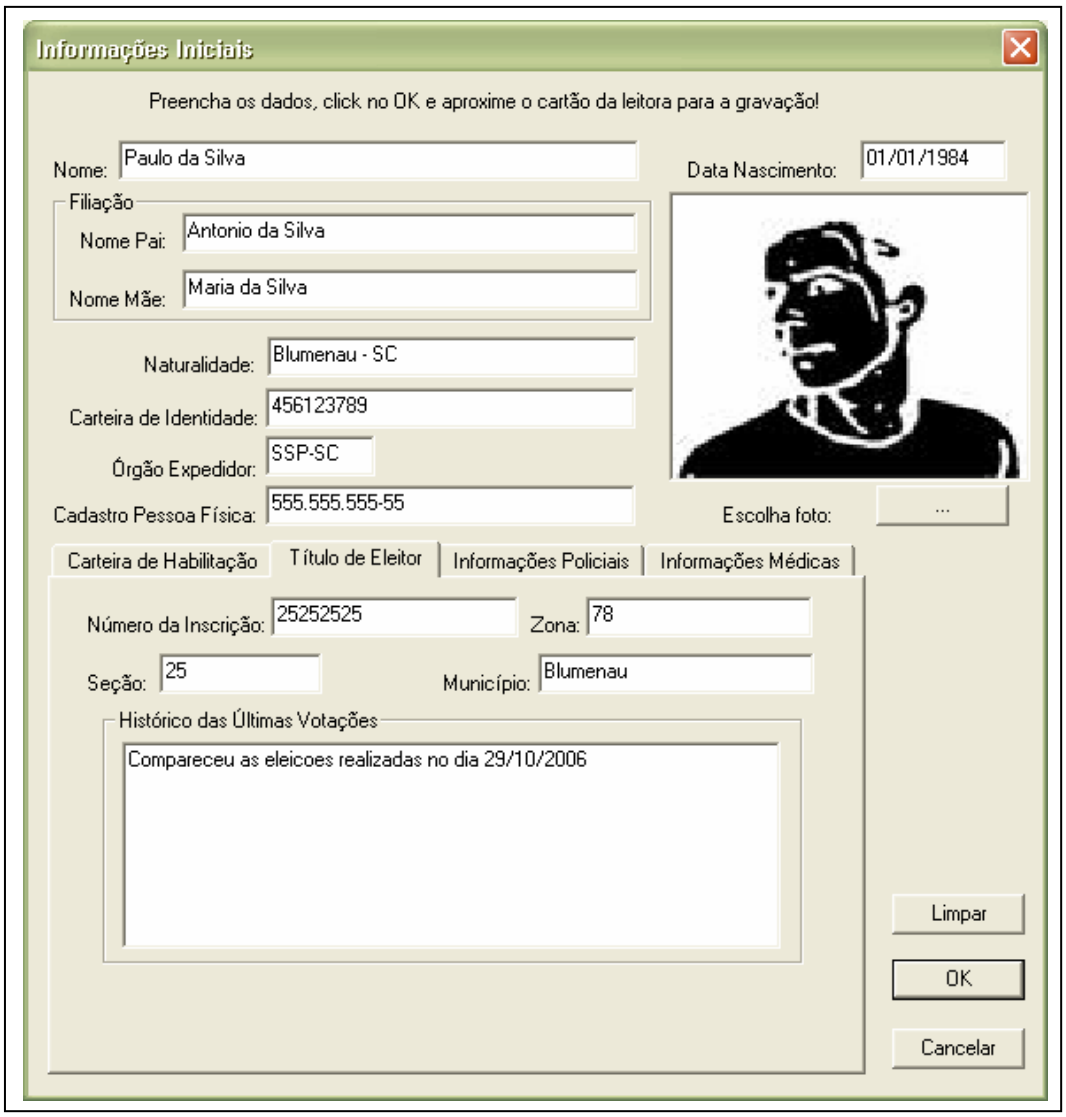


Figura 20 – Cadastro de informações do título de eleitor.

Em seguida, figura 21, informações policiais, onde consta se a pessoa possui alguma pendência ou passagem pela polícia.

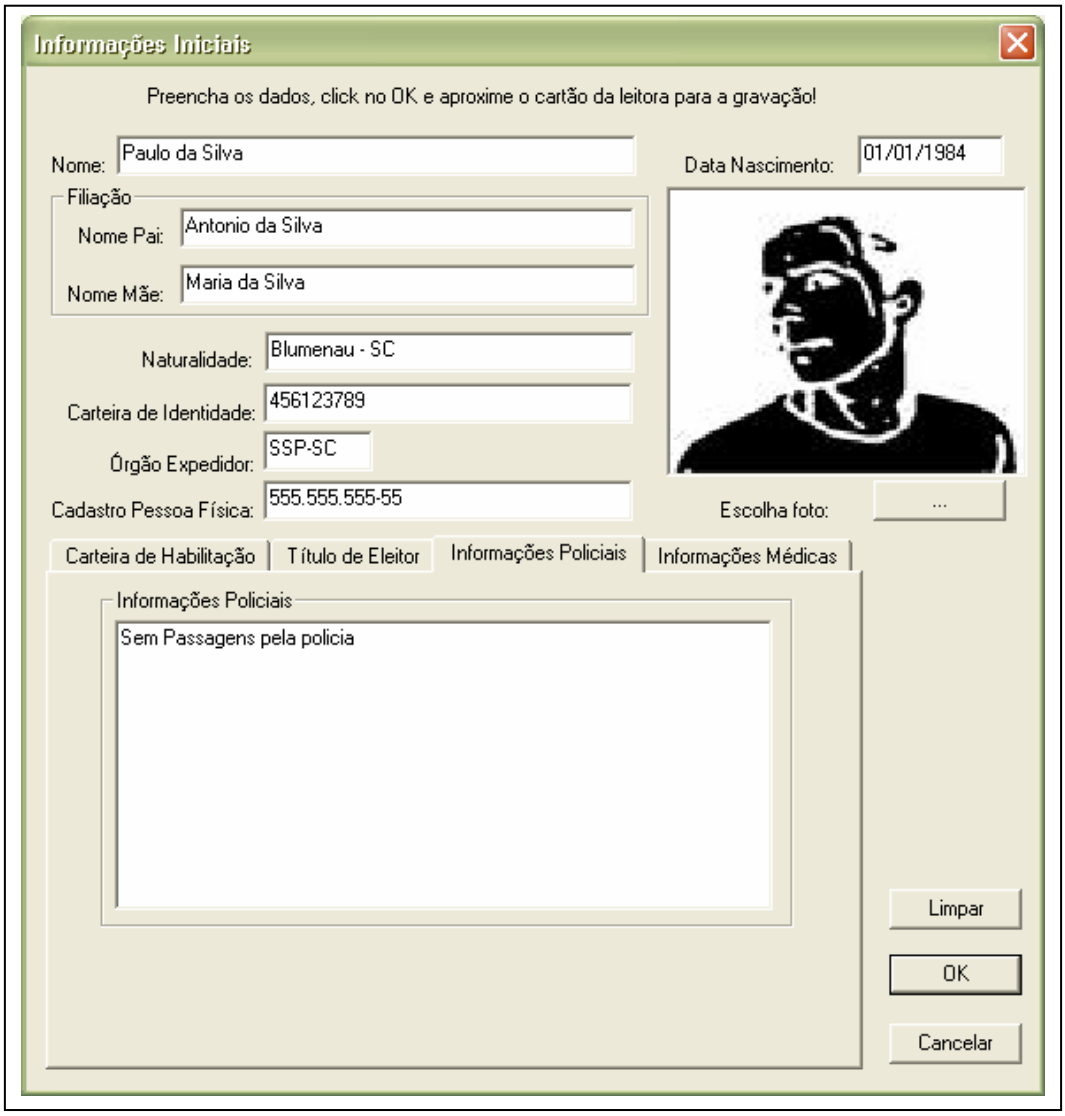


Figura 21 – Cadastro de passagens pela polícia.

E na última *tab*, figura 22, as informações médicas da pessoa. Nesta *tab*, podem ser cadastradas doenças graves que a pessoa teve ou ainda possui, algum tipo de alergia a medicamentos entre outras informações que os médicos acharem convenientes.

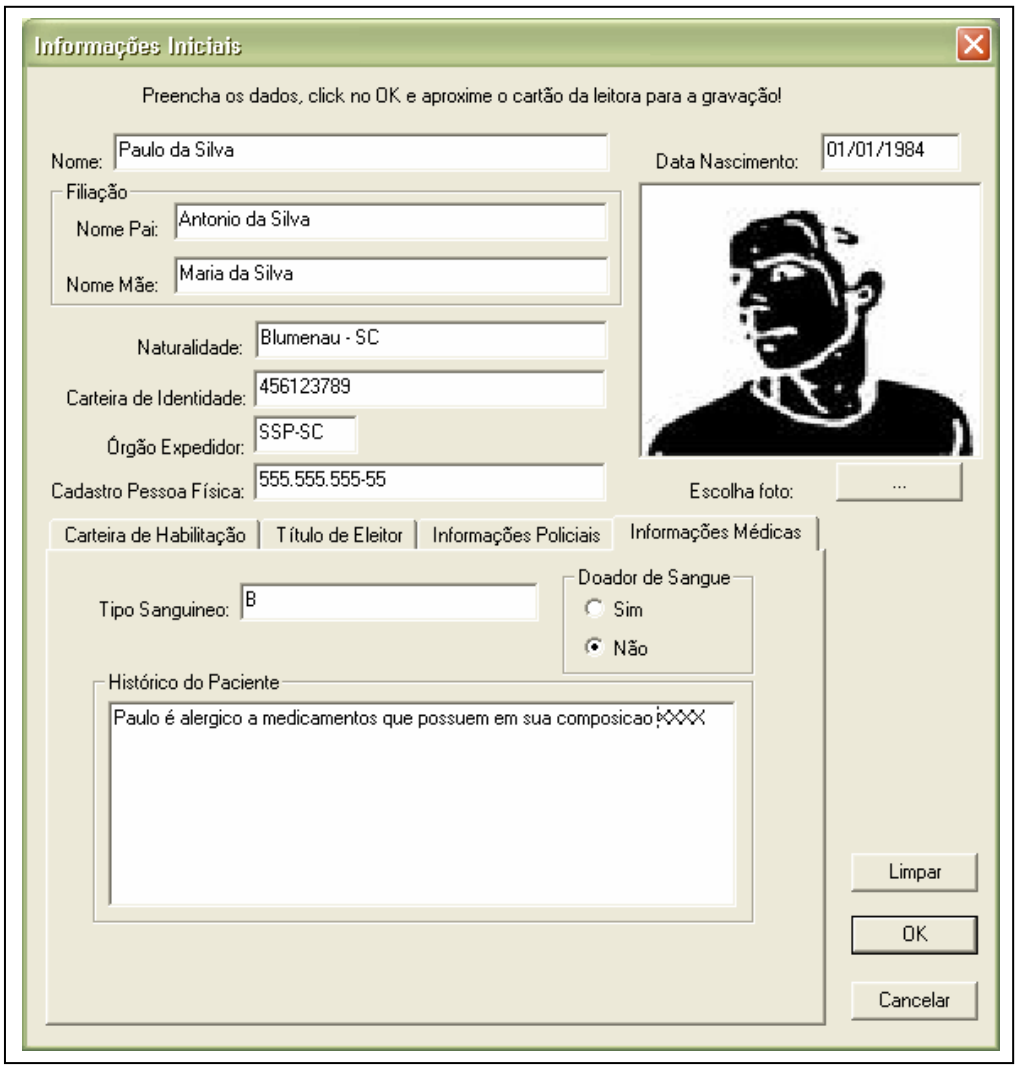


Figura 22 – Cadastro de Informações médicas.

Tendo finalizado o preenchimento de todas as informações necessárias, é só confirmar, clicando no OK, e depois aproximar o cartão da leitora para que possa ser atribuído para este cadastro o número do cartão que será destinado à pessoa cadastrada.

3.3.3 Características

Para que o sistema possa funcionar corretamente, é necessário possuir uma leitora e cartões de RFID. E para isso também se faz necessária à comunicação com a porta serial da máquina para obter as informações que são enviadas pela leitora.

O código fonte detalhado desta comunicação está no Quadro 10.

```
void CIniciais::OnXponderROMicroleitorctrl1(LPCTSTR sXponder)
{
	if(! m_bBtCadastrar)
	{
		CDBCadPessoa   dbCadPessoa(&m_DB);
		dbCadPessoa.m_strFilter.Format("Cod_Pessoa = '%s'",sXponder);
		try
		{
			dbCadPessoa.Open();
			if  (dbCadPessoa.IsEOF())
				AfxMessageBox("CPF não cadastrado na Base de Dados!");
			else
			{
				strcpy(m_sCodigoPessoa, sXponder);
				DadosBaseToTela(&dbCadPessoa);
			}
			dbCadPessoa.Close();
		}
		catch(CException* pE)
		{
			pE->ReportError();
			pE->Delete();
			return;
		}
	}
	else
	{
		CDBCadPessoa   dbCadPessoa(&m_DB);
		dbCadPessoa.m_strFilter.Format("Cod_Pessoa = '%s'",sXponder);
		try
		{
			dbCadPessoa.Open();
			if  (dbCadPessoa.IsEOF())
			{
				strcpy(m_sCodigoPessoa, sXponder);
				CString nome = m_Ctrl_Nome.GetTexto();
				CString cpf =  m_Ctrl_NumeroCPF.GetTexto();
				if(strcmp(nome, "") || strcmp(cpf, "") )
				      Gravar(&dbCadPessoa);
			}
			else
			{
				strcpy(m_sCodigoPessoa, sXponder);
				DadosBaseToTela(&dbCadPessoa);
			}

			dbCadPessoa.Close();
		}
		catch(CException* pE)
		{
			pE->ReportError();
			pE->Delete();
			return;
		}
	}
}
```

Do autor

Quadro 10 – Trecho do código fonte de comunicação com a porta serial

Esta função é chamada pelo MicroLeitor.ocx. Este é um componente ActiveX que foi desenvolvido pelo Sr. Werner Keske, ele é responsável pelo monitoramento da porta serial. Quando alguma informação for enviada pelo leitor, esta função é chamada, passando por parâmetro a informação que foi enviada do leitor para a porta serial.

A informação que é obtida é um código identificador único para cada cartão. Ao contrário do que foi especificado, conforme esclarecido na próxima seção “Resultados e Discussão”, por não ter sido possível gravar os dados básicos no cartão, estes tem que ser

obtidos desde a base de dados através da chave representada pelo identificador.

Se a tela que está sendo acessada neste momento pelo usuário do sistema, for de consulta, o sistema passará o código enviado pelo leitor para a base de dados, e ela retornará o registro encontrado. Caso não encontre nenhum registro com este código, o sistema apresentará em uma tela a mensagem de que não existe este CPF cadastrado na base de dados.

Mas, se as informações foram encontradas, o sistema irá apresentá-las em tela.

Caso a tela que está sendo usada pelo usuário, for de cadastro de pessoas, o sistema verifica se já existe um registro no banco com este código, se não existir e foram digitadas informações na tela para gravação (para saber se existe informação, verifica se existe nome ou CPF na tela), é realizada a gravação dos dados no banco. Caso algum registro seja encontrado, os dados do mesmo são apresentados em tela.

A função que faz a gravação das informações no banco de dados pode ser vista no Quadro 11.

```
void CIniciais::Gravar(CDBCadPessoa *pDB)
{
	if ( pDB==NULL)
	{
		CDBCadPessoa oDB(&m_DB);
		/* faz um filtro no banco de dados, passando o código da pessoa */
		oDB.m_strFilter.Format("Cod_Pessoa = '%s'",m_sCodigoPessoa);
		try
		{
			oDB.Open(); /*Abre a tabela*/
		/*Diz para a base de dados que é uma alteração dos dados que já estão gravados*/
			oDB.Edit();
			if  (oDB.IsEOF()) /*Procura por toda a base pelo registro "filtrado"*/
			{
				AfxMessageBox("CPF não cadastrado na Base de Dados!");
			oDB.Close();
				return;
			}
			else
			{
/* caso o registro for encontrado,  pega as informações que estão na tela e jogar para os devidos registros na tabela  */
				DadosTelaToBase(&oDB);
/*se foi  informada alguma foto para este registro, seta as informações necessárias da mesma para efetuar a gravação*/
				if(oDB.m_Foto.m_dwDataLength > 0)
				{
					oDB.SetFieldDirty(&oDB.m_Foto);
					oDB.SetFieldNull(&oDB.m_Foto,FALSE);
				}
				oDB.Update(); /*atualiza o registro na base*/
				oDB.Close(); /*fecha a conexão*/
			}
		}
/*caso aconteça algum erro, apresenta uma mensagem de acordo com o ocorrido*/
		catch(CException* pE)
		{
			pE->ReportError();
			pE->Delete();
			return;
		}
	}
	else
	{
		/*caso seja uma nova inclusão, "avisa" a base que esta sendo gravado um novo registro*/
		pDB->AddNew();
		/*busca as informações da tela e atribui para os devidos campos da tabela*/
		DadosTelaToBase(pDB);
		if(pDB->m_Foto.m_dwDataLength > 0)
		{
			pDB->SetFieldDirty(&pDB->m_Foto);
			pDB->SetFieldNull(&pDB->m_Foto,FALSE);
		}
		pDB->Update();
		pDB->Close();
	}
}
```

Do autor

Quadro 11 – Trecho do código fonte de gravação no banco de dados

A função apresentada é extremamente simples, é através dela que são efetuadas as gravações de novas informações no banco de dados, e também a atualização de registros que já estão na base. Para cada uma das tabelas existentes no banco de dados, existe uma função igual a esta para fazer a gravação/atualização das informações.

Para gravar a figura que foi adicionada ao registro na tela, no banco de dados, a imagem é primeiramente “jogada” para uma área de memória global, onde o banco também possa ter acesso à mesma, como mostrado no código fonte do quadro 12.

```
/*primeiramente verifica se existe figura vinculada*/
if(strcmp(m_sNomefigura, ""))
{
	CFile		fileImage;
	CFileStatus	fileStatus;

	/*abre a figura selecionada*/
	fileImage.Open(m_sNomefigura, CFile::modeRead);

	/*busca as informações sobre ela*/
	fileImage.GetStatus(fileStatus);

	/*Atualiza o Tamanho do Blob, campo da figura no banco de dados*/
	pDB->m_Foto.m_dwDataLength = fileStatus.m_size;
	/* Aloca uma área de memória Global*/
	HGLOBAL hGlobal	= GlobalAlloc(GPTR,fileStatus.m_size);
	/* "Trava" essa área e atribui para o Blob*/
	pDB->m_Foto.m_hData = GlobalLock(hGlobal);
	fileImage.ReadHuge(pDB->m_Foto.m_hData,fileStatus.m_size);
	m_sNomefigura[0] = 0;
}
```

Do autor

Quadro 12 – Trecho do código fonte de gravação da foto no banco de dados

Observa-se que se existir figura selecionada, ela é aberta, as propriedades da mesma são buscadas e o campo da figura no banco de dados é atualizado com o tamanho da mesma. Depois disso, uma área de memória global é criada, com o tamanho da figura selecionada. E por fim, atribuída a foto para o campo de destino no banco de dados.

3.4 RESULTADOS E DISCUSSÃO

3.4.1 Testes realizados

Os testes começaram a ser efetuados assim que o sistema estava pronto. O primeiro teste efetuado foi de conexão com o banco de dados, pois, no momento de informar usuário e senha, já existe a primeira conexão. Com esta conexão funcionando corretamente, verificou-se se os dados que estavam sendo gravados na tabela de usuários do sistema e de grupos de usuários estavam sendo gravadas também na base de dados. Constatado que as informações estavam sendo gravadas e lidas de forma correta, o próximo passo foi testar a comunicação com a porta serial.

Após, o passo mais importante, realizar a gravação das informações de pessoas. Informados todos os dados necessários, passado o cartão próximo a leitora, e por fim, os dados estavam gravados corretamente no banco de dados. Com os dados gravados, o último teste é verificar se passando o cartão próximo a leitora, os dados seriam apresentados corretamente em tela. Testes efetuados, e informações apresentadas conforme foram gravadas no banco.

Quando foi iniciado o presente trabalho, a empresa HidCorp gentilmente cedeu os equipamentos, um leitor/gravador, alguns cartões regraváveis e o protocolo de comunicação da leitora para a implementação das funções necessárias. Mas, no decorrer dos estudos verificou-se que a empresa utiliza em sua estrutura de leitura e gravação uma senha. Esta senha precisa ser fornecida para o equipamento de leitura antes de realizar qualquer operação. Antes de realizar uma simples leitura, ou seja, obter as informações que foram lidas pelo equipamento, faz-se necessário o envio de uma autenticação, para que o conteúdo do cartão possa ser alterado somente por pessoas autorizadas.

Assim que foi constatada a necessidade da geração desta chave de autenticação, entrou-se em contato com a empresa, pedindo que fosse enviada a forma utilizada para geração desta chave. Depois de várias tentativas e pedidos, inclusive colocando a disposição qualquer tipo de documento da universidade para comprovar o uso da tecnologia para fins acadêmicos, a empresa comunicou que a geração desta chave é uma DLL desenvolvida por eles e que ela faz parte do pacote de comercialização dos equipamentos. Para obter a mesma

seria necessária a compra dos equipamentos que inicialmente foram enviados em forma de empréstimo e mais da DLL, resultando em um valor considerável, o que dificultou a concretização do objetivo inicialmente estabelecido.

Para que o trabalho tivesse continuidade, conseguiu-se com a empresa WK Sistemas, pela pessoa do Sr. Werner Keske, como já foi citado, um leitor da empresa Texas Instruments e alguns cartões com *tag* RFID. Mas infelizmente estes cartões não são regraváveis, ou seja, são cartões com característica de somente leitura. São *tags* do tipo SAW, ou seja, já saem de fábrica com um número armazenado em sua memória que não pode ser alterado.

Isso fez com que ocorressem mudanças na forma inicial do projeto. Ao invés de armazenar informações no cartão, e utilizar o CPF como chave de pesquisa na base de dados, a solução encontrada foi armazenar no banco de dados, juntamente com os dados cadastrais, o código do cartão que será associado à pessoa e realizar as pesquisar utilizando este código.

Uma das principais desvantagens da mudança que houve diz respeito justamente ao acesso às informações, pois, com a proposta inicial de possuir os principais dados de identificação gravados no cartão, qualquer pessoa, em qualquer local, com um leitor de RFID e um micro computador, poderia identificar a pessoa sem ter a necessidade da conexão com a base de dados. Com a mudança, infelizmente faz-se necessária a conexão com o banco de dados para obter acesso a qualquer informação cadastrada.

3.4.2 Comparação com trabalhos correlatos

Atualmente, não encontra-se no mercado nenhum sistema que faça a integração de todos os documentos pessoais, ou o armazenamento das principais informações de cada indivíduo.

Como já foi apresentada anteriormente, a criação de um documento digital já foi citada em artigos de conclusão de curso (BEHNKE, 2004), mas neste caso, seria somente um documento, que não teria ligação alguma com outras informações e documentos.

Já no que diz respeito a utiliza a tecnologia de rádio freqüência, podemos citar vários sistemas, como os pedágios que já estão inclusive sendo usados em algumas estradas brasileiras, sistema este que já foi citado neste trabalho.

Rezena (2006), em seu trabalho de conclusão de curso, desenvolveu um sistema para controle de entrada e saída de ônibus de uma rodoviária usando para isso, a tecnologia de

RFID.

Várias podem ser as aplicações criadas utilizando esta tecnologia, mas, devido ao custo, e ao medo que está ligado a esta tecnologia, medo de perder informações ou ter as mesmas roubadas ainda impede o seu avanço.

Segundo informações obtidas juntamente com a empresa HidCorp, o valor de um leitor/gravador de RFID (figura 02), modelo simples, sem visor, gira em torno de setecentos reais (R$ 700,00), e as etiquetas em forma de cartão (figura 23), giram em torno de doze reais (R$ 12,00) cada uma.

Fonte: HidCorp

Figura 23 – iCLASS Card

Levando estes valores em consideração, dependendo da quantidade de equipamentos que uma empresa precisa para realizar o controle que necessita, o valor pode chegar a ser considerado alto.

4 CONCLUSÕES

Neste capítulo são analisados e discutidos os resultados e as dificuldades encontradas durante o desenvolvimento deste trabalho.

Apesar de já existirem alguns trabalhos publicados sobre a tecnologia de rádio freqüência, ela ainda é pouco conhecida pelas pessoas. Ainda existem muitos padrões a serem definidos quanto ao RFID. Como mostrado no desenvolvimento do trabalho, não existe uma forma única de armazenar as informações nas *tags*. Cada empresa que desenvolve e trabalha com esta tecnologia desenvolve sua própria forma, o que impede um avanço maior nesta área.

Esta falta de um padrão para desenvolvimento impediu que este trabalho fosse realizado da forma prevista inicialmente.

Conforme descrito no capítulo anterior, devido a problemas durante o desenvolvimento do trabalho, mais especificamente a falta de informações por parte da empresa que forneceu os equipamentos, um dos objetivos iniciais não pode ser atendido. Mas, para que o trabalho pudesse ser concluído e apresentado, a empresa WK Sistemas gentilmente cedeu os equipamentos que possuía, mas infelizmente os cartões por ela fornecidos não permitiam a gravação, pois vem de fábrica com identificador único. Isso fez com que a forma de pesquisar na base de dados sobre-se mudanças, passando a ser pelo identificador do cartão e não pelo CPF como previsto inicialmente. As conseqüências não foram somente estas, pois agora, para obter acesso a qualquer dado da pessoa, existe a necessidade da conexão com o banco de dados, diferentemente da forma inicialmente proposta.

Mesmo com a limitação imposta pela mudança, um objetivo foi atendido: conseguir unificar os documentos mais importantes em um só, diminuindo assim a quantia de papéis que precisam ser levados diariamente. E outro objetivo alcançado foi conseguir juntar a estes documentos outras informações que também são consideradas relevantes.

Um grande passo foi dado, pois, um levantamento inicial de informações importantes e foi feita uma estrutura inicial. Certamente não falta mais muito tempo para que este projeto que aqui foi apresentado, saia do papel e entre para a realidade de todas as pessoas. Para comprovar isso, há o exemplo do passaporte, que como foi mostrado no decorrer deste trabalho, já está migrando para uma versão digital, e usando inclusive a tecnologia que foi usada no SUIP, o RFID.

Apesar da questão segurança utilizando RFID ainda ser a geradora de grandes debates, a cada instante, surgem novidades sobre a tecnologia, ou seja, a qualquer momento pode

surgir uma forma de armazenar os dados que traga mais segurança para todos. Apesar das dificuldades encontradas durante o desenvolvimento do trabalho e das mudanças que foram necessárias, fica provado que a proposta ou modelo inicial do SUIP é possível de ser realizado.

Por fim, este trabalho veio engrandecer e muito em termos de conhecimentos pessoais, não somente sobre a tecnologia aqui utilizada, mas no que diz respeito a superação de dificuldades, afinal, diante dos fatos ocorridos a persistência e a vontade de fazer acontecer, foram ingredientes fundamentais.

4.1 FERRAMENTAS UTILIZADAS

Com exceção do mecanismo de gravação dos cartões da HidCorp que não nos foi fornecido, impossibilitando assim sua utilização, as ferramentas e os ambientes escolhidos para o desenvolvimento deste trabalho se mostraram ideais. Em nenhum momento apresentaram algum tipo de restrição para qualquer função necessária.

4.2 EXTENSÕES

Para que o SUIP tome sua forma do objetivo original, uma das extensões que podem ser feitas é tentar obter com outras empresas que também trabalham com esta tecnologia, os equipamentos necessários para obter a forma utilizada por eles para leitura e gravação e principalmente conseguir com eles a forma de cálculo utilizada para qualquer tipo de autenticação que seja utilizada nos cartões.

Ou ainda, fazer a aquisição dos equipamentos da HidCorp e da DLL que faz a geração da chave de autenticação, e assim conseguir fazer as operações de leitura e gravação nos cartões da forma com que havia sido prevista neste trabalho e como foi efetivamente especificado.

Outra possibilidade de extensão é tornar o SUIP um programa Web, incluindo mais informações no cadastro da pessoa, como por exemplo, histórico escolar, carteira de trabalho, passaporte, certidão de casamento, enfim, todo tipo de informação que possa ser útil, e faça

principalmente diminuir a quantidade de papéis que precisam ser arquivados em casa ou guardados na carteira.

Como este trabalho utiliza banco de dados, outra extensão possível é disponibilizar a base em um servidor, e todas as estações acessarem a base deste mesmo local, pois hoje, para que o sistema possa funcionar, a base precisa estar registrada na máquina em que se deseja operar o sistema.

REFERÊNCIAS BIBLIOGRÁFICAS

BEHNKE, Odair. **Carteira nacional de habilitação digital:** sistema de controle e emissão de notificações de trânsito. 2004. 12 f. Trabalho de Conclusão de Curso (Bacharelado em Sistemas de Informação) – Associação Educacional Leonardo da Vinci, Indaial.

BEZERRA, Eduardo. **Princípios de análise e projeto de sistemas com UML.** Rio de Janeiro: Campus, 2002.

BRAUN, Daniela. RFID: **Etiquetas inteligentes conquista território do código de barras.** São Paulo, 2006. Disponível em:< http://idgnow.uol.com.br/computacao_corporativa/2006/10/03/idgnoticia.2006-10-02.2435588597/?searchterm=Etiqueta%2520inteligente%2520conquista%2520territ%c3%b3rio%2520do%2520c%c3%b3digo%2520de%2520barras >. Acesso em: 04 abr 2007.

COMPUTERWORLD. **RFID está sujeito a fraudes, afirmam pesquisadores.** Sidney, 2006. Disponível em: < http://computerworld.uol.com.br/seguranca/2006/04/12/idgnoticia.2006-04-12.1739890681/IDGNoticia_view>. Aceso em: 04 abr 2007.

CONSELHO NACIONAL DE DESENVOLVIMENTO CIENTÍFICO E TECNOLÓGICO. **CNPq financia inovações em informação médica.** [S.l], 2003. Disponível em: <http://www.cnpq.br/noticias/150503.htm>. Acesso em: 29 jun. 2006.

EANBRASIL. Código EPC. São Paulo, 2007. Disponível em: <http://www.eanbrasil.org.br>. Acesso em: 20 maio 2007.

HIDCORP. Leitora/Gravadora RW300. [S.l] Disponível em: < http://www.hidcorp.com/português/prod_detail.php?prod_id=29>. Acesso em: 29 jun. 2006

HIGHTECHAID. RFID – The Technology. [S.l]. Disponível em: <http://www.hightechaid.com /tech/rfid/rfid_technology.htm>. Acesso em: 04 abr 2007.

INFO-AS. **RFID**. [S.l] Disponível em: <http://info-as.tripod.com/rfid.html>. Acesso em 05 abr 2007.

INOVAÇÃO TECNOLÓGICA. **Liberada utilização de chip de identificação pessoal nos EUA.** Campinas, 2004. Disponível em: <http://www.inovacaotecnologica.com.br/quem.html>. Acesso em: 20 maio 2006.

INOVAÇÃO TECNOLÓGICA. **Quebrada criptografia de etiquetas inteligentes RFID.** Campinas, 2005. Disponível em: < http://www.inovacaotecnologica.com.br/ noticias/noticia.php?artigo=010150050203>. Acesso em: 20 maio 2007.

LIMA, Adilson da Silva. **UML 2.0 do requisito à solução.** 1 edição. São Paulo: Érica, 2005.

LOES, João. **O RFID vai etiquetar o mundo.** [S.l] Disponível em: <http://wnews.uol.com.br/site/noticias/materia_especial.php?id_secao=17&id_conteudo=255>. Acesso em 22 mar 2007.

MEDALLIANCE. **Seus dados sempre acessíveis.** [S.l] Disponível em: <http://www.medalliance.com.br/produtos_e_servicos/prontuario.shtml>. Acesso em: 27 maio 2006.

PINHEIRO, José Mauricio Santos. **RFID Identificação por rádio freqüência.** Volta Redonda, 2004. Disponível em: <http://www.projetoderedes.com.br/artigos/artigo_identificacao_por_radiofrequencia.php>. Acesso em: 20 mar 2006.

PINHEIRO, José Mauricio Santos. **A evolução da revolução.** Volta Redonda, 2005. Disponível em: <http://www.projetoderedes.com.br/artigos/artigo_evulocao_da_revolucao.php>. Acesso em: 22 mar 2006.

PORTAL DA AUTOMAÇÃO. **Os prós e contras das RFID Tags, os chips que podem revolucionar a segurança.** [S.l.], 2004. Disponível em: <http://www.portaldaautomacao.com.br/materia_118.asp>. Acesso em: 21 mar 2006.

REZENA, Adriano Cosme. **Sistema para rastreamento de ônibus utilizando a tecnologia RFID.** 2006. 62 f. Trabalho de Conclusão de Curso (Bacharelado em Sistemas de Informação) – Centro de Ciências Exatas e Naturais, Universidade Regional de Blumenau, Blumenau.ç

SANTANA, Sandra Regina Matias. **RFID – Identificação por radiofreqüência.** 2005. Monografia - Curso de Tecnólogo em Informática com Ênfase em Gestão de Negócios. Faculdade de Tecnologia da Baixada Santista – Extensão Praia Grande.

SANTINI, Arthur Gambin. **RFID.** 2006. 83 f. Trabalho de Conclusão de Curso (Bacharelado em Sistemas de Informação) – Centro Universitário de Votuporanga. Votuporanga.

SERVIÇO FEDERAL DE PROCESSAMENTO DE DADOS. **A modernização do passaporte.** Brasília, 2004. Disponível em: < http://www.serpro.gov.br/noticias SERPRO/20041019_05>. Acesso em: 01 abr 2006.

SCHNOOR, Tatiana. **42 famílias no Brasil têm chips no corpo.** [S.l] 2006. Disponível em: < http://wnews.uol.com.br/site/noticias/materia_especial.php?id_secao=17&id_conteudo=215&id_coluna=5>. Aceso em: 14 mar 07.

TechGuru. Criado menor RFID do Mundo. [S.l] 2007. Disponível em: <http://www.techguru.com.br/post.aspx?cod=1599>. Acesso em: 14 mar 07.

WIKIPEDIA. **RFID.** [S.l] 2007. Disponível em: < http://pt.wikipedia.org/wiki/Rfid >. Acesso em: 05 abr 07.

ZEIDIN, Denise Carla dos Anjos. **Sistema de informação aplicado à integração da cadeia de suprimentos utilizando tecnologia RFID.** 2005. 88 f. Trabalho de Conclusão de Curso (Bacharelado em Sistemas de Informação) – Centro de Ciências Exatas e Naturais, Universidade Regional de Blumenau, Blumenau.