UNIVERSIDADE FEDERAL DE CAMPINA GRANDE
CENTRO DE ENGENHARIA ELÉTRICA E INFORMÁTICA
UNIDADE ACADÊMICA DE ENGENHARIA ELÉTRICA

TRABALHO DE CONCLUSÃO DE CURSO

SISTEMA DE LOGIN USANDO ETIQUETA RFID

Aluno
Tiago Carvalho Leite

Orientador
Prof. Dr. Bruno Barbosa Albert

Campina Grande, Abril de 2010

Sumário

Resumo

Este relatório foi desenvolvido como parte dos requisitos para obtenção do título de engenheiro eletricista através do Centro de Engenharia Elétrica e Informática - CEEI da Universidade Federal de Campina Grande (UFCG). Sendo realizado sob orientação do Prof. Dr. Bruno Barbosa Albert.

O objetivo do trabalho foi ampliar os conhecimentos da tecnologia de identificação RFID, partindo de um estudo teórico sobre ela e culminando com a montagem de uma aplicação prática, esta desenvolvida e implementada no Laboratório de Processamento de Sinais (LAPS). A aplicação consistiu da montagem de um sistema de *login* no sistema operacional Windows XP utilizando as etiquetas RFID como senha para os usuários.

No texto está o resultado da pesquisa teórica realizada antes da realização da implementação. Após a introdução, que dá uma visão geral da tecnologia, a secção 2 apresenta o resumo teórico, com as informações mais importantes a cerca de um sistema RFID. Discorrendo sobre os elementos que o compõe, sua classificação, características e aplicações.

Na secção 3 será descrito o sistema que será implementado, na secção 4 temos uma descrição do kit Phidgets USB 125 kHz e de suas etiquetas. Na secção 5 está todo o passo a passo para realizar a aplicação. Na secção 6 temos as conclusões sobre o trabalho.

1. Introdução

A tecnologia RFID (*Radio Frequency Identification*) é uma tecnologia de identificação automática (Auto-ID) que usa ondas de rádio para fazer sua identificação. Surgiu inicialmente como substituta de outra tecnologia Auto-ID bastante famosa, o código de barras. No lugar das listras paralelas pretas de largura diferentes o código no sistema RFID está nas *tags* (etiquetas ou *transponders*), que possuem um minúsculo chip com o código gravado e uma antena acoplada, que enviará o sinal com o código único guardado em uma memória do chip para o *reader* (leitor).

Com a evolução da tecnologia e o surgimento de etiquetas com memórias regraváveis e aumento do alcance e velocidade de leitura seu uso passou a ser mais abrangente. Além de identificar produtos em ambientes comerciais e industriais (substituindo o código de barras) o RFID é também utilizado para identificar pacientes em hospitais, veículos de carga e animais silvestres e de criação, sistemas de localização e aquisição de dados, com uso promissor em biossensores. Em controle de acesso substitui as chaves comuns, fáceis de serem copiadas.

O RFID tem vantagens frente às tecnologias que procura substituir. Seu sistema é de fácil leitura, o objeto a ser lido não precisa estar necessariamente no campo de visão do leitor, como ocorre com o código de barras. O alcance de leitura também é superior, mesmo para sistemas passivos (sem bateria para aumentar a energia do sinal). A quantidade de dados a serem armazenados e a possibilidade de regravação é outra importante vantagem dele.

O custo ainda é uma desvantagem em aplicações de larga escala, como identificação de produtos em supermercados. Mesmo com grande esforço do Wal-Mart (maior rede mundial de supermercados) ver etiquetas RFID substituindo os códigos de barras nos supermercados não está tão próximo como se previu, embora novas tecnologias para baratear seu custo de fabricação são pesquisadas continuamente e parece ser uma questão de tempo até que as etiquetas RFID cheguem aos produtos de supermercados. Um grande avanço nessa questão é visto em [8]. No entanto, em aplicações de menor escala, onde a eficiência é mais importante que o preço, o RFID já conquista grande parte do mercado.

O trabalho proposto para o Trabalho de Conclusão do Curso era implementar um sistema de *login* para um computador que usasse o cartão RFID como senha de acesso.

Utilizando para isso o kit *Phidgets*, já existente no Laboratório de Processamento de Sinais (LAPS), local onde foi desenvolvido o trabalho.

2. Resumo Teórico

2.1.Sistema RFID

Seja qual for a aplicação que o sistema RFID tenha os elementos que o compõe serão os mesmos, sendo eles: *tag*, *reader* e *host* (Figura 1). As *tags* são objetos que são acopladas ao objeto a ser identificado, possuindo um chip que armazena seu respectivo código de identificação. Elas possuem diversos tipos de encapsulamentos, que são feitos para se adequarem à sua aplicação. Assim existem pulseiras para identificar bebês e pacientes em hospitais, cartões em formato de cartão de crédito usados em sistemas de transportes coletivos urbanos, crachás para identificar e localizar funcionários e visitantes em museus, chaveiros para chaves de carro, etc.

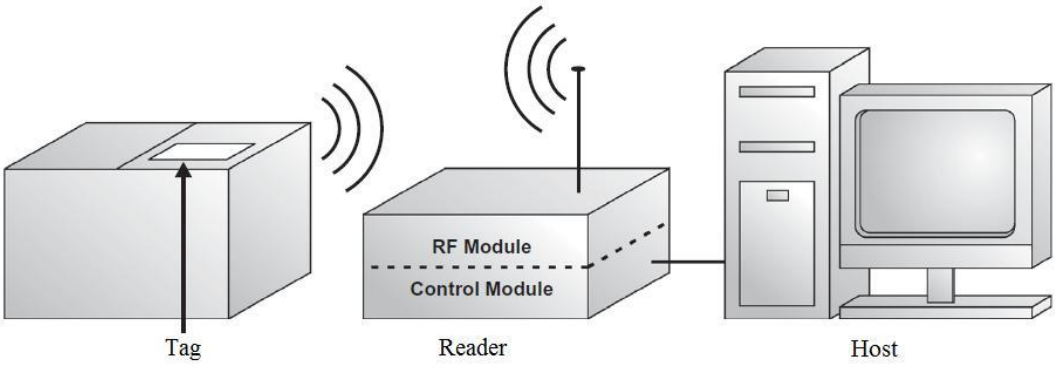


Figura 1: Componentes de um sistema RFID/Fonte [2]

O *reader* (leitor) é o dispositivo que interroga as *tags*, por meio de ondas eletromagnéticas enviadas pelo mesmo. Ele é geralmente conectado a um computador (*host*) ou outro componente para processamento da informação da *tag* e tomada de decisões.

O *host* pode ser não apenas um computador, mas também outros sistemas com capacidade de processamento, como microcontroladores, PDAs e CLPs. Para tanto cada *reader* tem uma ou mais portas de comunicação compatíveis com o *host* para com o qual foi projetado para trabalhar.

A transferência de dados nos sistemas RFID ocorre através de uma conexão entre a etiqueta e o leitor conhecida como acoplamento. O acoplamento pode ser do tipo magnético (indutivo) ou eletromagnético (*backscatter*). No acoplamento magnético o comprimento de onda do sinal emitido pelo leitor é várias vezes maior que a distância entre ele e a *tag*, o campo eletromagnético pode então ser tratado como um campo

magnético alternado com relação a distância entre a etiqueta e o leitor. No acoplamento eletromagnético trabalha-se em freqüências superiores as do caso anterior, e devido aos pequenos comprimentos de onda, não mais podemos simplificar a análise da onda em termos da componente magnética (Figura 2).

No acoplamento indutivo a *tag* absorve a energia enviada pelo leitor. Já no acoplamento *backscatter* a *tag* "reflete" a resposta de volta para o leitor (similar à operação de um radar).

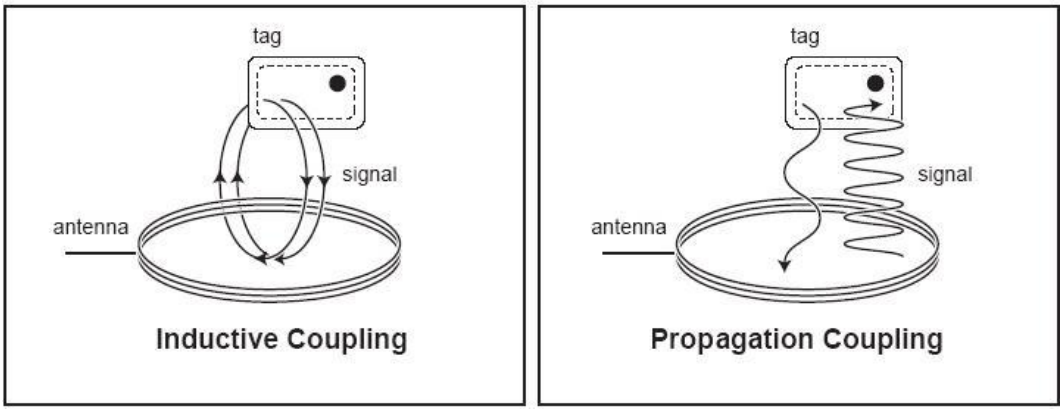


Figura 2: Acoplamento indutivo e backscater

2.2.Host

O *host* é o sistema computacional, dedicado ou não, que executará as tarefas de processamento para o sistema RFID em questão. O tipo de *software* a ser executado está associado com as características do *host*. É ele quem comanda as operações a serem realizadas pelo leitor. Cada leitor possui um protocolo de comunicação diferente com seu *host* e deve haver um *software* no *host* capaz de realizar essa comunicação.

2.3.Leitor

O leitor é o agente intermediário entre o *host* e a *tag*. É ele quem se comunica diretamente com as *tags*, através dos comandos do *host* ele executa uma operação (geralmente leitura de ID, escrita na memória ou leitura da memória) e responde ao *host* depois que finalizar sua comunicação com a *tag*.

No caso de etiquetas passivas, o leitor fornece a energia requerida para energizar a etiqueta por meio do seu campo eletromagnético. O alcance deste campo é geralmente determinado pelo tamanho da antena de ambos os dispositivos e pela potência do leitor.

O tamanho da antena geralmente é definido pelas necessidades da aplicação e da frequência utilizada. Geralmente a potência é bem baixa, visto que o alcance também é, aproximadamente até 15m para sistemas passivos.

A freqüência de operação pode variar de acordo com as especificações, padrões e regulações. O RFID utiliza as faixas de frequência regulamentadas peta ITU (*International Telecommunication Union*) conhecidas como ISM (*industrial, scientific and medical*). As faixas de freqüências mais comuns são:

- baixa freqüência (LF), 135 kHz ou menos, geralmente se utiliza 125 kHz;
- alta freqüência (HF), 13,56 MHz;
- ultra alta freqüência (UHF) a partir de 433MHz a 950MHz;
- e microondas entre 2,45 GHz e 5,8 GHz.

A freqüência está intimamente relacionada com a taxa de transferência de dados entre a etiqueta e o leitor. Quanto menor a freqüência, menor será a taxa de transferência. *Tags* passivas são construídas em frequências mais baixas, de 125 kHz até as faixas de UHF, enquanto a maioria das *tags* ativas está na frequência de 2,45 GHz, mas encontram-se também nas frequências de 433 MHz e 5,8 GHz.

2.4.Tags

As *tags* são compostas basicamente de um chip, onde está um circuito integrado (CI) com memória, uma antena para transmissão, e o encapsulamento, que protege as partes internas e possui estrutura própria para se acoplar ao objeto a ser identificado. Nas Figuras 3 e 4 temos imagens de etiquetas, a primeira é uma ilustração e a segunda uma foto de uma etiqueta de encapsulamento transparente do kit Phidgets. Por ela podemos ter uma noção de como é uma antena e um chip de uma etiqueta. Percebe-se claramente que a presença da antena em loop.

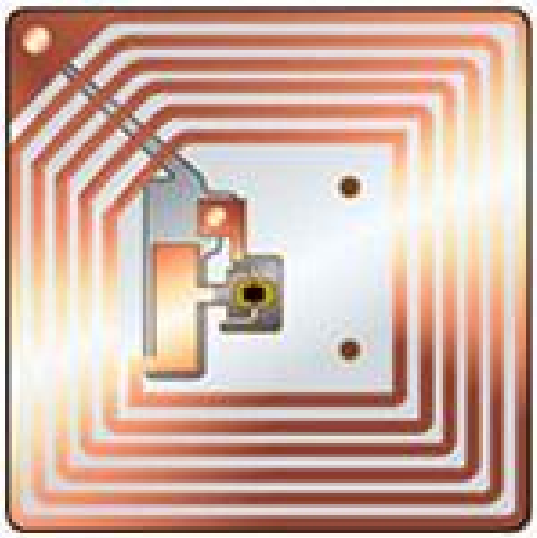


Figura 3: Estrutura interna de uma tag

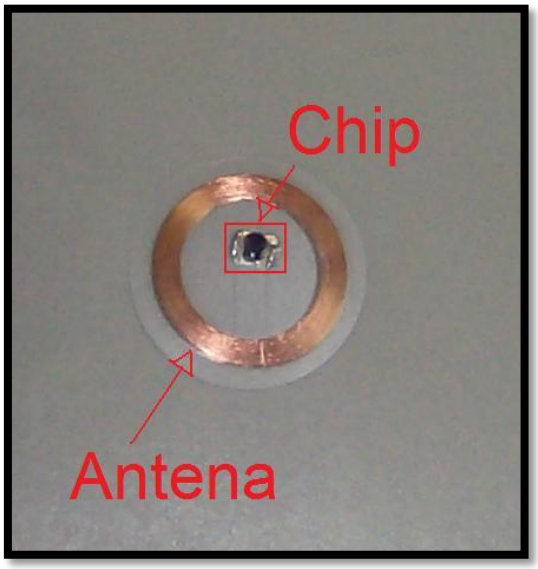


Figura 4: Tag de encapsulmanto transparente

As *tags* mais comuns hoje em dia possuem um circuito integrado (CI) com memória, essencialmente um microprocessador, mas existem *tags* que não possuem CI. Estas etiquetas são mais efetivas em aplicações onde simples funcionalidades são requeridas.

Quando uma *tag* é interrogada o dado em sua memória é transmitido. Ela pode executar tarefas básicas (leitura/escrita) ou manipular os dados em sua memória. A memória da etiqueta pode ser *read-write* (RW) ou *read-only* (RO). A capacidade de escrever na memória eleva o custo de uma etiqueta, assim como a capacidade de executar funções de alto nível. Uma vantagem de etiqueta somente leitura (RO) é a eliminação do risco de escrita acidental.

Em *tags* com memória RW ela em geral divide-se em duas partes. Uma fixa, chamada de ID, e outra regravável chamada de memória de dados. Também é possível encontrar *tags* que não fazem distinção dos dois tipos de memória, como também *tags* configuráveis, cuja memória pode ser uma memória de dados ou um ID, de acordo com a configuração.

As *tags* são classificadas quanto ao tipo de alimentação em passivas ou ativas.

***Tags* Passivas:** As *tags* passivas não possuem, em sua placa, uma fonte de alimentação (bateria), elas usam a energia emitida pelo leitor para suprir sua demanda e transmitir a informação de sua memória para aquele. Possuem boa resistência a ambientes rigorosos, pois não possuem partes móveis. Para este tipo de etiqueta, o leitor sempre inicia a comunicação. Sua faixa de alcance de leitura vai desde menos de 1cm até, aproximadamente, 15m. Uma grande vantagem das etiquetas passivas é que sua vida útil é virtualmente infinita. Uma vez que não necessitam de fonte de energia interna, enquanto não forem danificados estarão em funcionamento, assim ela possui vida útil virtualmente infinita. Existem *tags* passivas com memórias RO e RW.

***Tags* Ativas:** As *tags* ativas possuem uma fonte de energia interna e circuitos (ou equipamentos) eletrônicos para tarefas específicas. Utiliza sua fonte para transmitir dados ao leitor, não precisando da energia deste. Os circuitos eletrônicos podem conter microprocessadores, sensores e portas de entrada/saída alimentadas pela fonte interna. Desta forma, por exemplo, estes componentes podem medir a temperatura ambiente e gerar uma média. Os componentes podem utilizar esta informação para determinar outros parâmetros tais como a data de vencimento do produto ao qual a etiqueta está anexada. A etiqueta então envia estas informações para o leitor (junto com seu ID).

A comunicação, neste caso, pode ser iniciada pela *tag* ou pelo leitor. A *tag* pode transmitir continuamente mesmo na ausência de um leitor. Outro tipo de *tag* ativa permanece em estado de espera (estado de baixo consumo de energia - *sleep state*) na ausência de um leitor. O leitor então desperta a *tag* do *sleep state* a partir de um comando apropriado. A distância de leitura de uma etiqueta ativa pode chegar a 1km. Mas você não precisa trabalhar sempre na distância máxima. Para fins de economia de energia do leitor e da *tag* você pode configurá-los para trabalhar com área de cobertura menor.

Uma desvantagem comercial da etiqueta ativa é que ela, ao contrário da passiva, possui vida útil finita, determinada pela sua bateria. Como dito antes a *tag* pode entrar em modo de espera, com o objetivo de economizar sua bateria e aumentar sua vida útil. Em condições de operação, o tempo de vida útil médio de uma etiqueta ativa varia de 3 a 7 anos, mudando com o fabricante. A maioria dos produtos disponíveis no mercado apresenta vida útil de 5 anos.

Sistemas Ativos x Sistemas Passivos O que define um sistema RFID como ativo ou passivo é basicamente o tipo de etiqueta utilizada. Já foi visto a diferença básica entre as duas etiquetas. A ativa possui fonte de energia interna e a passiva não. Essa diferença faz com que um sistema ativo possua alcances de leitura e escrita muito maiores, assim suas aplicações se diferem baseadas nessa característica.

Por possuírem maior alcance de leitura as *tags* ativas são usadas em sitemas de localização e rastreamento. Para aplicações de curta e média distância *tags* passivas são mais recomendados, visto que o longo alcance das *tags* ativas é desnecessário ou mesmo desfavorável a suas aplicações. Sistemas passivos são usados em controle de acesso, sendo um substituto para chaves em portas tradicionais e para senhas em portas com trava elétrica. Para tanto usa-se geralmente cartões de 125kHz RO, como não necessariamente será preciso gravar informações no cartão de acesso uma memória RW adicional é dispensável. Mas caso deseje-se gravar algum tipo de informação, cartões com memórias também são encontrados.

2.5.Encapsulamentos

O encapsulamento é a carcaça responsável por dar proteção e formato à etiqueta RFID. Ele está intimamente relacionado com a função para o qual a etiqueta foi projetada. A seguir faremos uma abordagem sobre os principais tipos de encapsulamentos encontrados.

Os discos e moedas (Figura 5) são os mais comuns, muitos possuem um furo no meio próprio para serem parafusados em objetos, usados assim em ambientes industriais, para identificar produtos em linhas de montagem.

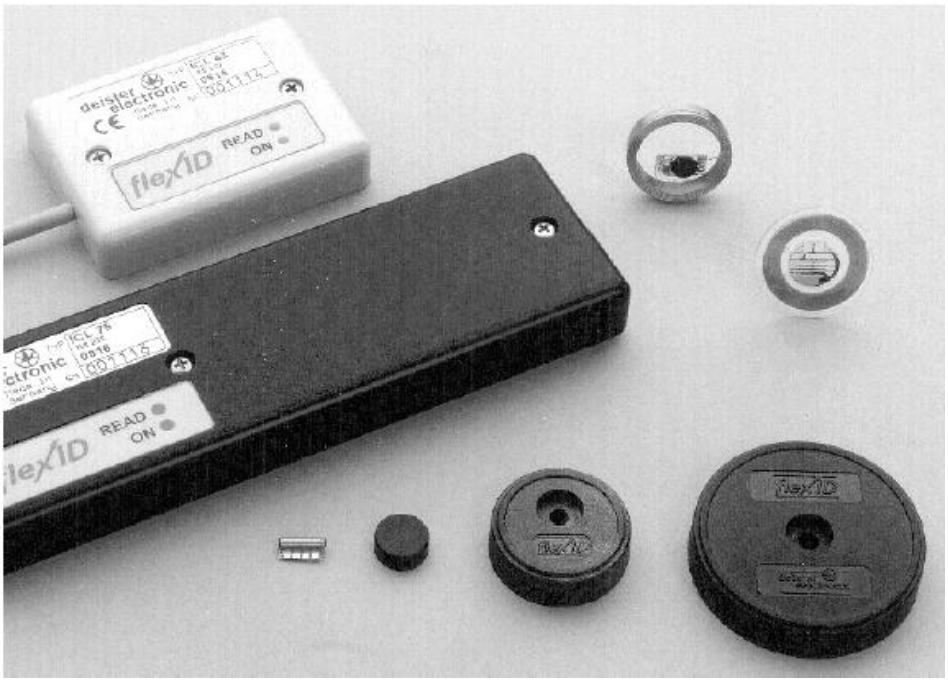


Figura 5: Discos e moedas / Fonte [2]

Os encapsulamentos de vidro (Figura 6) são usados em implantes para animais de criação e em animais silvestres, para pesquisas. Algumas etiquetas desse tipo estão sendo desenvolvidas para implante em seres humanos, vide exemplos no final deste relatório. Há também relógios (Figura 7) e chaveiros (Figura 8), que podem ser usados em controle de acesso. Existem chaveiros usados para substituir chaves de carro.

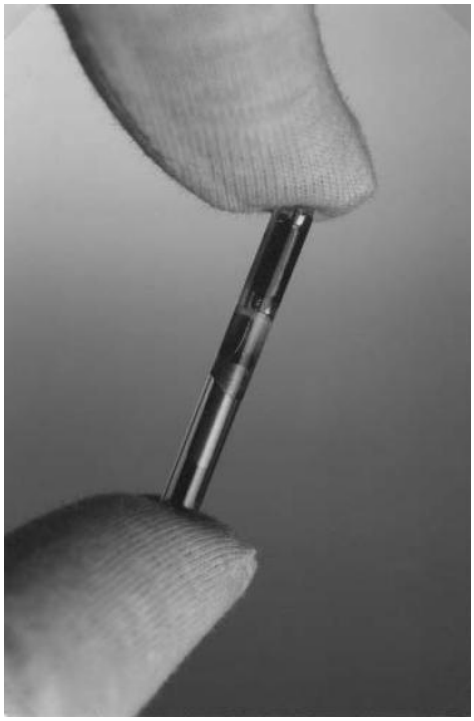


Figura 6: Encapsulamento de vidro / Fonte [2]

Figura 7: Relógios / Fonte [2]

Figura 8: Chaveiro / Fonte [2]

Os *smart cards* (Figura 9) também são usados em controle de acesso. Há ainda *smart cards* em com suporte para funcionar como crachá, sendo usados em sistemas ativos, para controlar funcionários e visitantes de locais como museus. Os *smart labels* (Figuras 10 e 11), são plásticos dobráveis, são usados pra identificar produtos, como caixas em supermercados. São eles que despontam como os substitutos dos códigos de barras em supermercados, várias pesquisas são feitas visando simplificar e baratear sua produção [8].

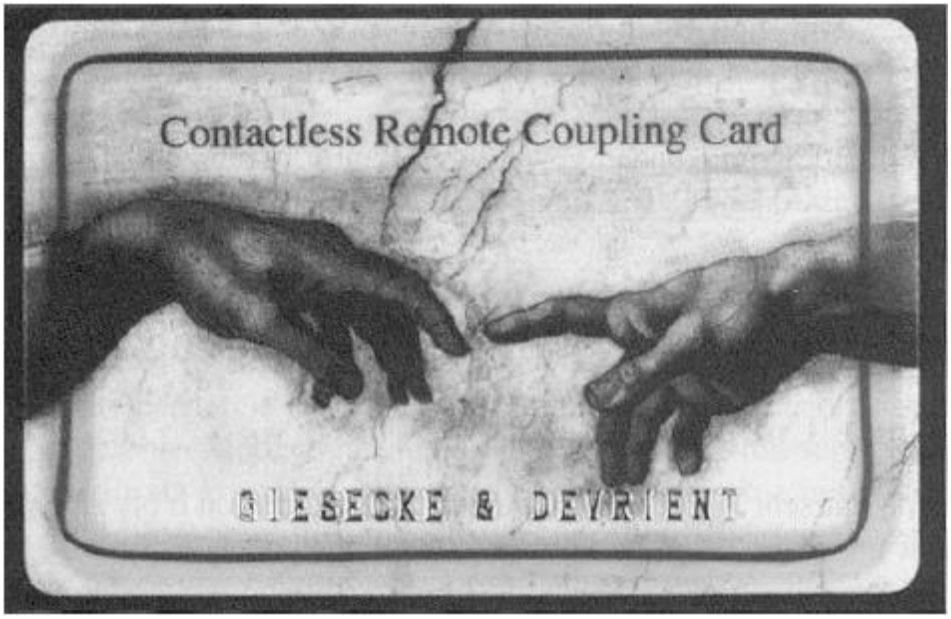


Figura 9: Smart Card / Fonte [2]

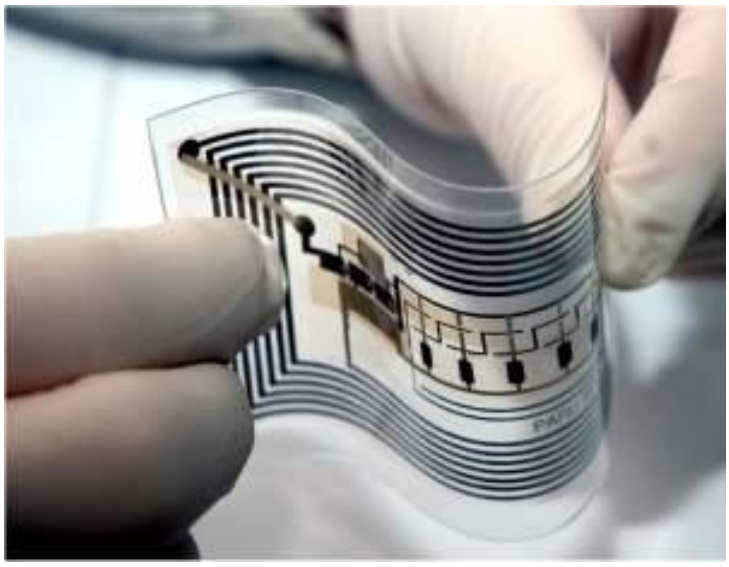


Figura 10: Smart Label / Fonte [8]

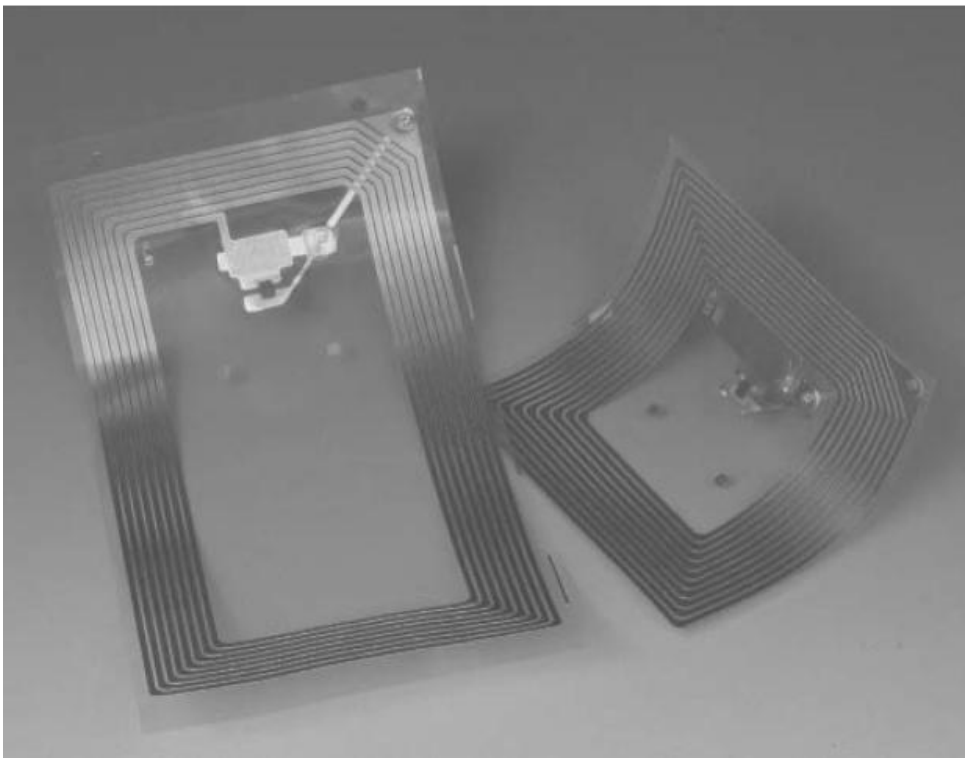


Figura 11: Smart Label / Fonte [2]

3. Descrição do sistema a ser implementado

A implementação proposta a ser feita foi fazer um sistema de Auto-login para computadores, no caso para o sistema operacional *Windows XP*. O kit utilizado foi o da empresa Phidgets, de frequência 125 kHz, que consiste do leitor, *Phidgets USB 125kHz RFID reader*, e de um conjunto de *tags* do tipo *Passive EM4102*.

No sistema de *login* do *Windows*, quando há mais de um usuário, ou quando o único usuário é protegido por senha, há uma tela onde você deve selecionar o usuário e posteriormente, caso o usuário seja protegido por senha, digitá-la. A idéia do sistema é substituir a digitação da senha por um cartão RFID. Com o sistema funcionando o que deve acontecer é o seguinte, ao invés de cada usuário digitar sua senha, ele apenas aproxima seu cartão, e o sistema irá liberar a máquina para o usuário do cartão correspondente. Paralelamente haverá um programa para fazer o cadastro de cartões e a associação deles aos usuários.

O responsável pela tarefa de *login* no sistema operacional é o *Windows* GINA, de *Graphical Identification and Authentication*, que é basicamente o que é visto na tela quando queremos fazer o *login.* Existe uma série de registros que indicam ao *Windows* que arquivo DLL ele deve usar para as funções do GINA. Para que o sistema de *login* com RFID funcione, o DLL original deve ser substituído por um novo, chamado PollGina.

Na verdade ele não faz uma substituição completa do DLL antigo. O PollGina cria uma nova camada de processos entre o *WinLogon* e o MSGINA.DLL. Caso a tentativa de *login* seja da maneira tradicional o processo é encaminhado para o DLL original do sistema operacional, caso a tentativa seja com o cartão RFID o processo é encaminhado para o mecanismo RFID. Uma diagrama do que foi explicado é mostrado na Figura 12. Assim mesmo com o sistema RFID em funcionamento não fica descartada a possibilidade do usuário utilizar a senha para acessar o computador.

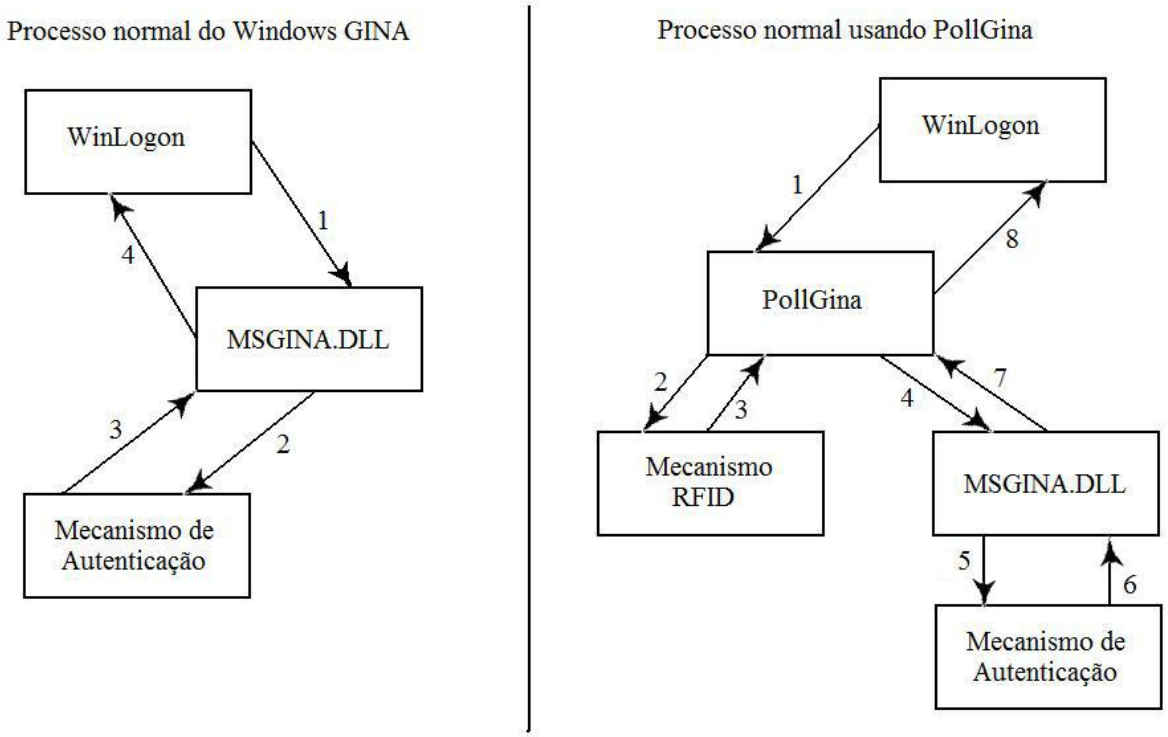


Figura 12: Processo de autenticação Windows GINA

4. Descrição do kit

4.1.Descrição geral

O kit consiste basicamente do leitor Phidgets USB 125kHz e do conjunto de *tags* EM4102. Como dito no próprio nome do leitor, ele se comunica com o *host* (computador) através da porta USB. O leitor não possui botão de *on-off*, assim ao ter sua entrada USB conectada no computador ele já estará ligado. Existem alguns programas exemplos disponíveis no endereço www.phidgets.com, na secção *Programming*, que servem para testar o funcionamento do leitor.

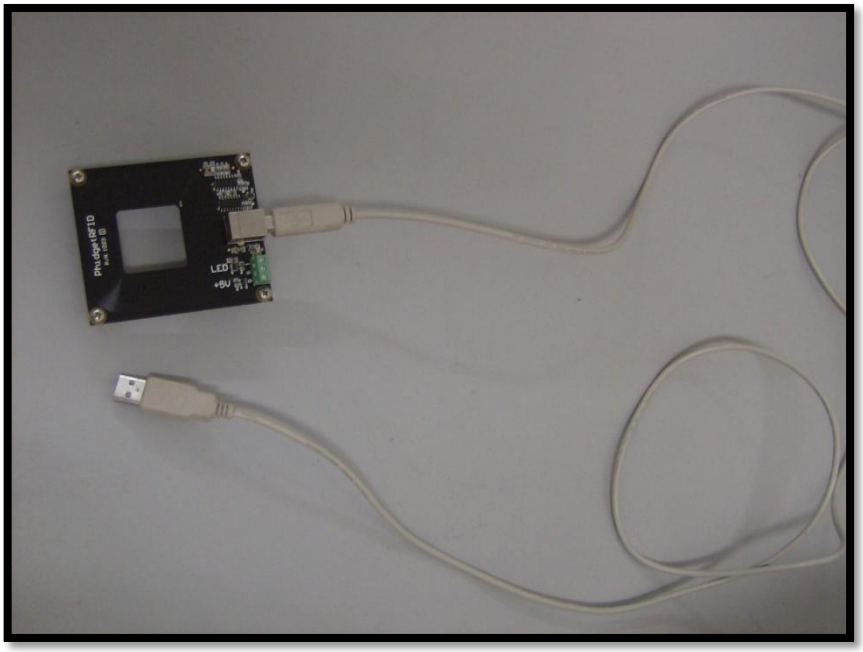


Figura 13: Leitor Phidgets USB 125 kHz

Figura 14: Conjunto de tags EM4102

No endereço www.phidgets.com/drivers.php estão disponíveis as bibliotecas, nelas estão contidas as funções utilizadas pelos programas que utilizam o kit, essas bibliotecas são chamadas de *Phidgets*. Para o sistema operacional *Windows XP* é necessário ter o ServicePack2 instalado para fazer a instalação do *Phidgets*, existe uma biblioteca para o sistema Linux também, que requer a versão *Linux Kernal 2.6+* para sua instalação.

Existem várias versões do arquivo de bibliotecas, quando for rodar algum programa é necessário conferir que tipo de versão da biblioteca ele utiliza, para evitar problemas de compatibilidade. Antes de implementar o sistema foi instalado um programa para testar se o leitor estava funcionando perfeitamente. O problema que surgiu foi que esse programa teste utilizava uma versão diferente da biblioteca, e quando o sistema foi implantado o cadastro de etiquetas não estava funcionando. A simples substituição de biblioteca, instalando a correta solucionou o problema.

4.2.Etiquetas EM4102

Os dados que serão mostrados nesta secção dizem respeitos às etiquetas EM4102, que são as usadas pelo kit Phidgets. Os dados foram retirados de um manual descritivo técnico da empresa EM Microeletronic.

O EM4102 (antes chamado de H4102) é um circuito integrado do tipo CMOS usado em *transponders* RF *Read Only*. O circuito é alimentado por um campo magnético externo, recebendo dele também o *clock master*. Quando ele é energizado ele manda um sinal RF de resposta com 64 bits de informação contidos em sua memória.

A taxa de dados pode ser igual a 64, 32 ou 16 vezes o período da frequência da portadora, como mostrado na Figura 15. Os dados são codificados com código de Manchester, Bifásico ou PSK (*Phase Shift Keying*). É preciso apenas uma bobina para suprir as funções do chip.

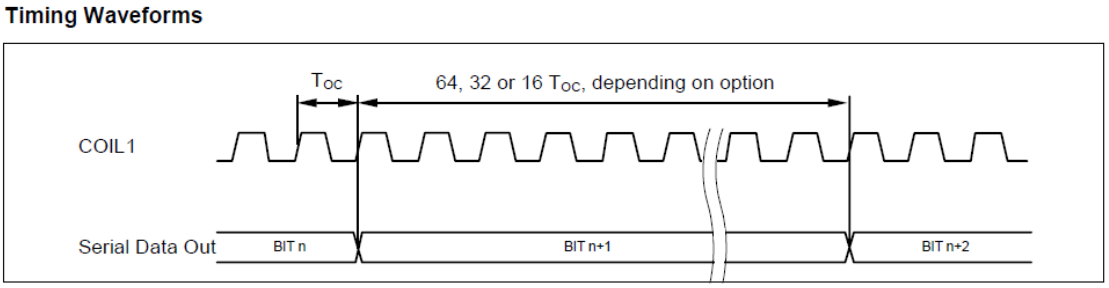


Figura 15: Fonte [4]

O fabricante define três aplicações para suas etiquetas:

- *Transponder* implantável em animais
- *Transponder* para orelhas de animais
- *Transponders* industriais

Na Figura 16 está um esquema simplificado do *tranceiver* (leitor) e do *transponder* (etiqueta), na Figura 17 o esquema do *transponder* é mostrado mais detalhadamente.

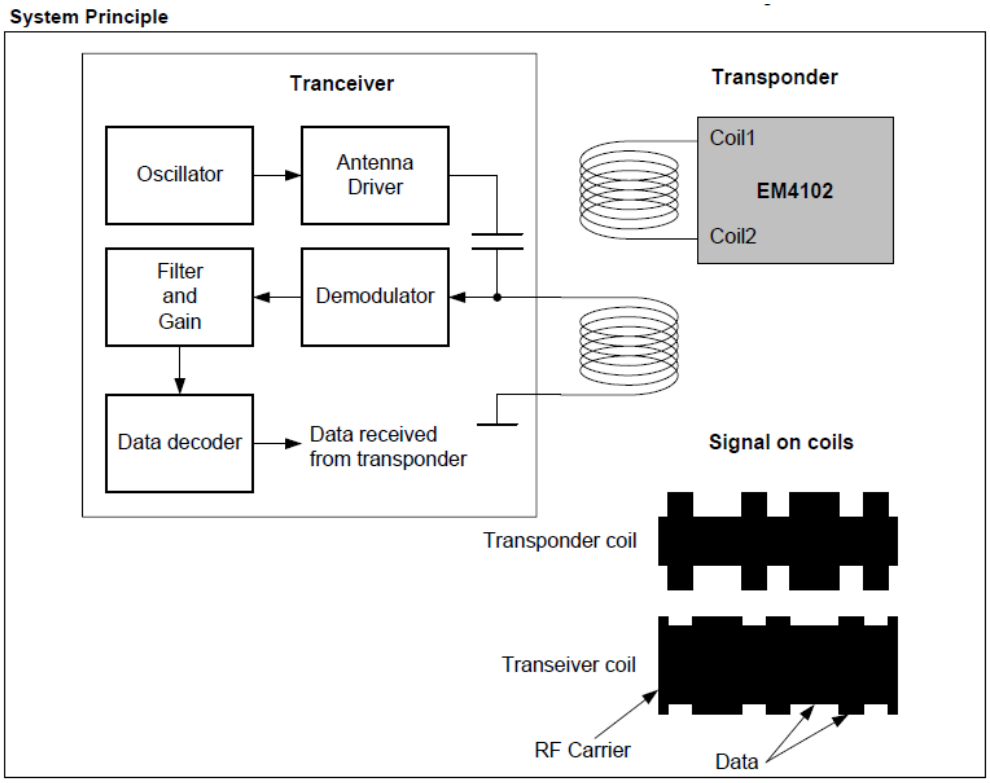


Figura 16: Tranceiver e transponder/Fonte [4]

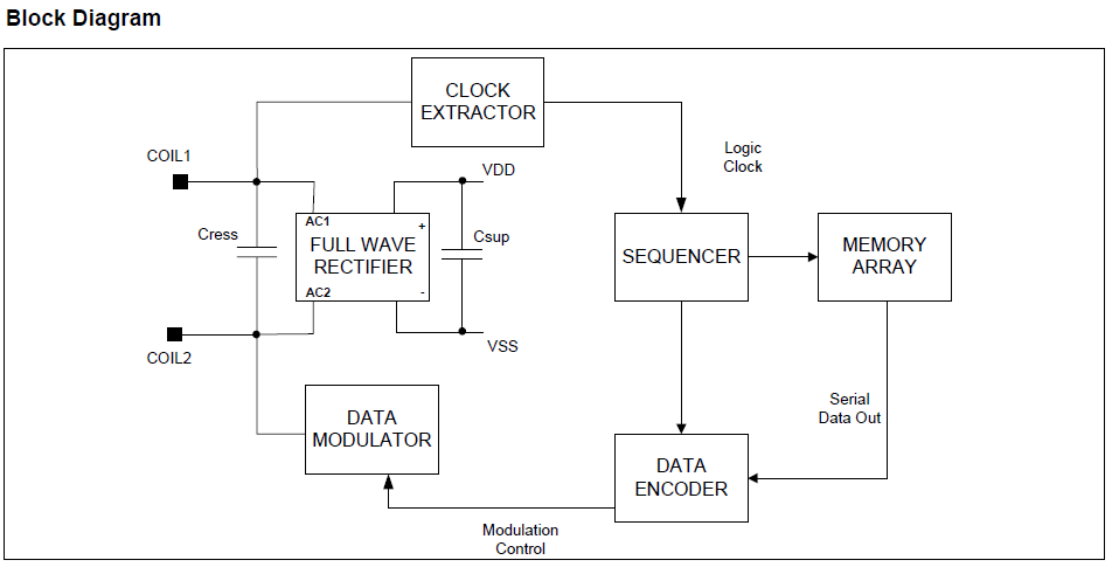


Figura 17: Transponder/Fonte [4]

A seguir é explicado cada bloco:

- **Geral:** O EM4102 é alimentado com um campo eletromagnético induzido na bobina do *transponder*. A voltagem AC é retificada para prover uma fonte de tensão interna DC. Quando o último bit é enviado, o chip continuará a mandar o sinal a partir do primeiro bit até que a fonte de energia desapareça.

- **Full Wave Rectifier:** A entrada AC induzida pelo campo incidente na bobina é retificado por uma ponte de Graetz. A ponte limita a tensão DC interna para evitar problemas com campos fortes.
- **Clock Extrator:** Um dos terminais da bobina (Coil 1) é usado para gerar um *master clock* para funções lógicas. A saída do *clock extractor* se dirige ao *sequencer*.
- **Sequencer:** O *sequencer* provê todo sinal necessário para endereçar a sequência de memória e codificar a saída serial de dados. Três tipos de codificações lógicas são possíveis, código de Manchester, bifásico e PSK. A taxa de bit para os dois primeiros pode ser 64 ou 32 períodos da frequência da portadora. Para a versão PSK, a taxa é 16. O *sequencer* recebe o *clock* do *clock extractor* e gera todo sinal interno que controla a memória e o codificador lógico de dados.
- **Data Modulator:** O modulador de dados é controlado pelo Modulation Control para induzir uma alta corrente na bobina. O transistor de Coil 2 carrega a alta corrente. Isto vai afetar o campo magnético de acordo com os dados estocados na memória.
- **Memory Array para codificação de Manchester e bifásico:** O EM4102 contém 64 bits divididos em 5 grupos de informação, 9 bits são usados para o cabeçalho, 10 bits de paridade para linhas (P0 – P9), 4 bits de paridade para colunas (PC0 – PC3), 40 bits de dados (D00 – D93), e 1 bit de parada com valor lógico 0. A estrutura dos dados é mostrada na Figura 11.

1	1	1	1	1	1	1	1	1	9 header bits
8 version bits or customer ID				D00	D01	D02	D03	P0	
				D10	D11	D12	D13	P1	
				D20	D21	D22	D23	P2	
32 data bits				D30	D31	D32	D33	P3	
				D40	D41	D42	D43	P4	
				D50	D51	D52	D53	P5	
				D60	D61	D62	D63	P6	
				D70	D71	D72	D73	P7	
				D80	D81	D82	D83	P8	
				D90	D91	D92	D93	P9	10 line parity bits
				PC0	PC1	PC2	PC3	S0	
				4 column parity bits					

Figura 18: Estrutura da memória/Fonte [4]

O cabeçalho é composto de 9 bits com todos os valores 1. Assim com a organização de dados e bits de paridade essa sequência não pode mais ser repetida. O cabeçalho é

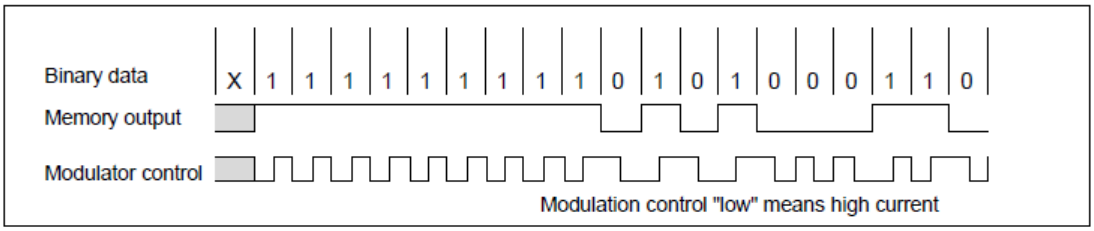
seguido por 10 grupos de 4 bits, permitindo 100 bilhões de combinações, há para esse grupo 1 bit de paridade par para cada linha. O último grupo consiste de 4 bits de paridade para colunas, sem um bit de paridade de linha para esta linha. S0 é o bit de parada que é sempre 0. Os bits D00 a D03 e os bits D10 a D13 são identificações específicas do cliente. Esses 64 bits são enviados de forma serial e quando o último bit é enviado o primeiro bit é enviado novamente, repetindo a sequência continuamente até que cesse a fonte de energia.

- **Memory Array para PSK:** O PSK é programado com paridade ímpar para os bits P0 e P1 e sempre com lógica zero. A paridade dos bits para P2 a P9 é par. A paridade de coluna PC0 a PC3 são calculadas incluindo os bits de versão e são de paridade par.

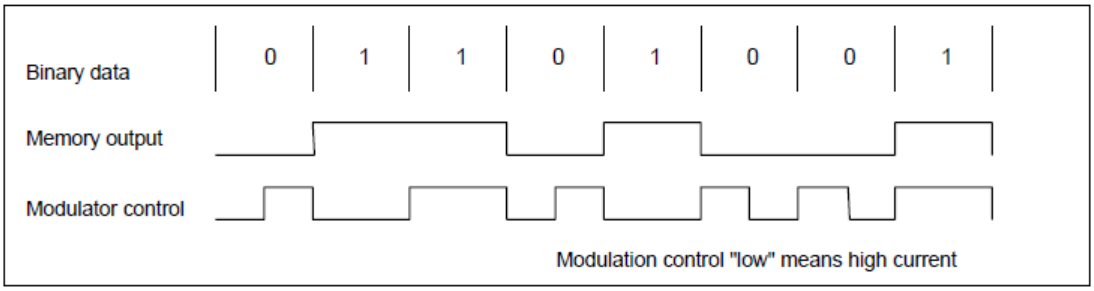
A seguir são explicadas as três codificações lógicas possíveis, na Figura 19 há um exemplo de sinal com cada uma das codificações para melhor explicá-las.

- **Manchester:** Há sempre uma transição de ON para OFF ou de OFF para ON no meio do período do bit. Se a mudança é de OFF para ON o bit lógico será 1, e se é de ON para OFF será 0. Assim quando ocorre uma mudança de fase no sinal do modulador ocorrerá uma mudança de bits nos dados.
- **Código Bifásico:** No início de cada bit uma transição sempre irá ocorrer. Se ocorrer uma transição de valor lógico no meio do período do bit o valor lógico do bit de dados será 0, se o valor lógico se mantiver durante todo o período do bit o valor lógico será 1.
- **PSK:** Quando uma mudança de fase ocorre, um 0 lógico é lido da memória. Se nenhuma mudança de fase ocorre depois do ciclo da taxa de dados um 1 lógico é lido.

Manchester Code



Biphase Code



PSK Code

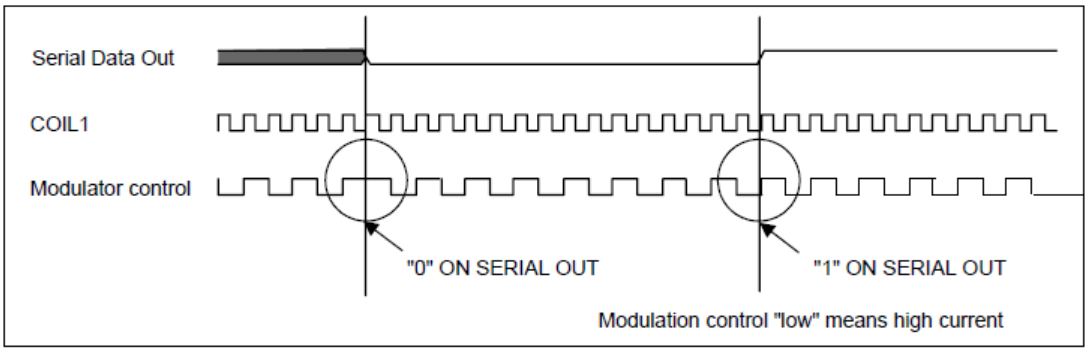


Figura 19: Codificações/Fonte [4]

5. Implementação

5.1. Instalação e Edição de Registro

Uma vez que o kit está instalado e testado podemos fazer agora a implementação. Como serão feitas modificações no registro do sistema operacional, uma área de risco para ser alterada, é recomendável fazer um *backup* e um ponto de restauração do sistema para evitar que qualquer erro comprometa o computador.

O primeiro passo é fazer o download do pacote de software RFIDGina, que está no endereço **www.rfidtoys.net** na secção **Downloads** e subsecção **RFIDGina (chapter 4)**. RFIDGina é uma coleção de arquivos de softwares que permitem ao leitor RFID atuar como um dispositivo de autenticação. A seguinte lista de arquivos está presente no pacote baixado.

- **PollGina.dll:** o arquivo que irá substituir o GINA original
- **RFIDAuth.exe:** usado para associar as tags RFID com as contas
- **RFIDGina.reg:** Arquivo de registro com as configurações do RFIDGina
- **rfidPoll.dll:** A biblioteca RFID para o PollGina

O arquivo compactado contém PollGina e rfidPoll. PollGina é usado para interagir com o sistema de autenticação Windows GINA, e rfidPoll é basicamente um plug-in que liga o leitor Phidgets RFID ao PollGina.

Não há instalador para o PollGina. Depois de descompactar os arquivos, devemos simplesmente mover os arquivos PollGina.dll e rfidPoll.dll para a pasta padrão do Windows, que é usualmente C:\WINDOWS. Como dito anteriormente é necessário editar o registro, algumas entradas de registro precisam ser modificadas e outras adicionadas para que o RFIDGina funcione.

Se a instalação do Windows foi padrão, ele foi instalado na pasta C:\WINDOWS. Uma vez que os arquivos PollGina.dll e rfidPoll.dll foram copiados para a pasta do Windows pode-se simplesmente usar o arquivo RFIDGina.reg para atualizar as configurações de registro. Um simples duplo-clique em RFIDGina.reg importa as configurações corretas de registro, você será perguntado para confirmar a operação, como mostrado na Figura 20. Clique em Yes (ou Sim, dependendo da configuração de idioma do seu Windows) e a tela da Figura 21 aparecerá. É preciso estar usando uma conta de administrador ou a operação irá falhar. É preciso lembrar também que as modificações de registro só surtirão efeito quando o computador for reiniciado.

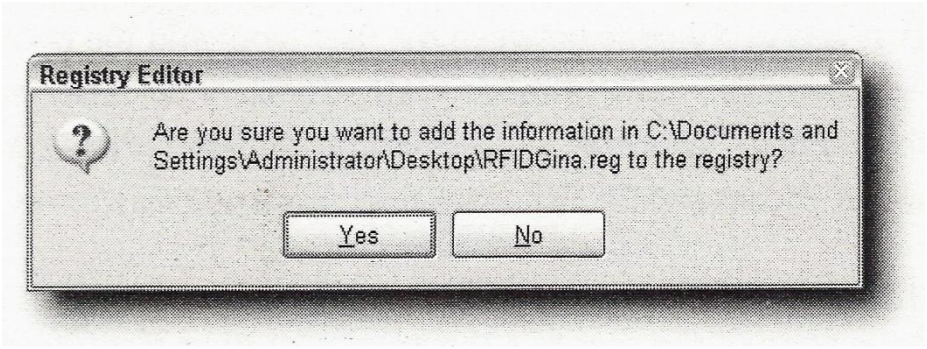


Figura 20

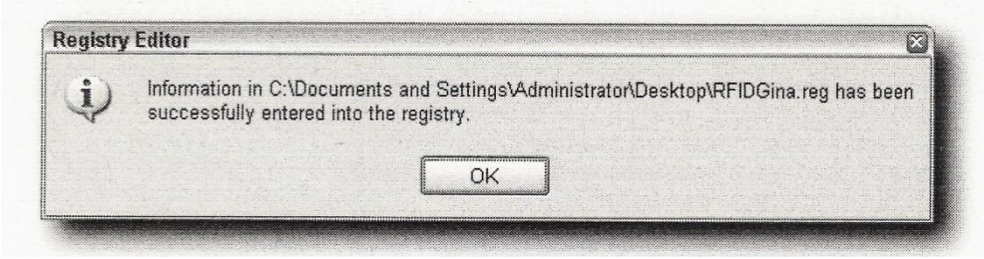


Figura 21

Atualização Manual do Registro

Se a instalação do Windows não foi padrão, a atualização de registro deve ser feita manualmente. No computador do laboratório onde foi feita esta implementação o Windows estava instalado em sua pasta padrão, mas como a primeira tentativa de execução do sistema foi falha, fiz a atualização de registro manualmente, achando que o erro pudesse ter sido nesse passo. Posteriormente verificou-se que o erro era decorrente da incompatibilidade de versão da biblioteca Phidgets que estava instalada, porque o programa que foi usado para testar o funcionamento do leitor utilizava uma versão diferente da biblioteca. De qualquer forma será descrito como fazer a atualização manualmente para que qualquer pessoa possa repetir a implementação em qualquer outro computador.

Para abrir o editor de registro faça os passos: Start(Iniciar) → Run → regedit. A primeira coisa a ser feita é mudar o GINA padrão para o PollGina, para fazê-lo você tem que adicionar ou modificar o valor string de GinaDLL (REG_SZ). Comece navegando para a chave de registro:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\WinLogon

Procure por um valor chamado GinaDLL. Se já houver uma string com esse nome, você deve modificar seu valor. Se não existe, você deve adicionar um novo valor string clicando em Edit → String Value como mostrado na Figura 22. Nomeie a nova string como GinaDLL, lembrando que o sistema é case-sensitive (diferencia caracteres maiúsculos e minúsculos). O valor de GinaDLL deve ser preenchido com o caminho completo do arquivo rfidPoll.dll, que foi copiado para a pasta padrão do sistema operacional. A Figura 23 mostra um exemplo do caminho.

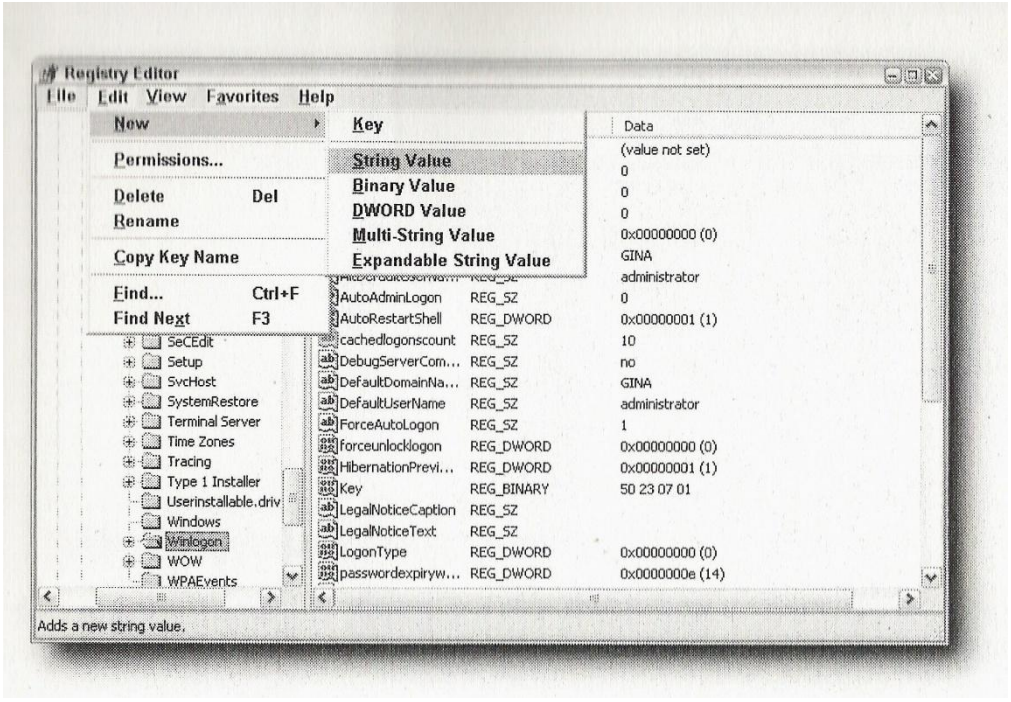


Figura 22

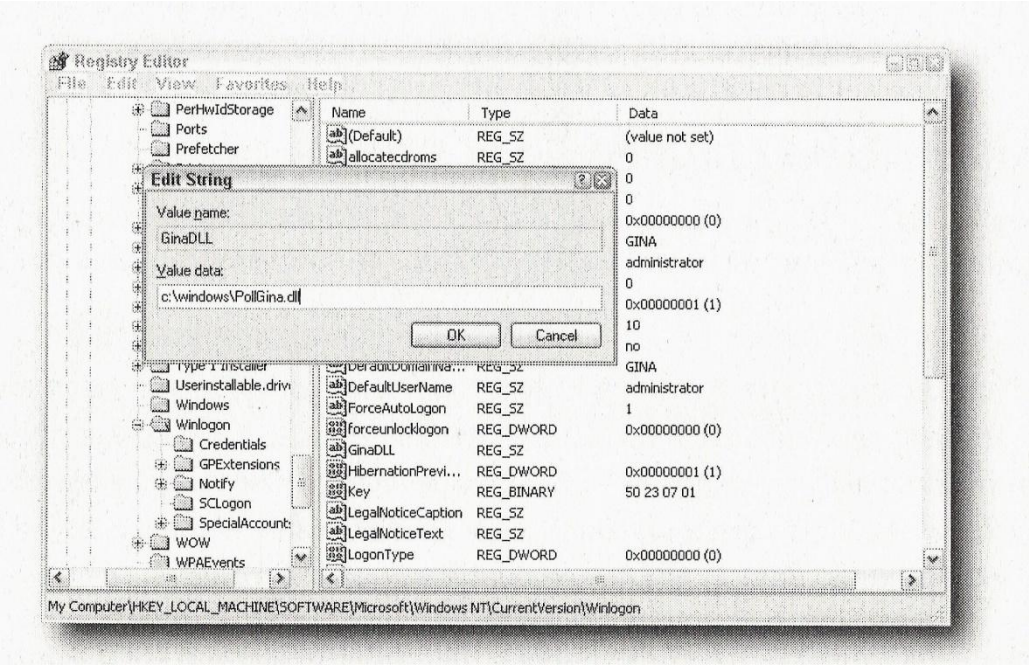


Figura 23

Agora deve-se adicionar algumas chaves de registro para as configurações adicionais do RFIDGina. Navegue para a seguinte secção:

HKEY_LOCAL_MACHINE\SOFTWARE

Adicione uma nova chave chamada PollGina. Então adicione um novo valor string chamado pollLib. Este valor deve ser o caminho correto do arquivo rfidPoll.dll, similar ao que foi feito com o valor de GinaDLL.

Desta vez você vai adicionar um valor do tipo DWORD. O nome desse novo valor será pollTime. Quando você for escolher o valor de polltime, terá a opção de mostrar o valor em hexadecimal ou decimal. Clique em decimal e escolha 500, como mostrado na Figura 24.

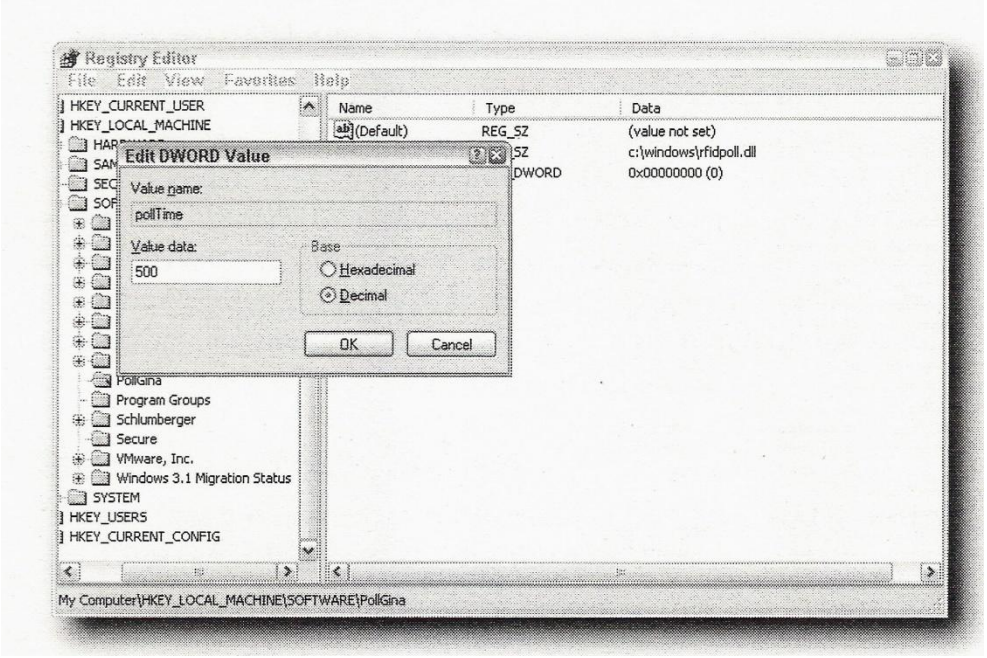


Figura 24

Pronto, feito esses passos o Windows GINA foi substituído pelo sistema RFID. Basta agora reiniciar o computador para que ele entre em operação. Na próxima secção discutiremos sobre como fazer o cadastro de cartões e a associação com as contas de usuário.

5.2.Cadastro de Cartões

O software que faz a associação entre os cartões RFID e as contas de usuário do Windows é o RFIDAuth. O problema comentando na secção anterior em relação à compatibilidade de diferentes versões da biblioteca Phidgets ocorreu com esse programa. Pensou-se que o sistema RFID não estava atuando, quando na verdade era o RFIDAuth que não estava fazendo a associação devida.

Não há processo de instalação para o programa, uma vez que ele foi descompactado e o Phidgets está instalado, basta um simples duplo-clique para executá-lo. Quando você o fizer, a tela mostrada na Figura 25 irá aparecer. Para adicionar uma etiqueta clique no botão Add New Tag, e então uma caixa de diálogo irá aparecer perguntando pelo Tag ID, Username, Password e Domain, assim como é mostrado na Figura 26.

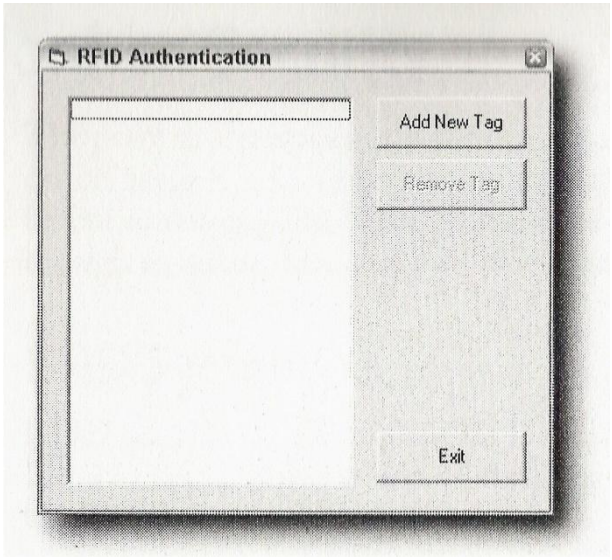


Figura 25

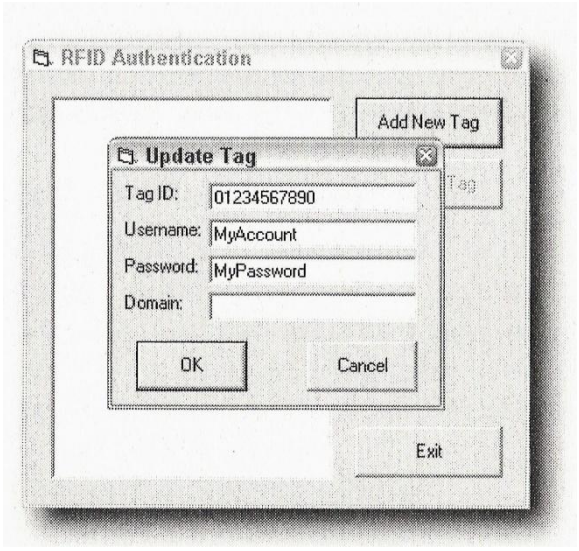


Figura 26

Quando você aproximar a *tag* do leitor nesse momento o campo Tag ID será preenchido. Basta preencher os demais campos e cliquar em OK para fazer a associação da *tag* com a conta. A ID da etiqueta irá aparecer como é mostrado na Figura 27. Você pode editar essa associação a qualquer momento, basta um duplo-clique na ID da etiqueta. A associação também pode ser removida selecionando-a e clicando no botão Remove Tag, a mensagem de confirmação mostrada na Figura 28 irá aparecer.

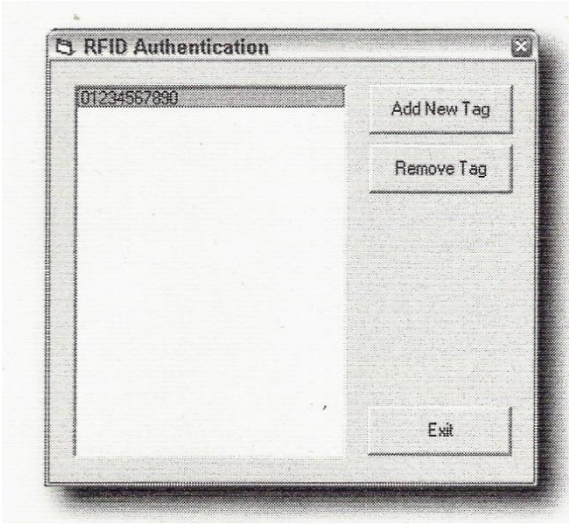


Figura 27

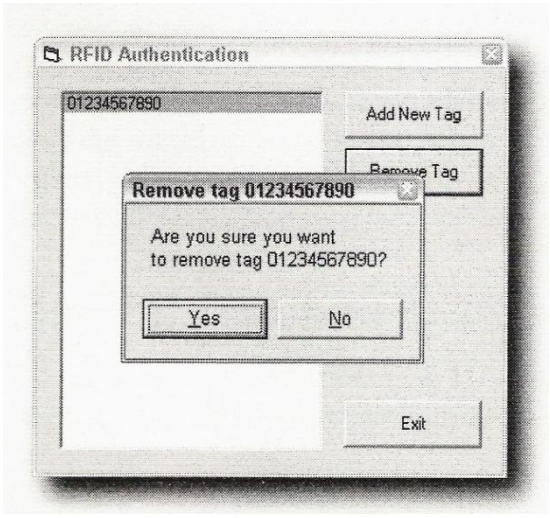


Figura 28

5.3.Avaliação Final

Fazendo as considerações finais sobre o sistema final, do ponto de vista da praticidade notou-se que o sistema é rápido, assim é mais prático simplesmente aproximar o cartão do leitor para fazer o *login* que digitar sua senha. E para pessoas que não gostam de decorar senhas, será uma senha a menos para ser decorada.

Do ponto de vista de segurança você pode pensar que, para sistemas que exijam alta segurança, houve uma perda, pois é bem mais fácil roubar um cartão de alguém que ter que descobrir sua senha. Porém, há etiquetas feitas para serem implantadas em

animais, que algumas pessoas fizeram testes implantando nelas mesmas (Figura 30), o que não tornaria mais tão fácil o roubo da senha de acesso, e de quebra resolveria o problema de perda do cartão, uma vez que ele está implantado. O próprio kit *Phidgets* traz uma dessas etiquetas, que é a que é mostrada na Figura 29.

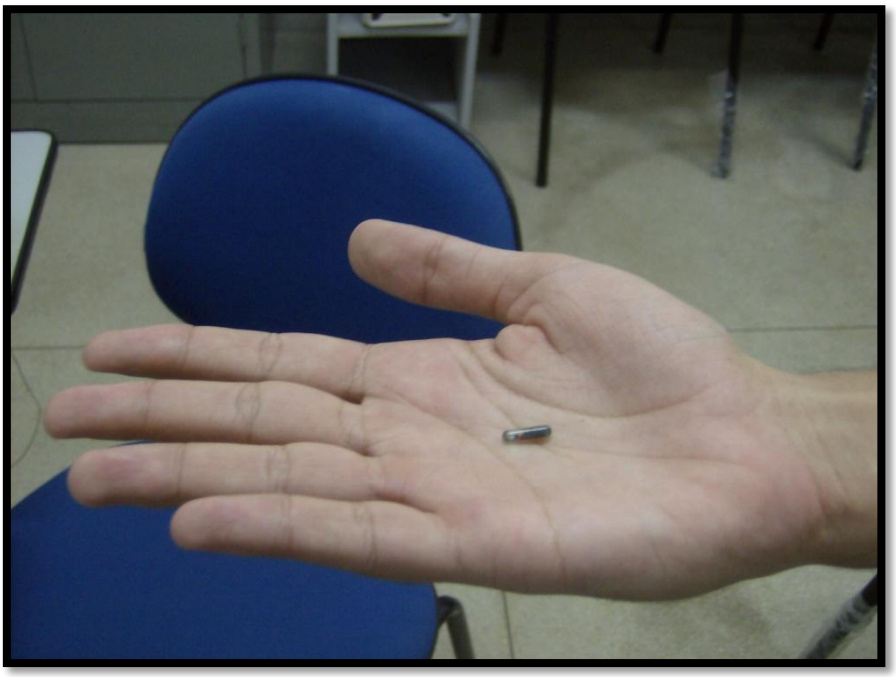


Figura 29: Tag para implante

Figura 30: Tag implantada

Não temos dados do ponto de vista médico sobre a segurança para a saúde deste tipo de implante, mas é de se esperar que implantes do tipo se tornem perfeitamente saudáveis em pouco tempo, se é que já não o são. Vale salientar também que existem biossensores que enviam a informação coletada por RFID. Um exemplo é mostrado em [7], que fala sobre um minúsculo biochip wireless que pode ser injetado em tumores cancerígenos, informando aos médicos, em tempo real, a dose exata de radiação e o alvo preciso para o qual o tratamento deve ser direcionado. Na Figura 31 é mostrado o biochip em questão.

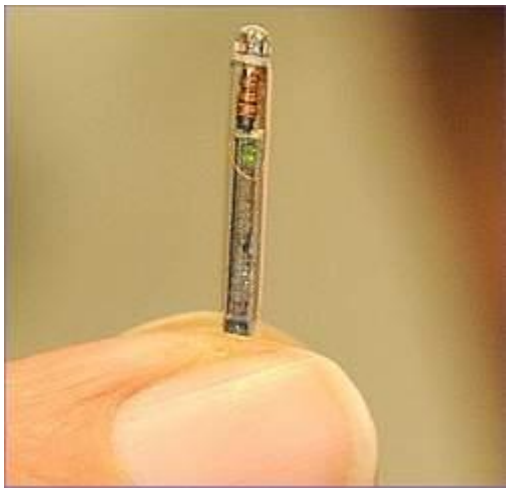


Figura 31: Biochip com RFID acoplado / Fonte: [7]

6. Conclusão

O trabalho proposto inicialmente foi concluído com sucesso. Os conhecimentos adquiridos durante a elaboração do trabalho de conclusão a cerca da tecnologia RFID foram bastante substanciais. E além desta última ampliação de conhecimentos antes do término do curso ficou a satisfação, de minha parte, de ter posto para funcionar um sistema funcional e prático, com valor mais que puramente científico ou acadêmico.

Neste relatório pretendeu-se deixar bem claro os passos que foram seguidos para que o trabalho possa ser repetido e, caso seja de interesse de alguém, que possa ser implementado em outros computadores.

Propostas para realização de trabalhos futuros a partir deste ficam por conta da expansão da quantidade sistemas operacionais, tentando fazer o mesmo sistema de *login* para Linux ou versões mais recentes de SO da Microsoft, Windows Vista e Windows 7. Não foi testado se as bibliotecas e programas mais recentes são compatíveis com os novos SO da Microsoft. Quanto ao Linux, sabe-se que versões mais recentes que a *Kernal 2.6+* são compatíveis com a biblioteca feita para ele. O maior trabalho de pesquisa seria estudar como é feito o sistema de *login* neste SO.

7. Bibliografia

[1] RFID Toys

Amal Graafstra, Editora Wiley, 2006

[2] RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification

Klaus Finkenzeller, Editora Wiley, Segunda Edição, 2003

[3] RFID Security

Frank Thornton, Brad Haines, Anand M. Das, Hersh Bhargava, Anita Campbell, John Kleinschmidt

Editora SynGress, 2008

[4] **Read Only Contactless Identification Device**

Manual da EM Microeletronic

[5] **www.phidgets.com**

Site da empresa Phidgets, fabricante do kit, acessado em: 16/09/2009

[6] **www.rfidtoys.net**

Site oficial do livro RFID Toys, acessado em: 24/08/2009

[7] **www.inovacaotecnologica.com.br**

Reportagem: “Biochip implantável em pacientes vai monitorar tumores e doses de radiação”, Redação do Site Inovação Tecnológica - 11/04/2008

[8] **www.inovacaotecnologica.com.br**

Reportagem: “Etiquetas nano-RFID poderão substituir os códigos de barras”, Redação do Site Inovação Tecnológica - 08/04/2010