

Universidade Federal do Rio de Janeiro

**Instituto Tércio Pacitti de Aplicações e
Pesquisas Computacionais**

Alexandre do Espírito Santo Correa

**REDES RFID E NFC:
Funcionamento e Aplicações**

Rio de Janeiro

2013

Alexandre do Espírito Santo Correa

REDES RFID E NFC

Funcionamento e Aplicações

Monografia apresentada para obtenção do título de Especialista em Gerência de Redes de Computadores no Curso de Pós-Graduação Lato Sensu em Gerência de Redes de Computadores e Tecnologia Internet do Instituto Tércio Pacitti de Aplicações e Pesquisas Computacionais da Universidade Federal do Rio de Janeiro – NCE/UFRJ.

Orientador:

Cláudio Miceli Farias, M.Sc, UFRJ, Brasil

Rio de Janeiro

2013

Alexandre do Espírito Santo Correa

REDES RFID E NFC

Funcionamento e Aplicações

Monografia apresentada para obtenção do título de Especialista em Gerência de Redes de Computadores no Curso de Pós-Graduação Lato Sensu em Gerência de Redes de Computadores e Tecnologia Internet do Instituto Tércio Pacitti de Aplicações e Pesquisas Computacionais da Universidade Federal do Rio de Janeiro – NCE/UFRJ.

Aprovada em março de 2013



Cláudio Miceli Farias, M.Sc, UFRJ, Brasil

RESUMO

CORREA, Alexandre do Espírito Santo. **REDES RFID E NFC: Funcionamento e Aplicações.** Monografia (Especialização em Gerência de Redes e Tecnologia Internet). Núcleo de Computação Eletrônica, Universidade Federal do Rio de Janeiro. Rio de Janeiro, 2013.

A origem dos conceitos base destas tecnologias datam da segunda guerra mundial onde o advento do radar permitiu o desenvolvimento de um método para identificação de aeronaves. A partir daí, com os aperfeiçoamentos ao longo dos anos, inúmeras aplicações foram desenvolvidas para a utilização da identificação por radiofreqüência. Atualmente a tecnologia é amplamente utilizada em várias áreas e a tendência é que esteja cada vez mais próxima das pessoas com o advento dos telefones inteligentes com chips NFC embarcados que poderão substituir os cartões de crédito, identificações e até as chaves que levamos no bolso.

ABSTRACT

CORREA, Alexandre do Espírito Santo. **REDES RFID E NFC: Funcionamento e Aplicações.** Monografia (Especialização em Gerência de Redes e Tecnologia Internet). Núcleo de Computação Eletrônica, Universidade Federal do Rio de Janeiro. Rio de Janeiro, 2013.

The origin of the base concepts from these technologies are dated from World War II where the advent of radar allowed the development of a method for identifying aircrafts. After that, with the improvements over the years, many applications were developed for the use of radiofrequency identification. Actually the technology is widely used in many areas and the tendency is to be closer to the people with the popularization of smartphones with embedded NFC chips that can replace the credit cards, ids and even the keys we carry in pocket.

LISTA DE TABELAS

	Página
Tabela 1 - Frequências RFID	17
Tabela 2 - Partes do padrão ISO 18000	21
Tabela 3 - Comparativo RFID e NFC	26
Tabela 4 - Modos de operação e características descritas na ISO 18092	27
Tabela 5 - Principais sistemas de pedágio automático brasileiros	31

LISTA DE FIGURAS

	Página
Figura 1 - Componentes do sistema	14
Figura 2 - Exemplo de supermercado com RFID	19
Figura 3 - Padrão ISO para RFID	20
Figura 4 - Formatação do número EPC	22
Figura 5 - Composição da memória de um <i>tag EPCGlobal</i>	23
Figura 6 - Busca de informações do EPCIS	24
Figura 7 - Funcionamento do pedágio automático	30
Figura 8 - <i>Tag</i> ativo utilizado pelo sistema Via Fácil	30
Figura 9 - <i>Tag</i> passivo utilizado pelos sistemas Passe Expresso e Onda Livre	31
Figura 10 - Estrutura do cartão <i>Mifare Classic</i> utilizado no transporte público	32
Figura 11 - Contracapa interna do passaporte brasileiro que contém o chip RFID	34
Figura 12 - Funcionamento do SINIAV	35
Figura 13 - Antena SINIAV em teste no Rio de Janeiro	36
Figura 14 - Apresentação Google Wallet, produto NFC do Google.	41

LISTA DE ABREVIATURAS E SIGLAS

ASK	<i>Amplitude-Shift Keying</i>
EPC	<i>Electronic Product Code</i>
EPCIS	<i>Electronic Product Code Information System</i>
IEC	<i>International Electrotechnical Commission</i>
IFF	<i>Identify Friend or Foe</i>
ISM	<i>Industrial, Scientific and Medical</i>
ISO	<i>International Organization for Standardization</i>
JPEG	<i>Joint Photographic Experts Group</i>
NFC	<i>Near Field Communication</i>
NFCIP	<i>Near Field Communication Interface and Protocol</i>
ONS	<i>Object Name Server</i>
PVC	Policloreto de Vinila
RF	<i>Radiofrequencia</i>
RFID	<i>Radio Frequency Identidication</i>
TID	<i>Transponder Identifier</i>

SUMÁRIO

	Página
1	INTRODUÇÃO
2	RFID
2.1	A SEGUNDA GUERRA MUNDIAL
2.2	DO CAMPO DE BATALHA PARA O MERCADO
2.3	FUNCIONAMENTO DA TECNOLOGIA RFID
2.3.1	Meio de Transmissão
2.3.2	Componentes Físicos do Sistema
2.3.2.1	Leitores
2.3.2.2	Antena
2.3.2.3	Controlador
2.3.2.4	Interface
2.3.3	Tag
2.3.4	Middleware
2.4	EXEMPLO DE FUNCIONAMENTO
2.4.1	Padrão ISO/IEC
2.4.1.1	ISO 11784 e ISO 11785
2.4.1.2	ISO 10536, ISO 14443 e ISO 15693
2.4.1.3	ISO 18000
2.4.2	Padrão EPC
2.4.2.1	Funcionamento do EPC
3	NFC
3.1	ORIGEM E DESENVOLVIMENTO
3.2	DIFERENÇAS ENTRE O NFC E O RFID
3.3	FUNCIONAMENTO DA TECNOLOGIA NFC
3.3.1	ISO/IEC 18092
4	APLICAÇÕES
4.1	APLICAÇÕES RFID
4.1.1	Pagamento automático de pedágio e estacionamento
4.1.2	Pagamento de transporte público
4.1.3	Passaporte Biométrico
4.1.4	SINIAV
4.2	NFC
4.2.1	Transmissão de dados entre dispositivos
4.2.2	Pagamentos Móveis
4.2.2.1	Funcionamento
4.2.2.2	Segurança
5	CONCLUSÕES
	REFERÊNCIAS

1 INTRODUÇÃO

O NFC é uma tecnologia inovadora que permite a criação de diversas aplicações para identificação de produtos e pessoas e a criação de novos meios de pagamento, porém ainda é desconhecida por grande parte das pessoas. Trata-se de uma tecnologia para transmissão de dados sem fio, sendo uma evolução da tecnologia RFID que, no Brasil, já é conhecida desde o início dos anos 2000 (Época, 2011) por proporcionar passagem automática em pedágios de rodovias e permitir pagamento automático de estacionamentos através da identificação por sinais de rádio. Sua utilização já vem sendo popularizada com a utilização de bilhetes eletrônicos no transporte público e crachás de controle de acesso nas empresas, o que já dá uma pista de uma das principais diferenças entre o RFID e o NFC: o alcance da comunicação. As novas redes NFC possuem um alcance muito pequeno, por volta de 10 centímetros [NFC Forum, 2012], o que torna a tecnologia ideal para cartões de pagamentos, transferência de contatos, controle de acesso e todo o tipo de aplicação em que os dados devam ser lidos por algum terminal próximo à pessoa que o utiliza.

Este trabalho tem como objetivo mostrar a origem da tecnologia RFID e sua evolução até o NFC, comparando as duas. Aplicações já em uso são apresentadas assim como as tendências para uso futuro da tecnologia.

O trabalho estrutura-se da seguinte forma: o capítulo um apresenta uma breve introdução dos temas abordados nos capítulos seguintes do trabalho, o capítulo dois mostra a origem e a evolução das tecnologias, o capítulo três detalha o funcionamento do RFID, o capítulo quatro é dedicado ao NFC, o capítulo cinco

demonstra aplicações e o capítulo seis apresenta as conclusões e futuro das tecnologias.

2 RFID

Embora tenha muitas aplicações recentes, o desenvolvimento dos conceitos que deram origem à tecnologia RFID data de algumas décadas atrás [RFID Journal, 2012]. Ao longo dos anos, novos usos foram dados à tecnologia de identificação por radiofrequência, que vão desde a simples identificação de produtos, até modernos meios de pagamento que podem vir um dia a substituir os cartões de crédito. Neste capítulo será detalhado o surgimento da tecnologia e sua evolução.

2.1 A SEGUNDA GUERRA MUNDIAL

Durante a Segunda Guerra, as forças em combate utilizavam o radar, inventado anos antes, que alertava sobre a aproximação de aeronaves a grandes distâncias. O instrumento consistia em uma antena que enviava um sinal que era refletido pelas aeronaves ao seu alcance e então recebido de volta, que assim alertava ao operador sua presença. O sistema, entretanto, não poderia identificar se o objeto pertencia a uma força inimiga ou era do próprio país.

Para resolver o problema, os britânicos desenvolveram um sistema que consistia em um transmissor em cada avião que, ao receber o sinal do radar, enviava de volta outro sinal que identificava a aeronave como sendo da própria força. O sistema de identificação por radiofrequência era conhecido como IFF (*identify friend or foe*) e pode ser considerado como a primeira aplicação da tecnologia RFID [RFID Journal, 2012].

2.2 DO CAMPO DE BATALHA PARA O MERCADO

Após o desenvolvimento do sistema IFF, cientistas nos Estados Unidos, Europa e Japão participaram de pesquisas nos anos 60 e 70 e apresentaram documentos explicando como a radiofreqüência poderia ser utilizada para identificar objetos, com isso empresas passaram a comercializar produtos com a tecnologia, permitindo que nas décadas de 70 e 80 já fosse possível ver no mercado aplicações como sistemas antifurto em lojas que utilizavam etiquetas RFID nas mercadorias que disparavam um alarme caso o cliente tentasse deixar a loja sem passar pelo caixa (onde geralmente a etiqueta era retirada após o pagamento) e sistemas de controle de acesso, onde um cartão era lido pela antena na fechadura destravando ou não a porta de acordo com o acesso concedido ao usuário. Outras aplicações que datam da mesma época são a identificação de animais (cada animal com sua etiqueta RFID, sendo possível manter um histórico individual em um sistema com possibilidade de rápida identificação quando necessário), controle de entrada e saída de veículos e rastreamento de substâncias perigosas.

Com o passar dos anos, evoluções da tecnologia como o desenvolvimento de uma etiqueta (*tag*) com memória regravável e a patente de um transmissor utilizado para abrir uma fechadura sem chave surgiram, permitindo novas aplicações que serão descritas ao longo dos capítulos seguintes.

2.3 FUNCIONAMENTO DA TECNOLOGIA RFID

2.3.1 Meio de Transmissão

Como o próprio nome sugere (RFID – Identificação por radiofreqüência, sigla em inglês), o funcionamento da tecnologia é, desde o início, baseado em ondas de

rádio. Desde a época dos radares na segunda guerra, o sinal eletromagnético enviado pelas antenas e refletido na fuselagem dos aviões nada mais é do que um sinal de rádio, da mesma forma que no sistema IFF que hoje funciona enviando um sinal de 1030MHz para descobrir aeronave que responde com um sinal de 1090MHz com a identificação [Federal Aviation Administration, 2011].

2.3.2 Componentes Físicos do Sistema

Um sistema RFID é composto por uma antena responsável por receber o sinal enviado pelos *tags*, que são os circuitos que contêm a identificação do que se quer identificar. As antenas ficam ligadas a dispositivos que rodam algum tipo de *software* responsável pela aplicação utilizada (controle de acesso, inventário, tarifação, etc.). Normalmente uma lista de códigos (números de identificação únicos) que identificam cada *tag* está armazenada em um banco de dados que é consultado pelo *software* responsável pela aplicação.



Figura 1 - Componentes do sistema. Fonte: Abinee Tec Sul

2.3.2.1 Leitores

É o equipamento responsável por enviar o sinal eletromagnético que alimentará os *tags* e receber a resposta dos mesmos, repassando a informação para processamento. No leitor está localizada a antena do sistema (pode estar fisicamente dentro do aparelho ou ligada a ele para gerenciamento remoto), o controlador que gerencia os protocolos de transmissão e recepção do sinal e a interface que faz a ligação com o *middleware* que receberá os dados dos *tags* para processamento.

2.3.2.2 Antena

Antenas são dispositivos que servem para transmitir ondas de rádio através de um meio natural (ar, terra, água, etc.) para comunicação ponto a ponto ou para recepção da energia desta onda de rádio [USPTO 343]. Nos sistemas RFID são responsáveis por transmitir e receber os sinais gerados pelos leitores e *tags*, estando assim presente em ambos. O tipo de antena, tamanho e formato podem variar de acordo com a aplicação e a frequência de operação do sistema.

2.3.2.3 Controlador

O controlador do leitor é responsável por controlar o sistema de leitura, ele identifica as informações recebidas dos *tags* pela antena e decide quais podem gerar um evento que deverá ser transmitido via rede para processamento. O controlador está sempre conectado a uma ou várias antenas, que pode estar localizada em seu próprio corpo ou estar conectada por cabos (uma ou mais)

dependendo da necessidade da aplicação utilizada. Uma saída de rede também está presente e é utilizada para envio das informações para processamento.

2.3.2.4 Interface

A interface de rede é responsável pelo envio dos eventos gerados pelo controlador do leitor para processamento, podendo utilizar tecnologias de transmissão com fio (*serial, ethernet*) ou tecnologias sem fio (*bluetooth, wifi*).

2.3.3 *Tag*

Um *tag* RFID é o dispositivo que armazena a informação que será repassada ao sistema para a identificação do mesmo. Geralmente é um número (por exemplo, o código de barras de um produto ou o número de cadastro de um cliente). O dispositivo consiste em um chip com circuito eletrônico e uma antena e pode ser um pouco maior que um grão de arroz, no formato de um cartão ou até mesmo do tamanho de um maço de cigarros dependendo da aplicação e do local onde ficará instalado [Klaus, 2010].

Os *tags* podem ser de quatro tipos:

- Passivos - são alimentados pelas ondas eletromagnéticas emitidas por um leitor RFID, ativando o chip interno que, ao alcançar certa voltagem, emite de volta a informação nele armazenada;
- Ativos - possuem fonte de alimentação própria, geralmente baterias, o que os torna capaz de enviar um sinal mais forte como resposta, aumentando bastante o alcance do sinal;

- Semi-passivos - possuem uma bateria no próprio circuito que alimenta apenas o chip, fazendo com que responda mais rápido;
- Semi-ativos - possuem uma bateria que alimenta todo o *tag*, porém quando ocorre a comunicação, é utilizada a energia recebida do leitor para a transmissão.

Outra característica que pode variar nos *tags* de acordo com a aplicação é a faixa de frequência de operação do dispositivo. Os sistemas utilizam bandas reservadas (faixas ISM) que não precisam de licenciamento por parte das autoridades responsáveis por gerir o espectro eletromagnético. A frequência de operação do sistema está diretamente relacionada ao custo, velocidade e alcance do dispositivo, conforme mostra a tabela 1.

Tabela 1 - Frequências RFID. (Wyld, 2006)

Frequência	Alcance Aproximado	Velocidade	Custo do Tag	Aplicações - Exemplos
<i>Low Frequency</i> -LF (Frequência Baixa) 125kHz	5cm (passivo)	Baixa	Baixo	Controle de acesso, identificação de animais
<i>High Frequency</i> - HF (Frequência Alta) 13,56MHz	1m (passivo)	Moderada/Baixa	Médio/Baixo	Cartões inteligentes, pagamentos
<i>Ultra High Frequency</i> - UHF (Frequência Ultra Alta) 433MHz	100m (ativo)	Moderada	Alto	Defesa
<i>Ultra High Frequency</i> - UHF (Frequência Ultra Alta) 865-928MHz	7m (passivo)	Moderada/Alta	Baixo	Identificação de mercadorias, rastreamento de bagagens e encomendas
Microondas - 2.45 e 5,8GHz	15m (passivo), 40m (ativo)	Alta	Alto	Rastreamento de conteineres, pagamento automático de pedágio e estacionamento

2.3.4 **Middleware**

O *middleware* é responsável por receber os dados enviados pelos leitores na interface de rede, filtrá-los e formatá-los para entrega nas respectivas aplicações consumidoras dos dados. Pode exercer a função de disseminador de dados quando a informação a ser enviada for utilizada por várias aplicações ou sistemas externos e disponibilizar outras funções de acordo com a necessidade da aplicação. Um middleware pode oferecer suporte a sistemas legados da empresa que o utiliza, assim como ter a capacidade de gerar relatórios e outras informações de apoio ao negócio. Um bom exemplo é o middleware utilizado pelo Walmart nos Estados Unidos, que além de viabilizar o funcionamento dos leitores repassando a informação para os sistemas e ser compatível com os padrões EPCglobal de etiquetagem, é capaz de gerar etiquetas em código de barras, codificar e validar tags, gerenciar e monitorar a rede local, emitir diversos relatórios relativos ao estoque e vendas de mercadorias e oferecer uma interface para operação de todo o sistema [RFID Infotek, 2012] .

2.4 EXEMPLO DE FUNCIONAMENTO

Um exemplo simples para a compreensão do funcionamento do sistema e do papel exercido por cada um dos componentes é a identificação de produtos para pagamento de compras em um supermercado. Por analogia com o sistema de código de barras, pode-se dizer que o código de barras do produto seria a *tag* RFID. Ao passar no caixa, o operador não precisaria apontar o scanner para a leitura da etiqueta, pois ao invés de utilizar um leitor ótico onde o laser precisa atingir a etiqueta, o caixa tem uma antena que alimenta o *tag* do produto que por sua vez responde com um sinal de radiofrequência contendo sua identificação. Após a

resposta ser recebida pela antena, o sinal chega ao controlador que identifica um evento, fazendo com que o mesmo seja enviado via rede ao *middleware* executado em um computador. Através do evento recebido, o *middleware* identifica o código do produto e o envia para a aplicação utilizada pelo supermercado que fará uma consulta ao banco de dados para obter a descrição e preço, gerando assim a informação que será apresentada para o cliente na tela do caixa.

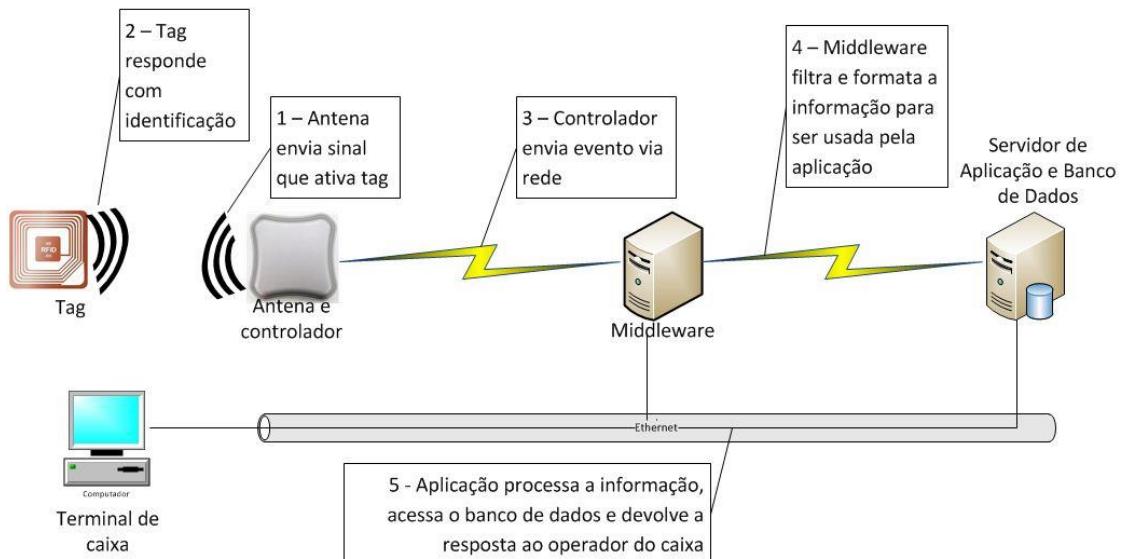


Figura 2 - Exemplo de supermercado com RFID

A comunicação entre o *tag* e o controlador ocorre com o uso de protocolos (ISO/IEC e EPC) que definem as regras de transmissão das informações entre os dois elementos. Inicialmente cada fabricante tinha sua própria arquitetura e tecnologia, o que levou à tentativa de criar uma padronização dos equipamentos.

2.4.1 Padrão ISO/IEC

Um comitê formado pela ISO (*International Standards Organization*) e a IEC (*International Electo-technical Commision*) foi estabelecido para definição de normas para a tecnologia RFID.

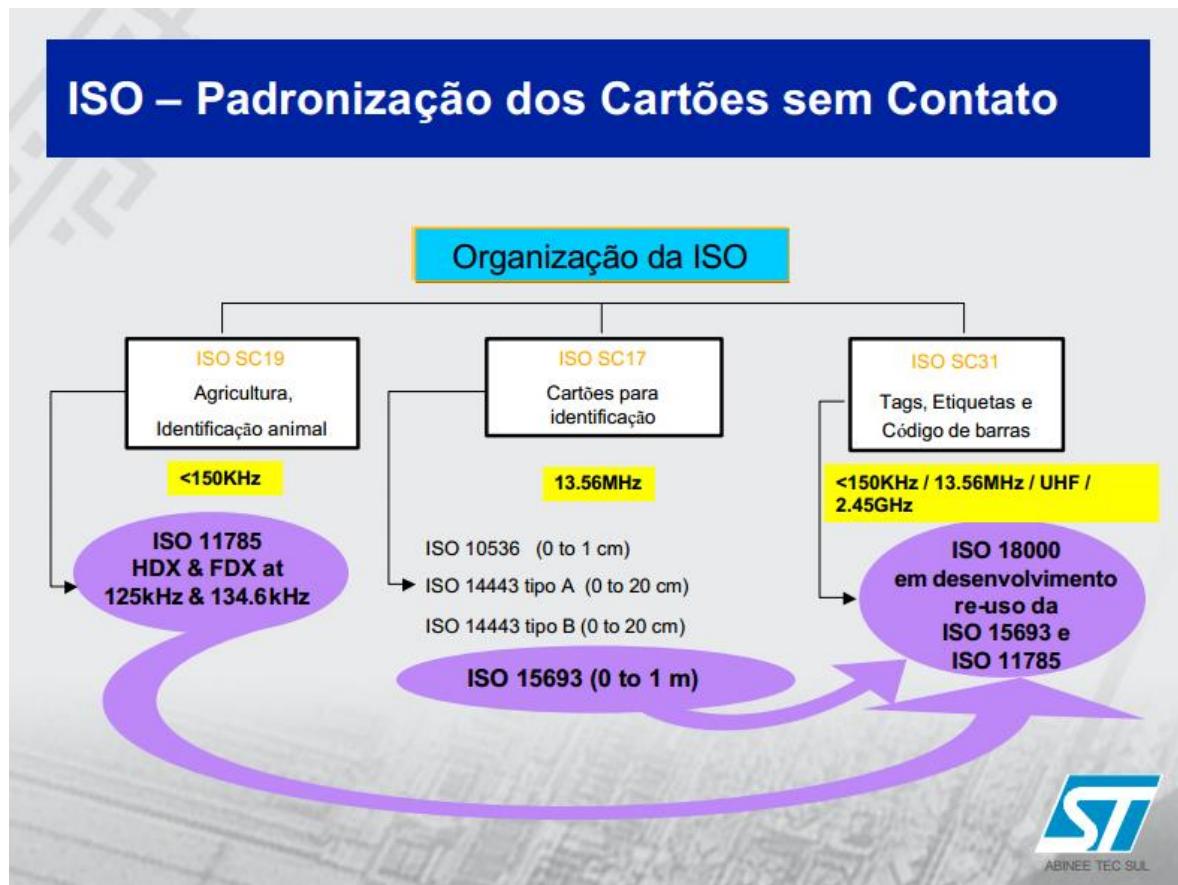


Figura 3 - Padrão ISO para RFID. Fonte: Abinee Tec Sul

2.4.1.1 ISO 11784 e ISO 11785

São dois padrões que definem regras para a utilização de etiquetas RFID em animais. Enquanto a ISO 11784 define a estrutura do código de identificação da tag inserida sob a pele do animal, a ISO 11785 define como é feita a ativação do tag e como a informação nele contida é transmitida para o receptor.

2.4.1.2 ISO 10536, ISO 14443 e ISO 15693

Padrões que definem o funcionamento de cartões de identificação por aproximação. O padrão ISO 10536 define as características dos cartões utilizados, enquanto o ISO 14443 define os protocolos utilizados na transmissão de dados sem fio. O padrão ISO 15693 define os protocolos utilizados em cartões que têm uma distância de leitura maior que os cartões de aproximação (até 1,5m).

2.4.1.3 ISO 18000

O padrão ISO 18000 é dividido em várias partes, definindo padrões para diversas freqüências de comunicação em diferentes aplicações do RFID.

Tabela 2 - Partes do padrão ISO 18000

Parte	Definição
1	Arquitetura genérica
2	Comunicações abaixo de 135 kHz
3	Comunicações em 13,56 MHz
4	Comunicações em 2,45 GHz
5	Comunicações em 5,8GHz
6	Comunicações entre 860 e 960 MHz
7	Comunicações em 433MHz

2.4.2 Padrão EPC

Em 2003 foi criado o grupo EPCglobal formado por representantes de empresas de vários ramos da indústria e varejo com o objetivo de definir a padronização EPC. Neste padrão, um número único (EPC) é utilizado para identificar um produto específico. Este número é armazenado em um *tag* RFID e, após identificado pelo sistema de leitura, é possível obter informações sobre o

produto como origem e data de fabricação. As informações sobre os produtos estão armazenadas em um banco de dados mundial chamado *EPCglobal Network*.

2.4.2.1 Funcionamento do EPC

Cada unidade de um produto possui um número único que está armazenado na *EPCglobal Network* [EPCglobal, 2012]. Este número é composto de 96 *bits* divididos da seguinte forma: 8 bits para o cabeçalho, 3 bits para o filtro que indica o tipo de logística (produto para consumidor final, empacotamento em grupo, etc.), 3 *bits* para determinar o tamanho do campo seguinte e entre 20 e 40 *bits* para identificação do fabricante, números que são alocados pela *EPCGlobal*. Os restantes são divididos em entre 4 e 24 *bits* para identificação do tipo de produto (de acordo com o tamanho do campo anterior) e 38 *bits* correspondentes ao número de série do objeto, no caso valores alocados pelo fabricante do produto.

	Header	Filter Value	Partition	Company Prefix	Item Reference	Serial Number
SGTIN-96	8	3	3	20-40	24-4	38
	0011 0000 (Binary value)			999,999 – 999,999,9 99,999 (Max. decimal range*)	9,999,999 – 9 (Max. decimal range*)	274,877,906 ,943 (Max. decimal value)

*Max. decimal value range of Company Prefix and Item Reference fields vary according to the contents of the Partition field.

Figura 4 - Formatação do número EPC. Fonte: *EPCGlobal/GS1*

O número está armazenado em uma área reservada (EPC) da memória do *tag*, conforme pode ser visto na figura 5. Além desta área, o *tag* possui campos reservados para armazenamento de dados do usuário (opcional, utilizado por alguns fabricantes), de senhas de acesso e destruição (uma senha que quando utilizada inutiliza o *tag*, não respondendo mais a pedidos de leitura) e o campo TID que armazena o número de série (identificador) do *tag*.

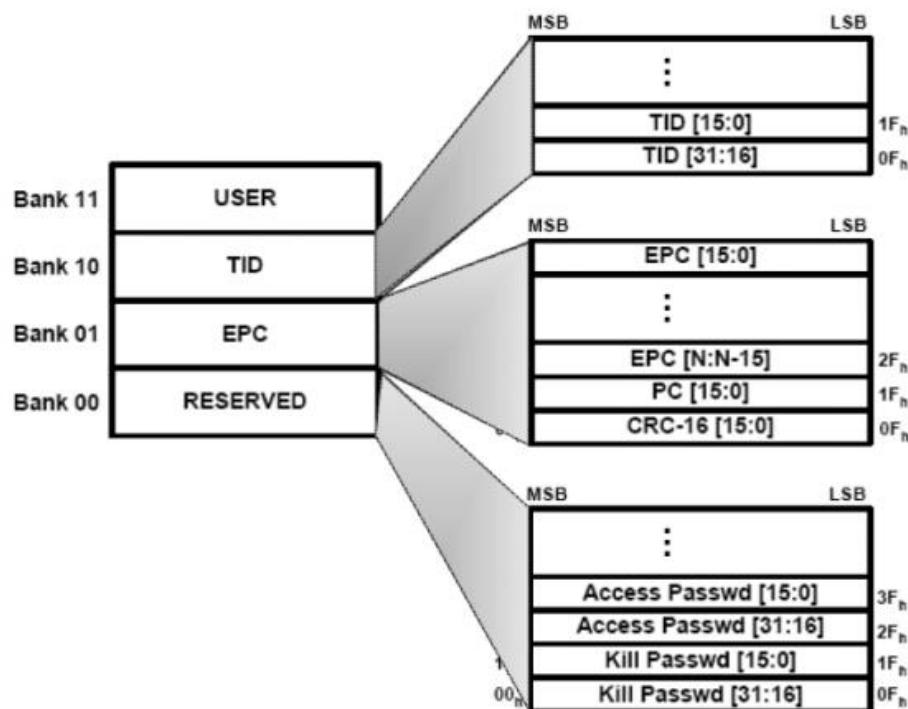


Figura 5 - Composição da memória de um *tag* EPCGlobal. Fonte: *EPCGlobal/GS1*

O padrão EPC define uma norma (EPCIS – *EPC Information Services*) para troca de informações entre os parceiros comerciais de forma a melhorar a eficiência e segurança na cadeia de valor dos produtos, além de um conjunto de serviços destinados a permitir que a informação relativa a um número EPC seja encontrada para que o acesso a ela seja solicitado.

Ao identificar um *tag* EPC, o leitor repassa a informação ao *middleware* que, através da EPCIS acessa um serviço chamado ONS (*Object Name Server*). O serviço ONS recebe como entrada um número EPC e responde com uma URL que aponta ao repositório EPCIS do detentor da informação do objeto lido, sendo possível, assim, obter através da *EPCGlobal* diversas informações sobre o objeto (descrição, data de fabricação, validade, etc.).

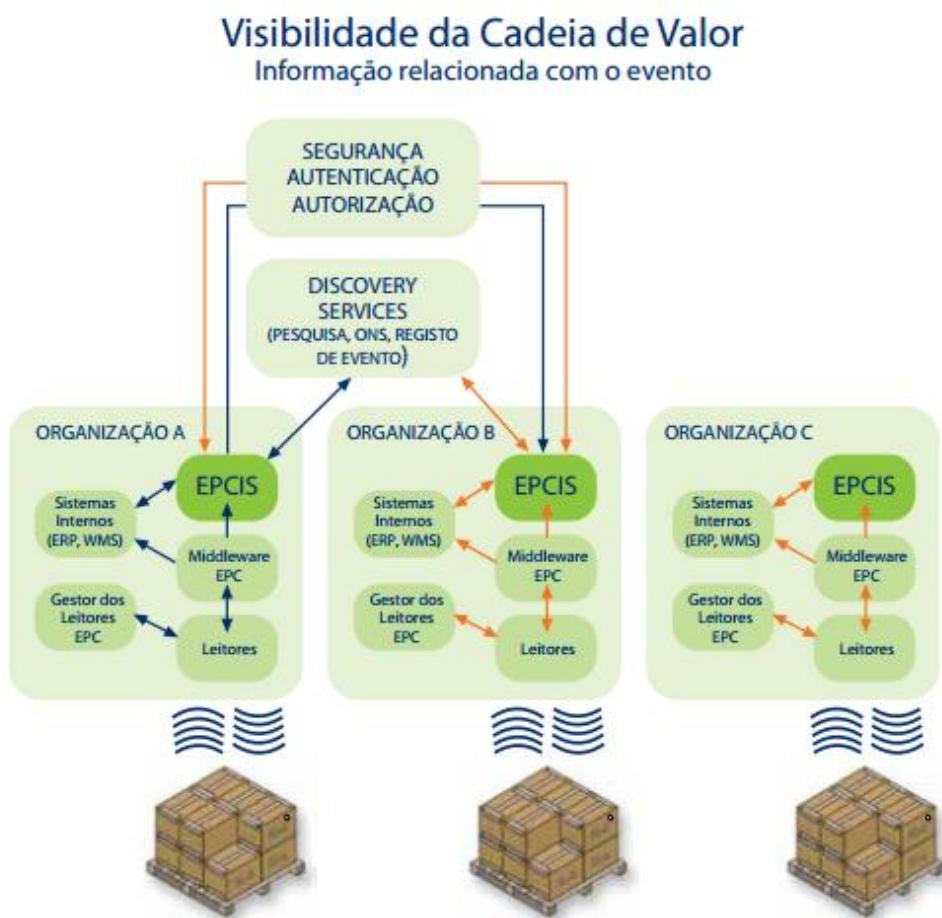


Figura 6 - Busca de informações do EPCIS. Fonte: EPCglobal/GS1

3 NFC

A tecnologia NFC(Near Field Communications) é baseada no RFID [NFC Forum, 2012], as duas utilizam radiofrequência para transmissão de dados, porém a característica principal que difere uma da outra é a mesma que dá a origem ao nome: o alcance. Enquanto o RFID pode variar a distância de comunicação de acordo com a freqüência e tipo de *tag* utilizado, o NFC opera apenas em curtas distâncias (até 10 cm), daí vem a abreviação NFC (*Near Field Communication*, ou seja, comunicação de curta distância).

3.1 ORIGEM E DESENVOLVIMENTO

Em 2004 Nokia, Sony e Philips unem-se em um grupo dedicado a desenvolver um padrão de comunicação de curto alcance fácil de usar e seguro. O grupo era responsável também por popularizar a tecnologia e assegurar que os fabricantes seguissem o padrão de forma a manter a compatibilidade entre diferentes dispositivos.

A primeira aplicação da tecnologia foi em 2006 com a criação de cartazes inteligentes que guardavam informações que poderiam ser lidas por um dispositivo compatível com a tecnologia NFC, trazendo informações, por exemplo, sobre filmes, obras de arte ou espetáculos. Com a evolução da tecnologia, novos dispositivos passaram a incorporá-la e hoje já é possível encontrar diversos modelos de telefones celulares habilitados para NFC.

3.2 DIFERENÇAS ENTRE O NFC E O RFID

Apesar de ser uma extensão da tecnologia RFID e possuir muitas semelhanças no funcionamento, a utilização de dispositivos NFC proporciona uma série de novas aplicações, principalmente na área de controle de acesso e transações financeiras, pois requer que o *tag* esteja praticamente encostado no leitor, o que evita acesso não autorizado aos dados por dispositivos que estejam ao redor.

Tabela 3 - Comparativo RFID e NFC. Fontes: Wyld, 2006 e NFC Forum

RFID		NFC	
Frequência	Alcance Aproximado	Frequência	Alcance Aproximado
<i>Low Frequency</i> -LF (Frequência Baixa) 125kHz	5cm (passivo)		
<i>High Frequency</i> - HF (Frequência Alta) 13,56MHz	1m (passivo)		
<i>Ultra High Frequency</i> - UHF (Frequência Ultra Alta) 433MHz	100m (ativo)	<i>High Frequency</i> - HF (Frequência Alta) 13,56MHz	10cm (ativo e passivo)
<i>Ultra High Frequency</i> - UHF (Frequência Ultra Alta) 865-928MHz	7m (passivo)		
Microondas - 2.45 e 5,8GHz	15m (passivo), 40m (ativo)		

A tabela 3 mostra as frequências e alcance para cada uma das tecnologias. Percebe-se que enquanto os dispositivos RFID podem ter uma variedade de características dependendo da aplicação, os que operam com NFC têm uma única opção com alcance muito curto. Outra característica dos leitores NFC é que os mesmos podem emular um *tag*, ou seja, é possível, por exemplo, fazer com que o

leitor NFC de um celular se comporte como um *tag* que será lido por outro leitor, permitindo assim uma série de novas aplicações.

3.3 FUNCIONAMENTO DA TECNOLOGIA NFC

O funcionamento é baseado no padrão ISO/IEC 18000-parte 3 que já define o funcionamento da tecnologia RFID na frequência de 13,56 MHz. Assim como no RFID o receptor gera um campo magnético que ativa uma tag ou outro dispositivo sem a necessidade de uso de baterias no caso de uma *tag* passiva. A primeira padronização da plataforma se chama NFCIP-1 (*Near Field Communication Interface and Protocol 1*) descrita na norma ISO/IEC 18092. A segunda padronização, implementada nos dispositivos atuais, é a NFCIP-2, descrita na ISO/IEC 21481.

3.3.1 ISO/IEC 18092

Norma que define os modos de comunicação, modulação, codificação, taxas de transmissão, formato dos quadros e controle de colisão de dados.

Tabela 4 - Modos de operação e características descritas na ISO 18092. Fonte: ECMA, 2008

Velocidade	Modo	Modulação	Codificação
424 kbps	Ativo	ASK	Manchester
424 kbps	Passivo	ASK	Manchester
212 kbps	Ativo	ASK	Manchester
212 kbps	Passivo	ASK	Manchester
106 kbps	Ativo	ASK	Miller Modificado
106 kbps	Passivo	ASK	Manchester

No modo passivo, o dispositivo que inicia a comunicação (iniciador) produz um sinal na frequência de 13,56 MHz. O dispositivo que recebe o sinal (alvo) quando

entra no alcance da transmissão pode utilizar o mesmo para obter energia e ser ativado. A comunicação em ambas as direções acontecem segundo o padrão ISO14443 (no Japão existe o padrão FeLiCa que é utilizado em alguns dispositivos naquele país, porém não foi normatizado pela ISO). Este modo permite que o dispositivo RFID possa se comunicar com *tags* RFID ISO18000-3 operando em 13,56 MHz.

No modo ativo os dois lados produzem uma emissão de radiofrequência, cada um transmite informação modificando sua emissão através da modulação ASK. Para evitar colisão apenas o dispositivo que está a transmitir emite o sinal de radiofrequência enquanto o dispositivo que recebe os dados desliga sua emissão.

4 APLICAÇÕES

Atualmente as tecnologias RFID e NFC já são utilizadas em diversas aplicações no dia a dia das pessoas e outras novas estão em fase de desenvolvimento ou teste. A seguir algumas destas aplicações serão apresentadas e terão seu modo de funcionamento detalhado.

4.1 APLICAÇÕES RFID

Por ser a tecnologia que deu origem ao NFC, suas aplicações já estão mais consolidadas e têm algum tempo de mercado. Muitas já são conhecidas do público em geral, com destaque para a utilização em transporte público.

4.1.1 Pagamento automático de pedágio e estacionamento

Sistema utilizado no Brasil desde o início dos anos 2000 para pagamento automatizado de pedágio em rodovias privatizadas. Posteriormente adotado também para o pagamento de estacionamentos, eliminando a necessidade de tickets e possibilitando o débito direto na conta corrente ou cartão de crédito do usuário.

Diversas empresas atuam na prestação do serviço, cada uma com convênios com diferentes rodovias e estacionamentos e com a utilização de diferentes sistemas, porém todos baseados em RFID e funcionando de maneira semelhante.

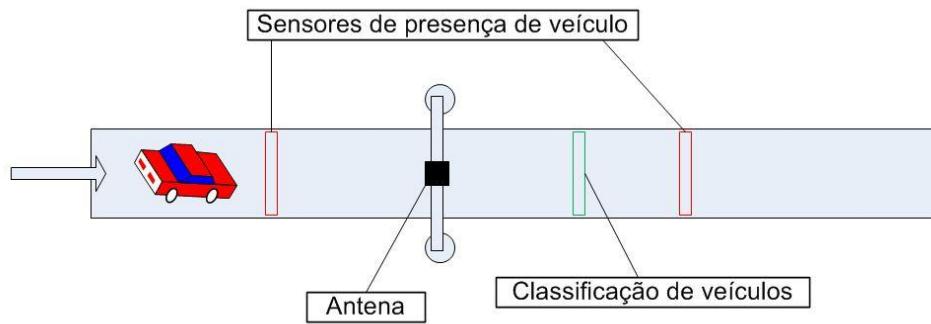


Figura 7 - Funcionamento do pedágio automático

O veículo entra na pista automática, onde é detectado pelo primeiro sensor de presença. Logo após, o carro entra na área de alcance da antena, que envia o sinal para “acordar” o *tag* e recebe a resposta do mesmo. Imediatamente o leitor repassa a informação pela interface de rede para o *middleware* que envia a informação para o servidor e acessa o banco de dados exibindo o sinal verde para o motorista se o cadastro estiver sem problemas ou vermelho caso exista alguma pendência. A seguir o veículo passa em outro sensor que identifica a categoria do veículo (carro, caminhão, número de eixos, etc.), para cobrança do valor de acordo com a tarifa correta e finalmente o segundo sensor de presença que evita que a cancela seja fechada antes da saída do veículo da pista automática.



Figura 8 - *Tag* ativo utilizado pelo sistema Via Fácil



Figura 9 - Tag passivo utilizado pelos sistemas Passe Expresso e Onda Livre

Tabela 5 - Principais sistemas de pedágio automático brasileiros

Sistema/Local	Tipo de tag	Padrão	Frequência
Passe Expresso (RJ)	Passivo	ISO18000-6	928MHz
Onda Livre (RJ)	Passivo	ISO18000-6	928MHz
Via Fácil (vários)	Ativo	ISO18000-5	5,8GHz
Auto Expresso (vários)	Passivo	ISO18000-6B	915MHz

4.1.2 Pagamento de transporte público

Há alguns anos os passes de metrô e vale-transporte foram substituídos por cartões com leitura por aproximação. Na verdade o sistema é mais uma aplicação da tecnologia RFID utilizando *tags* passivos em formato de cartão que podem ser lidos sem que seja necessário retirá-los da carteira ou bolsa.

No transporte público do Rio de Janeiro são utilizados cartões do tipo Mifare (marca registrada da Philips, atual NXP) que operam na freqüência de 13,56 MHz e seguem a norma ISO/IEC 14443. O cartão é feito de PVC com uma antena formada por um fio que o percorre quatro vezes próximo às bordas e um chip instalado dentro de sua estrutura que funciona como um dispositivo de armazenamento, onde a memória é dividida em blocos e setores. Suporta o armazenamento de até 1024

bytes, divididos em 16 setores, cada um deles protegido por duas chaves (A e B) de 6 bytes cada que podem ser programadas para permitir operações específicas (leitura, gravação).

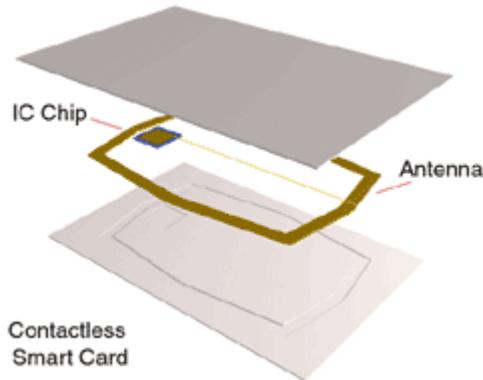


Figura 10 - Estrutura do cartão *Mifare Classic* utilizado no transporte público

Ao aproximar o cartão, o leitor define um setor para acesso e escolhe a chave A ou B. O cartão então lê a chave secreta e as condições de acesso para o setor (armazenadas sempre no último bloco do setor), enviando em seguida um número randômico como desafio para o leitor. O leitor calcula a resposta utilizando a chave secreta e o número enviado pelo cartão. A resposta, junto com um desafio randômico do leitor é enviada para o cartão, que a verifica comparando com o seu próprio desafio e calcula a resposta para o desafio do leitor, efetuando sua transmissão em seguida. O leitor verifica a resposta do cartão comparando-a com seu próprio desafio. Todo esse procedimento é chamado de autenticação em três passos. Após completado, toda a comunicação entre o cartão e o leitor é criptografada e as informações de saldo podem ser lidas e gravadas na memória do cartão.

4.1.3 Passaporte Biométrico

O passaporte biométrico foi introduzido em 2004 com o objetivo de aumentar a segurança na identificação de pessoas na imigração. Além dos dados impressos contidos nos passaportes comuns, ele dispõe de um a memória onde são armazenados os dados já disponíveis na versão em papel, assim como dados digitais para identificação por biometria.

O documento consiste de um livro, semelhante aos passaportes comuns, porém com um *tag* RFID na contracapa obedecendo a norma ISO 14443 além de obedecer a normas específicas para documentos de viagens documentadas na ICAO9303 de forma a garantir a interoperabilidade dos documentos e leitores disponíveis em todos os países.

Os passaportes equipados com o chip RFID são identificados com um símbolo na capa e instruções de manuseio na contracapa interna de forma a orientar o portador a evitar danos no dispositivo.

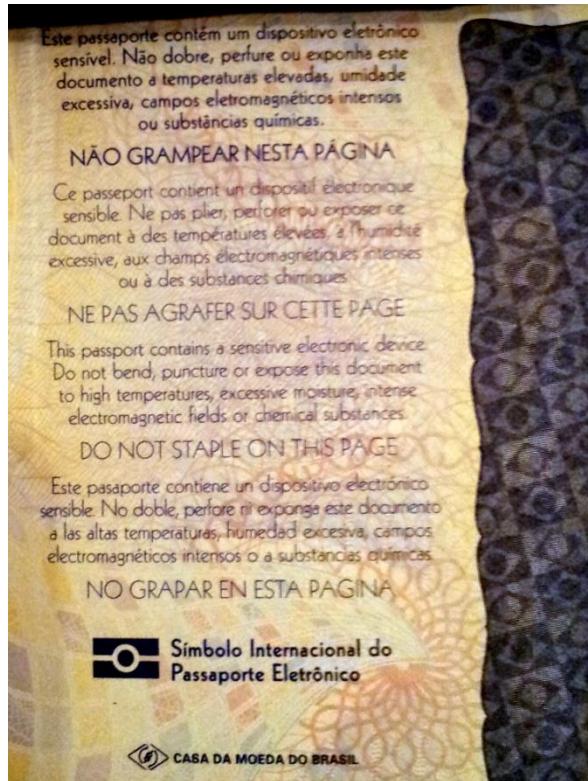


Figura 11 - Contracapa interna do passaporte brasileiro que contém o chip RFID

O chip contido no *tag* possui uma memória de 32KB, onde, além dos dados do passaporte em papel, pode ser armazenada a informação biométrica do portador (foto, impressão digital, identificação da íris, etc.) em formato de imagem (JPEG). Quando passando pela imigração o funcionário precisa digitar algumas informações impressas no passaporte (usualmente data de nascimento do portador, validade e número do passaporte) antes de efetuar a leitura. Essas informações funcionam como uma chave para a informação criptografada do documento de forma a evitar que a informação transmitida seja lida por equipamentos não autorizados. Além da criptografia, alguns países implementam uma capa com uma blindagem que evita que o sinal seja irradiado para fora do documento quando o mesmo está fechado, de forma a evitar ataques para acesso aos dados enquanto o documento é transportado pelo portador na rua, por exemplo.

4.1.4 SINIAV

O Sistema Nacional de Identificação Automática de Veículos (SINIAV) prevê que até 2014 (o prazo já foi adiado algumas vezes) os veículos em circulação no território nacional recebam um *tag* de identificação. O sistema consiste de uma placa de licenciamento eletrônica instalada no veículo, que nada mais é do que a placa no carro com o tag RFID instalado. A partir daí, será criada uma estrutura de leitores com antenas espalhadas pelas cidades e rodovias que farão a leitura e identificação automática dos veículos em circulação.

O sistema funciona de forma semelhante ao utilizado para o pagamento de pedágios e estacionamentos, porém os leitores estarão espalhados por vários pontos das cidades de forma a monitorar constantemente o trânsito de veículos. Após um período de testes foi definida a utilização de um tag passivo operando na frequência de 915MHz que deve ter sua produção comercial iniciada em 2013.

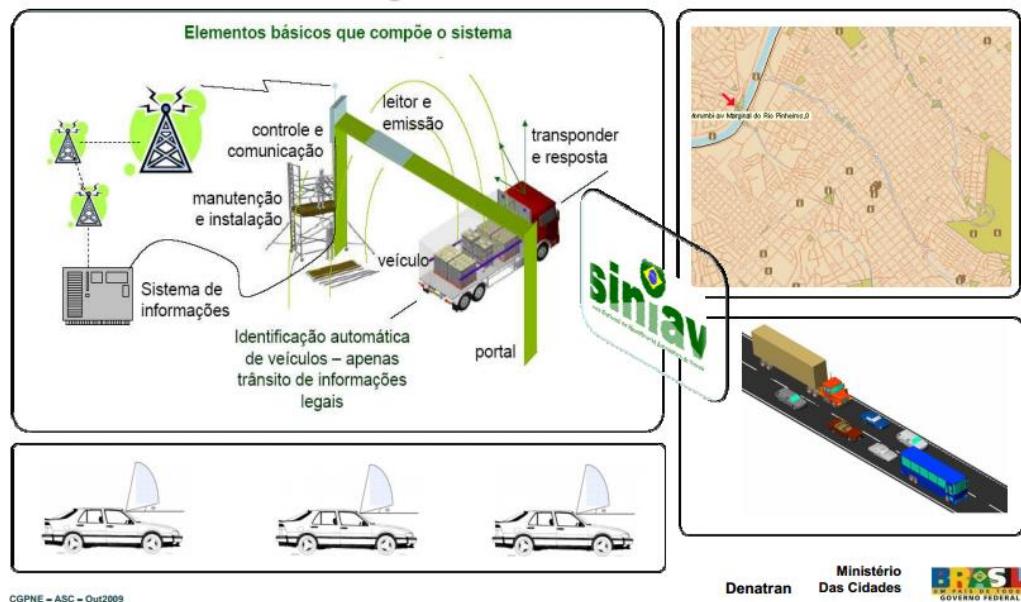


Figura 12 - Funcionamento do SINIAV. Fonte: Denatran

Ao cruzar um leitor, será possível saber a localização do veículo, verificar a situação do licenciamento do mesmo, assim como fiscalizar possíveis infrações cometidas. O sistema promete ser um aliado das autoridades no combate ao roubo de carros, pois será possível acompanhar o deslocamento de um veículo nessa condição, além de permitir que as autoridades sejam acionadas para interceptação de um veículo que circule sem o pagamento das taxas ou com multas pendentes. Com a participação de toda a frota no sistema, será possível a implementação de esquemas de trânsito para amenizar os congestionamentos, uma vez que será possível saber em tempo real o comportamento do fluxo de veículos nas ruas.

Críticos do sistema argumentam que tais informações de localização e movimentação dos veículos sendo transmitidas às autoridades pode configurar uma invasão da privacidade dos motoristas, além do argumento de que o sistema deve ter uma política de segurança de forma a evitar que tais informações caiam na mão de pessoas não autorizadas ou mal intencionadas.



Figura 13 - Antena SINIAV em teste no Rio de Janeiro. Fonte: Seagull Tecnologia

4.2 NFC

Com a popularização dos celulares, principalmente *smartphones*, a cada dia surgem novas aplicações para os aparelhos. Começam a aparecer no mercado celulares que possuem chips NFC embarcados e, com isso, aplicações são desenvolvidas para uso principalmente com esses aparelhos.

4.2.1 Transmissão de dados entre dispositivos

A implementação de chips NFC nos celulares proporcionou uma forma rápida de compartilhamento de conteúdo entre dispositivos. Com a utilização de dois aparelhos habilitados para a tecnologia, é possível a troca de dados apenas com aproximação. O usuário que deseja compartilhar o conteúdo seleciona a função de envio via NFC e aproxima o celular do dispositivo receptor. O receptor detecta a presença do emissor e inicia uma comunicação via NFC, por onde são enviados dados necessários (nome da rede, chave, etc.) para o estabelecimento automático de uma comunicação *wifi* mais rápida para envio do conteúdo propriamente dito. Para o usuário isso fica transparente, como se tudo fosse feito via NFC, mas na verdade ele é utilizado apenas para troca de parâmetros de forma a estabelecer uma conexão mais rápida por outro meio para o envio da informação, evitando que toda a configuração tenha que ser feita manualmente pelas duas partes.

4.2.2 Pagamentos Móveis

Vários testes vêm sendo conduzidos para utilização desses aparelhos como meio de pagamento devido à segurança proporcionada pela tecnologia e a

praticidade de reunir vários cartões que andam nas carteiras em apenas um dispositivo que hoje em dia quase todas as pessoas carregam consigo.

4.2.2.1 Funcionamento

Para utilização de pagamentos móveis pelo celular com a tecnologia NFC, o usuário primeiramente deve ser cadastrado em um serviço de pagamentos móveis, onde estarão armazenadas suas informações bancárias (cartões de crédito, contas, etc.). Ao efetuar o pagamento em um estabelecimento, o princípio de funcionamento é o mesmo dos demais dispositivos RFID, o usuário aproxima o celular do leitor, que receberá a informação transmitida pelo chip NFC armazenada no telefone e irá acessar o banco de dados da empresa que provê o serviço de pagamento móvel para o usuário. A partir daí o sistema da empresa debita o cartão já cadastrado na conta do usuário e o mesmo recebe a fatura normalmente como se tivesse feito a compra utilizando o cartão tradicional. A qualquer momento o usuário pode alterar os cartões cadastrados para débito das compras, assim como pode bloquear o dispositivo para evitar compras em caso de perda.

4.2.2.2 Segurança

Uma grande preocupação na utilização de cartões de crédito, principalmente em compras online é o roubo do número e clonagem. A utilização de pagamentos por NFC permite que as transações sejam efetuadas sem a utilização do número de qualquer cartão. Os dados bancários ficam guardados exclusivamente na empresa responsável pelo processamento dos pagamentos, não sendo necessário o armazenamento de nenhuma informação bancária no celular. Além de não conter

nenhum dado bancário, a informação transmitida só pode ser lida por dispositivos muito próximos (menos de 10 cm) e é criptografada, ou seja, mesmo que outro leitor esteja ao alcance da transmissão, a mesma não poderá ser decodificada.

No caso de perda do dispositivo, o usuário necessita apenas bloquear o mesmo com o fornecedor do serviço e cadastrar um novo, sem preocupação com violação do cartão, uma vez que os dados não estão no aparelho e a utilização da aplicação que efetua os pagamentos móveis é mediante impostação de senha.

5 CONCLUSÕES

Embora presente em várias aplicações há bastante tempo, as tecnologias baseadas em identificação por radiofrequência agora começam a ocupar cada vez mais as publicações e noticiários em geral, deixando de figurar apenas nas páginas de veículos especializados em tecnologia.

Até pouco tempo atrás ficava transparente para as pessoas em geral a utilização da tecnologia. Quando um serviço era contratado (pedágio automático, passe para transporte público, etc.), o usuário recebia o dispositivo que era utilizado para o fim específico, nunca se pensava na relação que poderia existir entre um cartão do metrô e o aparelho colado no vidro do carro para abertura da cancela do pedágio. Agora isto começa a mudar graças a popularização dos telefones inteligentes com suporte ao NFC, que permitirão que vários dispositivos utilizados pelas pessoas sejam substituídos pelos seus telefones.

Diferente do que acontecia quando o usuário contratava e a empresa responsável fornecia o dispositivo, agora o usuário já terá equipamento necessário, bastando a contratação do serviço. Isto é o suficiente para que as empresas que exploram serviços baseados em NFC comecem suas campanhas de *marketing* e divulgação da tecnologia fora dos veículos direcionados a profissionais de tecnologia, de forma que o público em geral tenha conhecimento do funcionamento e das possibilidades, criando assim interesse pela aquisição de produtos compatíveis com o consequente aumento do número de clientes em potencial.

Com a venda de 200 milhões de dispositivos equipados com NFC em 2012 e a expectativa de que mais 300 milhões sejam vendidos em 2013 [Teletime, 2013],

em breve será realidade a substituição de cartões de crédito, passes para transporte público, crachá de acesso às empresas e até a chave do carro por um celular inteligente que armazenará todas as credenciais necessárias pelo usuário.

Pode-se esperar nos próximos anos uma divulgação cada vez maior da tecnologia NFC por parte de empresas que farão parte do ecossistema das aplicações, principalmente fabricantes e operadoras de celular, bancos, bandeiras e credenciadoras de cartões de crédito e empresas de transporte público. Todos já conduzem testes em campo com a tecnologia e já existem inclusive operações comerciais em início de funcionamento no Brasil (*Visa PayWave, Mastercard PayPass, PagSeguro NFC* entre outros).

A tecnologia tem potencial de mudar radicalmente o conteúdo dos bolsos das pessoas, permitindo que boa parte das coisas que hoje temos que levar para todos os lugares sejam substituídas pelo telefone celular e fazendo com que carteiras cheias de cartões passem a ser apenas uma lembrança.



Figura 14 - Apresentação Google Wallet, produto NFC do Google.

REFERÊNCIAS

- [1] ANDRION, R. **Mobile Time**, 2012. Disponível em: <<http://www.mobiletme.com.br/23/10/2012/gsm-association-aposta-no-desenvolvimento-da-tecnologia-nfc-para-alem-dos-pagamentos-moveis/307439/news.aspx>>. Acesso em: 30 out. 2012.
- [2] C.WYLD, D. RFID 101: The Next Big Thing For Management. **Management ResearchNews**, Louisiana, v. 29, n. 4, p. 154-173, 2006.
- [3] CEITEC SA. Produtos RFID, 2013. Disponível em: <<http://www.ceitec-sa.com/pt/rfid>>. Acesso em: 22 fev. 2013.
- [4] CLEMENTE, I. Via Rápida para o Lucro. **Revista Época**, 2011. Disponível em: <<http://revistaepoca.globo.com/Revista/Epoca/0,EMI243878-15223,00-VIA+RAPIDA+PARA+O+LUCRO.html>>. Acesso em: 30 out. 2012.
- [5] COMPUTERWORLD. Carros brasileiros serão identificados por RFID apartir de janeiro, 2012. Disponível em: <<http://computerworld.uol.com.br/2012/10/03/carros-brasileiros-serao-identificados-por-rfid-a-partir-de-janeiro/>>. Acesso em: 22 fev. 2013.
- [6] DENATRAN. **Seminário SINIAV Denatran**. Denatran/Ministério das Cidades. Brasília, p. Disponível em:http://www.denatran.gov.br/download/APRESENTACAO_SEMINARIO_SINIAV.pdf. 2009.
- [7] DUARTE, O. C. M. B. RFID - Radio Frequency Identification. **Grupo de Teleinformática e Automação - UFRJ**, 2010. Disponível em: <http://www.gta.ufrj.br/grad/10_1/rfid/index.html>. Acesso em: 29 out. 2012.
- [8] ECMA INTERNATIONAL. **Near Field Communication - Interface and Protocol (NFCIP-1)**. Geneva. 2008.
- [9] ECMA INTERNATIONAL. **Near Field Communication Interface and Protocol 2 (NFCIP-2)**. Geneva. 2010.
- [10] EPCGLOBAL. ElectronicProductCode (EPC): An Overview. **EPCglobal**. Disponível em: <www.gs1.org/docs/epcglobal/an_overview_of_EPC.pdf>. Acesso em: 29 out. 2012.
- [11] FEDERAL AVIATION ADMINISTRATION. **Future Supportability of 1030/1090 MHz Systems & Operations in the NAS**. [S.I.]: Spectrum Engineering Services, 2011.
- [12] FILHO, O. L. D. S. F. **Comunicação NFC (Near Field Communication) entre Dispositivos Ativos**. Recife: Universidade Federal de Pernambuco, 2010.
- [13] FINKENZELLER, K. **RFID Handbook**. [S.I.]: Wiley, 2010.

- [14] HECKEL, A. P. **Identificação Por Radiofrequência(RFID): Estudo Teórico e Experimentação via Simulação.** Novo Hamburgo: C Universitário Feevale, 2007.
- [15] MOBILE TIME. **Mobiletime**, 2013. Disponível em: <<http://www.mobiletime.com.br/30/01/2013/vivo-e-tim-lancam-projetos-com-nfc-em-parcerias-com-bancos/323371/news.aspx>>. Acesso em: 31 jan. 2013.
- [16] NATIONAL INSTRUMENTS. O Status da Identificação Por Radiofrequência (RFID). **National Instruments**, 2011. Disponível em: <<http://www.ni.com/white-paper/4299/pt>>. Acesso em: 29 out. 2012.
- [17] NFC FORUM. FAQ, 2012. Disponível em: <<http://www.nfc-forum.org/resources/faqs>>. Acesso em: 29 out. 2012.
- [18] PAIVA, F. **Mobile Time**, 2012. Disponível em: <<http://www.mobiletime.com.br/05/10/2012/onibus-no-rio-de-janeiro-farao-teste-com-nfc/304359/news.aspx>>. Acesso em: 12 out. 2012.
- [19] PAIVA, F. NFC é estrela este ano em Barcelona. **Mobile Time**, 2013. Disponível em: <<http://www.mobiletime.com.br/24/02/2013/nfc-e-estrela-este-ano-em-barcelona/326697/news.aspx>>. Acesso em: 2013 fev. 24.
- [20] RFID INFOTEK. RFID Tag Manager for Wal-Mart & DoD, 2012. Disponível em: <<http://www.rfidinfotek.com/detail/walmart-dod-tag-manager-system/417.html>>. Acesso em: 02 mar. 2013.
- [21] ROBERTI, M. The History of RFID Technology. **RFID Journal**, 2002. Disponível em: <<http://www.rfidjournal.com/article/view/1338>>. Acesso em: 29 out. 2012.
- [22] SEAGULL TECNOLOGIA. Sobre o SINIAV, 2012. Disponível em: <<http://www.seagull.com.br/siniac.php?id=1>>. Acesso em: 22 fev. 2013.
- [23] SOUZA, J. A. D. **RFID - Identificação por Radiofrequência: Estudo de Caso da Chiptiming.** Praia Grande: CEET Paula Souza, 2009.
- [24] TI INSIDE. **TI Inside**, 2012. Disponível em: <<http://www.tiinside.com.br/19/11/2012/sino-brasileiro-implanta-rfid-para-inventario-de-equipamentos/ti/311882/news.aspx>>. Acesso em: 15 jan. 2013.
- [25] TI INSIDE. **TI Inside**, 2013. Disponível em: <<http://www.tiinside.com.br/19/11/2012/sino-brasileiro-implanta-rfid-para-inventario-de-equipamentos/ti/311882/news.aspx>>. Acesso em: 04 fev. 2013.
- [26] UNITED STATES PATENT AND TRADEMARK OFFICE. Class 343. Disponível em: <<http://www.uspto.gov/web/patents/classification/uspc343/defs343.htm>>. Acesso em: 08 fev. 2013.
- [27] WEISS, S. A. **RFID (Radio Frequency Identification): Principles and Applications.** [S.I.]. 2007.