Centro Universitário de Brasília
Instituto CEUB de Pesquisa e Desenvolvimento - ICPD

KELLY CRISTINA DE OLIVEIRA CRUZ

ESTUDO SOBRE O NEAR FIELD COMMUNICATION E SEU PAPEL EM PAGAMENTOS VIA DISPOSITIVOS MÓVEIS

Brasília
2013

KELLY CRISTINA DE OLIVEIRA CRUZ

ESTUDO SOBRE O NEAR FIELD COMMUNICATION E SEU PAPEL EM PAGAMENTOS VIA DISPOSITIVOS MÓVEIS

Trabalho apresentado ao Centro Universitário de Brasília (UniCEUB/ICPD) como pré-requisito para obtenção de Certificado de Conclusão de Curso de Pós-graduação *Lato Sensu* na área de Rede de Computadores, com ênfase em Segurança.

Orientador: Msc. Rafael Sarres

Brasília
2013

KELLY CRISTINA DE OLIVEIRA CRUZ

ESTUDO SOBRE O NEAR FIELD COMMUNICATION E SEU PAPEL EM PAGAMENTOS VIA DISPOSITIVOS MÓVEIS

Trabalho apresentado ao Centro Universitário de Brasília (UniCEUB/ICPD) como pré-requisito para a obtenção de Certificado de Conclusão de Curso de Pós-graduação *Lato Sensu* na área de Rede de Computadores, com ênfase em Segurança.

Orientador: Msc. Rafael Sarres

Brasília, 27 de novembro de 2013.

Banca Examinadora

_____

Prof. Ms. Luciano Henrique Duque

_____

Prof. Dra. Tânia Cristina da Silva Cruz

Gostaria de dedicar este trabalho ao meu marido.
Sempre companheiro, amigo, e eterno namorado.

AGRADECIMENTO(S)

Gostaria de agradecer àqueles que me deram força e incentivo durante toda a minha caminhada até aqui. Mas, primeiramente, a minha querida mãezinha, mulher batalhadora e de fé. Pois se cheguei onde estou, foi por causa dela.

“Ser homem é ser responsável. É sentir que colabora na construção do mundo.”

“Tu te tornas eternamente responsável por aquilo que cativas”

Antoine de Saint-Exupéry

RESUMO

Esse trabalho apresenta um estudo sobre o que é o NFC e como ele funciona, analisando seus protocolos, sua segurança, suas aplicações no mundo real, auxiliando aqueles que desejam desenvolver novas soluções com esta tecnologia ainda pouco conhecida. A pesquisa baseou-se no levantamento dos protocolos relacionados ao NFC, buscando conceitos técnicos herdados principalmente do RFID e do *smart card*, bem como na análise sobre sua segurança, confrontando opiniões de alguns pesquisadores e pesquisando soluções disponíveis. Também foi analisado o NFC inserido no contexto do *mobile payment*, pesquisando sua arquitetura e protocolos de comunicação do sistema mobile NFC, isto é, sistema onde o celular NFC é usado no *mobile payment*. Uma ferramenta de emulação da infraestrutura NFC real (dispositivos celulares, *tags*, leitoras, etc.) foi apresentada, com o objetivo de auxiliar aqueles que desejam desenvolver novas aplicações NFC. Por fim, o NFC se apresenta como uma tecnologia promissora e de grande potencial inexplorado, mas ainda é ignorado pela grande maioria da população no Brasil.

Palavras-chave: NFC. radiofrequência. *m-payment. contactless.* OpenNFC.

ABSTRACT

This paper presents a study on what is NFC and how it works, analyzing their protocols, their security, their real-world applications, helping those who wish to develop new solutions with this technology that is still little known. The research was based on a survey of protocols related to NFC, seeking technical concepts inherited mainly from the smart card and RFID, as well as analysis of their security, confronting opinions of some researchers and researching available solutions. Also analyzed the NFC inserted in the context of mobile payment, researching its architecture and communication protocols NFC mobile system, in other words, system where the mobile NFC is used in mobile payment. An emulation tool of real NFC infrastructure (mobile devices, tags, readers, etc…) was presented, in order to assist those who wish to develop new NFC applications. Finally, the NFC is presented as a promising technology and large untapped potential, but it is still ignored by the vast majority of people in Brazil.

Key words: NFC; radiofrequency; m-payment; contactless; OpenNFC;;

LISTA DE FIGURAS

LISTA DE TABELAS

SUMÁRIO

INTRODUÇÃO

Novos recursos tecnológicos, que buscam tornar mais simples e prática tarefas e experiências de nossa vida cotidiana, têm sido um dos focos principais de pesquisadores e indústrias. Os *smartphones*, *smart tv*'s e *tablets*, são exemplos desta revolução e vem fazendo parte do dia-a-dia das pessoas em geral de forma crescente. Soluções que tornam transparente aos usuários como as tecnologias operam, e que necessitam a mínima interação do usuário, com simples ações como: um toque, um gesto, um comando de voz, ou aproximação, mudando paradigmas no campo da interação homem x máquina a qual até há pouco tempo era feita através de um teclado ou mouse.

O NFC – *Near Field Communication* é um padrão de comunicação *contactless* (sem contato) entre dois dispositivos, operando com um raio limitado de, em média, 10 cm de distância entre eles. Baseado no protocolo RFID – *Radio-Frequency Identification* (identificação por radiofrequência) e especificado pela padronização ISO/IEC 18092 (CURRAN; MILLAR; MC GARVEY, 2012), este novo conceito conta com uma infinidade de aplicações, visando trazer agilidade em vários contextos do nosso cotidiano: transações de pagamentos, transferências de dados, identificações, comunicações *peer-to-peer*, e muitas outras.

Outra característica que promete alavancar o uso desta nova tecnologia e a possibilidade de ser embarcada em vários tipos de dispositivos. Sendo que o mais explorado atualmente são os aparelhos celulares, por se tratar de um dispositivo que a grande maioria das pessoas o possui, por sua versatilidade, funcionalidade e baixo custo relativo. Segundo dados preliminares da Anatel, o Brasil atingiu a marca de 134,2 celulares a cada 100 habitantes (TELECO, 2013).

O NFC estende, ainda, características do protocolo ISO/IEC 14443, que especifica *Identification cards* (cartões de identificação), *Contactless integrated circuit cards* (chips sem contato) e *Proximity cards* (cartões de aproximação). Portanto, herda as propriedades dos *smart card*'s bem como dos *readers* (leitores), ou seja, tem a capacidade de receber, processar e também de enviar dados. Assim, com apenas um celular que possua esta tecnologia pode se comunicar com um *contactless smart card*, um dispositivo de leitura, ou algum outro dispositivo NFC

(AGRAWAL; BHURARIA, 2012), pois são comunicações padronizadas pelos mesmos protocolos.

A conexão NFC, por não haver a necessidade de conexão física, evita desgastes de sockets e rompimento de cabos em redes cabeadas, desgaste da máquina e do plástico de cartões, e assim por diante. Outra característica interessante é a agilidade no estabelecimento de pareamento de dispositivos, dispensando sincronização manual, como no Bluetooth. Quanto à segurança, considerando que o protocolo trabalha com transmissões de dados por um curto raio de alcance, possíveis escutas indesejáveis ou possíveis ataques são dificultados pela própria característica deste padrão.

O NFC tem sido embarcado principalmente em celulares pela sua vasta gama de funcionalidades, conectividade a redes móveis, poder de processamento e por ser um dispositivo já muito comercializado mundialmente. Com a capacidade de um celular NFC reunir também as funcionalidades de um cartão *contactless* (NFC-FORUM, 2008), criou-se o *mobile payment* que é o pagamento eletrônico através deste tipo de dispositivo. Pelo mundo, várias cidades vêm utilizando o *mobile payment* como forma de pagamento (PRADO, 2012). Entre elas, Barcelona se destaca, sendo a primeira cidade a utilizar o celular como principal meio de pagamento (AMERICAN BANKER *apud* PRADO, 2012).

No Brasil, recentemente foi criada a MP 615/13 (2013) que propõe as bases para a regulamentação de novas formas de pagamento, inclusive o *mobile payment*, mas ainda deve ser aprovada pelos plenários da Câmara e do Senado. Contudo, na esfera federal, o governo já estuda projeto para utilizar o celular como um cartão de banco, mas se baseando na ideia do SMS ser utilizado como dinheiro eletrônico (WIZIACK, 2012). Na cidade de São Paulo, a SPTrans, empresa de transporte coletivo urbano, tem pesquisado a utilização do *mobile payment* como forma de bilhetagem (PRADO, 2012).

Assim, este estudo se propõe a compreender como se comporta o padrão NFC, analisando seu funcionamento, e explorando os protocolos relacionados a esta tecnologia. Propõe-se, ainda, a analisar a segurança do NFC, pesquisando vulnerabilidades e possíveis ataques, bem como buscar ferramentas e solução já implementadas com a função de prover maior segurança. Assim, espera-se demonstrar a importância de realizarem-se pesquisas a respeito desta nova

tecnologia, pois pouco tem se discutido sobre o assunto focando-se o mercado brasileiro até o presente momento. E, atualmente, muito poucas empresas têm desenvolvido projetos de implantação da tecnologia NFC no país (FAVORETTO, 2012).

Este trabalho foi dividido em 4 capítulos. No primeiro capítulo, apresentamos os protocolos e produtos relacionados à tecnologia NFC, demostrando os conceitos e paradigmas de cada um pertinente ao contexto deste estudo. No segundo capítulo é feito o estudo aprofundado sobre o protocolo NFC, analisando seus protocolos, sua segurança e seu papel no serviço de *mobile payment*, assunto no qual o NFC está diretamente relacionado. No terceiro capítulo, é feito uma apresentação do OpenNFC, que é um emulador NFC que contém bibliotecas necessárias para o desenvolvimento de aplicativos (*applets*) NFC. É sugerida uma estrutura de instalação com a finalidade de preparar um ambiente de testes para desenvolvedores, sem ter que dispor de uma estrutura real NFC, considerando-se o difícil acesso aos recursos necessários aqui no Brasil, como *tags* e dispositivos NFC. No quarto e último capítulo, é discorrido sobre a conclusão sobre o estudo desenvolvido neste trabalho.

1. Produtos e protocolos relacionados ao NFC

Neste capítulo são apresentados os vários protocolos e tecnologias em que o NFC se baseia. E como o objeto desse estudo é o NFC, são discutidos apenas as características e especificações relevantes a este assunto.

1.1. RFID

O RFID (*Radio Frequency Identification*, Identificação por Radiofrequência), basicamente, explora os sinais de rádio de ondas contínuas para captar dados, onde dispositivos eletrônicos, como etiquetas eletrônicas, *tags* ou *transponders*, emitem sinais e leitoras captam estas informações, possibilitando realizar um processo de identificação (UFRJ, 2013).

Esta tecnologia surgiu junto a Segunda Guerra Mundial, na década de 40. Quando os alemães, japoneses, americanos e ingleses utilizavam radares (descobertos, em 1937, por Sir Robert Alexander Watson-Watt, um físico escocês) para avisá-los, com antecedência, sobre aviões enquanto eles ainda estavam bem distantes. O problema era identificar dentre esses aviões qual era inimigo e qual era aliado. Os alemães, então, descobriram que, se os seus pilotos fizessem curvas de 360º com seus aviões quando estivessem retornando à base, iriam modificar o sinal de rádio que seria refletido de volta ao radar. Assim os técnicos responsáveis pelo radar sabiam que se tratava de aviões alemães.

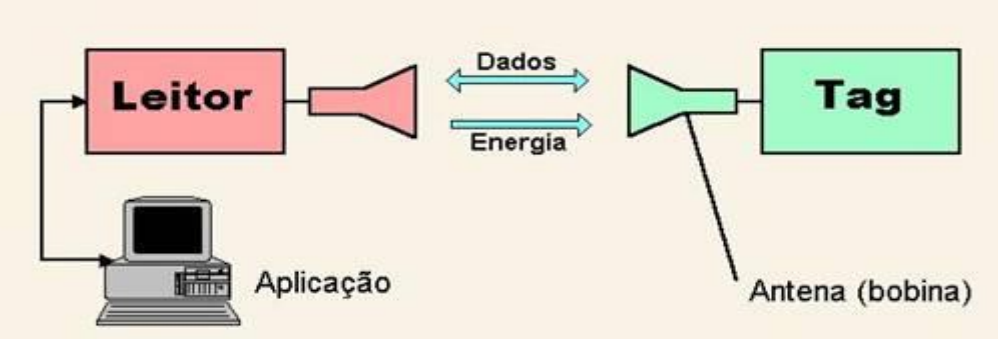
Assim, sob o comando de Watson-Watt, os ingleses desenvolveram o primeiro identificador ativo de amigo ou inimigo (IFF – *Identify Friend or Foe*), colocando um transmissor em cada um dos aviões britânicos. Quando esses transmissores recebiam sinais das estações de radar no solo, começavam a transmitir um sinal de resposta, que o identificava como amigo.

Avanços na área de radares e de comunicação RF (Radiofrequência) continuaram durante as décadas de 50 e 60. Cientistas e acadêmicos dos Estados Unidos, Europa e Japão realizaram pesquisas e apresentaram estudos explicando como a energia RF poderia ser utilizada para identificar objetos remotamente.

Empresas começaram a comercializar sistemas antifurto que utilizavam ondas de rádio para determinar se um item havia sido roubado ou pago normalmente, as *etiquetas de vigilância eletrônica,* as quais ainda são utilizadas nos dias de hoje. Cada etiqueta utiliza um bit. Se a pessoa paga pela mercadoria, o bit é posto em 0, e os sensores não dispararam o alarme. Caso o contrário, o bit continua em 1, assim, se a mercadoria passar através dos sensores, um alarme é disparado (ROBERTI, 2013).

A figura 1 demonstra como um sistema RFID é composto basicamente. Onde há um *transponder* (ou *tag*), contendo uma antena e programada com alguma informação para identificação, afixado ao objeto que se deseja identificar e um dispositivo leitor, que também possui uma antena e um decodificador, acoplado a um computador.

Figura 1. Modelo básico de funcionamento de um sistema RFID.



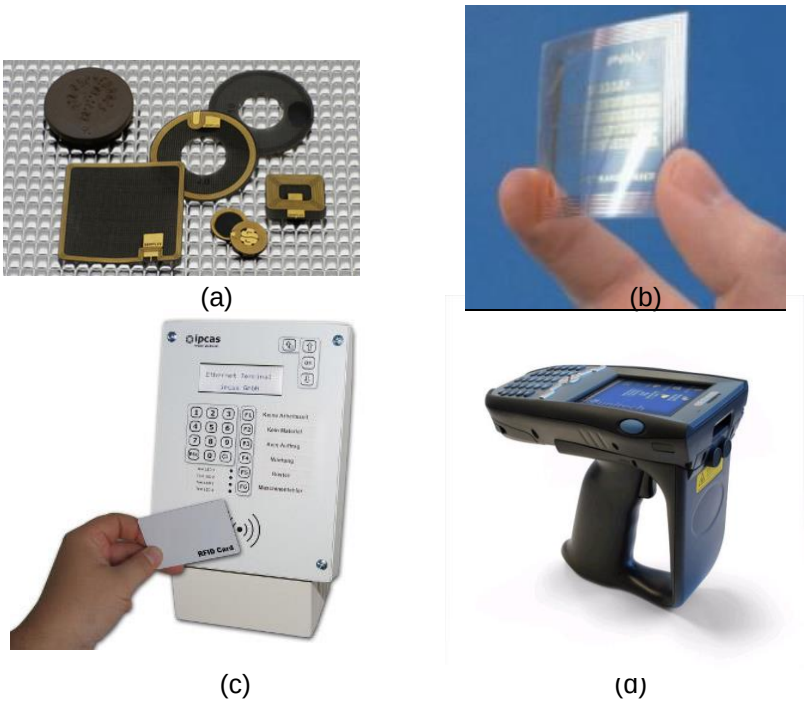
Fonte: UFRJ, 2013.

O leitor, a todo o momento, emite sinais eletromagnéticos. Quando alguma *tag* passa pela área de cobertura da antena, o campo magnético é detectado pelo leitor. O leitor então decodifica os dados que estão codificados na *tag*, e através de um computador o processamento destes dados são feitos.

Existem três tipos de *tags* RFID: as ativas, as passivas e as semi-passivas. As ativas (figura 2.a) possuem fonte de energia própria, uma bateria interna à *tag*. Ela é usada para ativar os circuitos do microchip e para transmitir sinais para um leitor. As *tags* passivas (figura 2.b) não possuem bateira. Usam as

ondas eletromagnéticas emitidas pelo leitor (figuras 2.c e 2.d), transformando-as em energia através de indução eletromagnética. Já as semi-passivas usam bateria para ativar os circuitos interno do chip, mas para transmissão usa a indução de um leitor (RFID JOURNAL, 2013).

Figura 2. (a) Tags RF ativas, (b) Tags RF passivas (c e d) Leitor RF.



Fonte: UFRJ, 2013 e RFIDBr, 2013.

Entre os tipos de *tags*, existem também outros diferenciais técnicos e funcionais relevantes, os quais são apresentados no quadro 1. Tanto as passivas como as ativas, apresentam vantagem e desvantagens. Adotar a mais adequada depende da aplicação que será usada.

Na prática, o RFID é muito utilizado em áreas diversificadas do setor de produção e serviço, como, por exemplo, os sistemas de cobrança automática nas praças de pedágio. Através da instalação prévia de uma *tag* no veículo do usuário, ao passar pela cancela onde está o leitor estático, a *tag* do veículo é ativada, assim

informações do veículo são capturadas e salvas em um banco de dados, para uma posterior cobrança por meio de boletos bancários ou débito em conta. Outro exemplo é seu uso na gerência de estoques e armazéns, quando estes tem um alto fluxo de produtos. Com o RFID, é possível se ter um controle mais ágil, já que não é preciso contato direto entre os funcionários e os produtos, e podendo estes ser rastreados do estoque até os estabelecimentos comerciais.

Tabela 1. Comparações técnicas e funcionais entre o RFID ativo e passivo.

	Ativo	Passivo
Fonte de energia	**Interna à tag**	**Energia transferida do leitor via RF**
Bateria	**Presente**	**Ausente**
Disponibilidade energética	**Contínua**	**Apenas no raio de alcance do leitor**
Força do sinal necessária entre o leitor e a tag	**Muito baixa**	**Muito alta**
Força do sinal disponível entre a tag e o leitor	**Alta**	**Muito baixa**
Alcance de comunicação	**Longo alcance (100 m ou mais)**	**Curto ou muito curto alcance (3 metros ou menos)**
Leitura de múltiplas tags	**Um leitor lê até mil *tags* em um raio de 0,03 Km^2**	**Um leitor lê cerca de 100 *tags* em um raio de 3 metros**
Armazenamento de dados	**Grande capacidade (128 Kbytes)**	**Pouca capacidade (128 bytes)**

Fonte: SAVI TECNOLOGY (2002).

1.2. Smart Cards

Smart card é um termo genérico usado para dispositivos eletrônicos de termos técnicos como *chip card* ou ICC (*integrated circuit card*). Eles são emboçados em cartões com forma e tamanho de um cartão de crédito comum feitos de plástico, e, também, em chips SIM de celulares (figura 3). O circuito integrado é composto de memória e processador, e é controlado por sistema operacional, mas também pode ser um chip de memória não-programável (SIMÕES, 2008).

Figura 3. Exemplos de smart cards.

Fonte: Wikipedia, 2013.

Segundo Rankl e Effing (1997), o cartão incorporado a um microprocessador foi inventado por dois engenheiros alemães em 1967. Mas esta invensão não foi divulgada até o ano de 1974, quando Roland Moreno, um jornalista francês, anunciou a patente do Smart Card na França. Assim, com os avanços na tecnologia de fabricação de microprocessadores, o custo de produção do *smart card* tem reduzido muito. Mas o grande avanço ocorreu em 1984, quando a empresa francesa *Postal and Telecommunications Services* (PTT) realizou, com sucesso, um teste de campo com cartões telefônicos. Desde então, os smart cards não são mais exclusividade do mercado de cartões bancários.

Com a especificação ISO 7816, criada em 1987, o formato dos cartões *smart cards* foi padronizado. Então, os *smart cards* de diferentes fornecedores passaram a poder se comunicar com qualquer máquina leitora que usar o mesmo protocolo de comunicação. Um maior detalhamento deste protocolo será apresentado na próxima seção. Mas os padrões que mais se destacam atualmente, pela difusão do uso dos *smart cards* no comércio eletrônico e na telefonia móvel, são: o EMV (Europay, Mastercard e Visa) - criado em 1993, especifica os cartões de debito e de crédito das instituições internacionais financeiras, Visa, Mastercard e Europay, abrangendo os eletrômecanismos, o protocolo de comunicação, os elementos de dados e as intruções e transações envolvendo os microprocessadores de smart cards bancários (EMVCO, 2013); e o GSM (*Global Standard for Mobile Communications*) - criado em 1987, em um acordo entre 13 países europeus, um

dos mais importantes padrões de cartão inteligente usados na telecomunicação móvel digital (GSMA, 2013).

Pela capacidade de manipulação de dados, os smart cards podem ser usados em diversas aplicações. Com ele é possível realizar transações de identificação, autenticação, armazenamento de dados e aplicações de processamento (HENDRY, 2007). Atualmente, já é usado como: cartão de crédito – em transação eletrônica de pagamentos de compras a crédito; cartão de débito – em transações de pagamentos eletrônicos de compras à vista; cartão de recarga – onde um valor inicial é carregado no cartão e, em contato com um leitor apropriado, este valor é deduzido; cartão de gestão de informação – onde o cartão contém informações úteis para uma determinada finalidade, como, por exemplo, o e-CPF que permitem autenticação junto à receita federal e outros estabelecimentos públicos; cartão de fidelidade – o qual acumula pontos ou créditos com a finalidade de oferecer alguma vantagem ou recompensa ao portador.

Simões (2008) apresenta vantagens do smart card sobre outros recursos até então existentes, como a tarja magnética, por exemplo, capacidade de processamento; execução de operações sobre informações armazenadas; grande capacidade de armazenamento; e elevado nível de segurança e privacidade.

No que se refere à segurança dos *smart cards*, Ferrari, Mackinon, Poh e Yatawara (1998) apontam cinco itens de grande importância que precisam se combinar para que sua segurança seja mantida:

- itens de segurança legíveis no cartão – dados que identifiquem o proprietário e origem do cartão impressos no plástico, como: foto, assinatura, hologramas, emboço (dados em alto relevo), código de segurança;
- itens de segurança do chip – medidas tomadas durante a fabricação do chip que evitam o acesso ao circuito interno e o acesso indevido dos dados armazenados nele;
- itens de segurança do sistema operacional – proteção do acesso aos dados dos *smart card* com uma senha ou uma chave criptográfica, ou medidas como inutilização do chip após um número de tentativas de inserção de senha inválida;

- itens de segurança da rede – instalação de componente *anti-skimming*, que torna a comunicação entre o *smart card* e o leitor segura, ou equipamentos com leitor de *smart card* que retém o cartão caso alguma tentativa de fraude seja verificada.
- itens de segurança da aplicação – preocupação no desenvolvimento da aplicação com a integridade, autenticidade, privacidade e não-repúdio dos dados.

1.2.1. ISO/IEC 7816

A ISO/IEC 7816 é um padrão internacional para os cartões de identificação eletrônica com contato, especialmente os *smart cards*. E foi criada pela *International Organization for Standardization* – ISO (Organização Internacional de Normalização) e pela *International Electrotechnical Commission* – IEC (Comissão Eletrotécnica Internacional), em conjunto.

Ela subdivide-se em quatorze partes:

Part 1: Physical characteristics
Part 2: Cards with contacts — Dimensions and location of the contacts
Part 3: Cards with contacts — Electrical interface and transmission protocols
Part 4: Organization, security and commands for interchange
Part 5: Registration of application providers
Part 6: Interindustry data elements for interchange
Part 7: Interindustry commands for Structured Card Query Language (SCQL)
Part 8: Commands for security operations
Part 9: Commands for card management
Part 10: Electronic signals and answer to reset for synchronous cards
Part 11 Personal verification through biometric methods
Part 12 Cards with contacts — USB electrical interface and operating procedures
Part 13: Commands for application management in multi-application environment
Part 15: Cryptographic information application

Porém, neste trabalho, o estudo será focado na ISO 7816-4, que especifica a organização, a segurança e os formatos de comandos para troca de dados.

No uso de aplicações com *smart cards*, a comunicação entre o host e o cartão ocorre de forma "*half-duplex*", ou seja, enquanto o host envia dados para o

cartão, o mesmo não envia dados para o host, e vice-versa. E, o cartão se comporta de modo escravo, ou seja, ele sempre aguarda comandos do host, os processa e retorna a resposta (CARDWERK, 2013).

No início da comunicação, assim que o *smart card* é energizado, ele emite um pacote inicial chamado ATR – *Answer To Reset* (Resposta a requisição), que contém algumas informações como: protocolo de transporte suportado, taxa de transmissão, e características do hardware do cartão. Em seguida, são trocados pequenos pacotes de dados conhecidos como APDU – *Application Protocol Data Unit* (Unidade de Dado de Aplicação), que é o protocolo de nível de aplicação entre o host e o cartão, e compreende dois tipos de pacotes: o *command APDU*, usado para envio de dados para o cartão; e o *response APDU*, usado para respostas do cartão para o host. Os quadros 2 e 4 mostram a estrutura de um comando APDU e response APDU, respectivamente, e os quadros 3 e 5 descrevem cada um dos seus parâmetros.

Tabela 2. Estrutura de um pacote command APDU.

Header (obrigatório)				***Body* (opcional)**		
CLA	INS	P1	P2	Lc	Data	Le

Fonte: CARDWERK, 2013.

Quadro 3.

Tabela 3. Descrição dos campos de um command APDU.

Campo	**Nome**	**Tam (bytes)**	**Descrição**
CLA	Classe	1	Classe da Instrução
INS	Instrução	1	Código da Instrução
P1	Parâmetro 1	1	Para qualificar o INS, ou para dados de *input*
P2	Parâmetro 2	1	Para qualificar o INS, ou para dados de *input*
Lc	Comprimento	1 a 3	Número de bytes presentes no campo Data
Data	Dados	1 a 256 (Lc)	Dados de comando a serem enviados ao cartão
Le	Comprimento	1 a 3	Quantidade de dados esperado na resposta do cartão

Fonte: CARDWERK, 2013.

Tabela 4. Estrutura de um response APDU.

Body (opcional)	Trailer (obrigatório)	
Data	SW1	SW2

Fonte: CARDWERK, 2013.

Tabela 5. Descrição dos campos de um pacote response APDU.

Campo	**Nome**	**Tam (bytes)**	**Descrição**
Data	Dados	Le – 2	Dados de resposta
SW1	Estado 1	1	Estado do processamento do comando
SW2	Estado 2	1	Qualificador do processamento do comando

Fonte: CARDWERK, 2013.

Na ISO são apresentados os códigos válidos para os campos CLA, INS, SW1 e SW2, bem como suas descrições. Os campos de dados (Data) devem seguir um dos tipos de codificação TLV – *Tag, Length and Value* (*Tag*, Tamanho e Valor): BER-TLV ou SIMPLE-TLV.

1.2.2. ISO/IEC 14443

Criada pela *ISO/IEC Joint Technical Committee 1* (Comitê Técnico Conjunto da ISO e IEC), a ISO/IEC 14443 é um padrão internacional que especifica os *Identification cards* (cartões de identificação), os *Contactless integrated circuit cards* (cartões de circuitos integrados sem contato) e os *Proximity cards* (cartões de aproximação). E subdivide-se em quatro partes (ISO/IEC 14443):

Part 1 – Physical characteristics;
Part 2 – Radio frequency power and signal interface;
Part 3 – Initialization and anticollision;
Part 4 – Transmission protocol.

Focaremos-nos, neste estudo, apenas na especificação 14443-3, que define os protocolos de inicialização e anticolisão, pois as demais especificações não são relevantes ao conteúdo apresentado neste projeto.

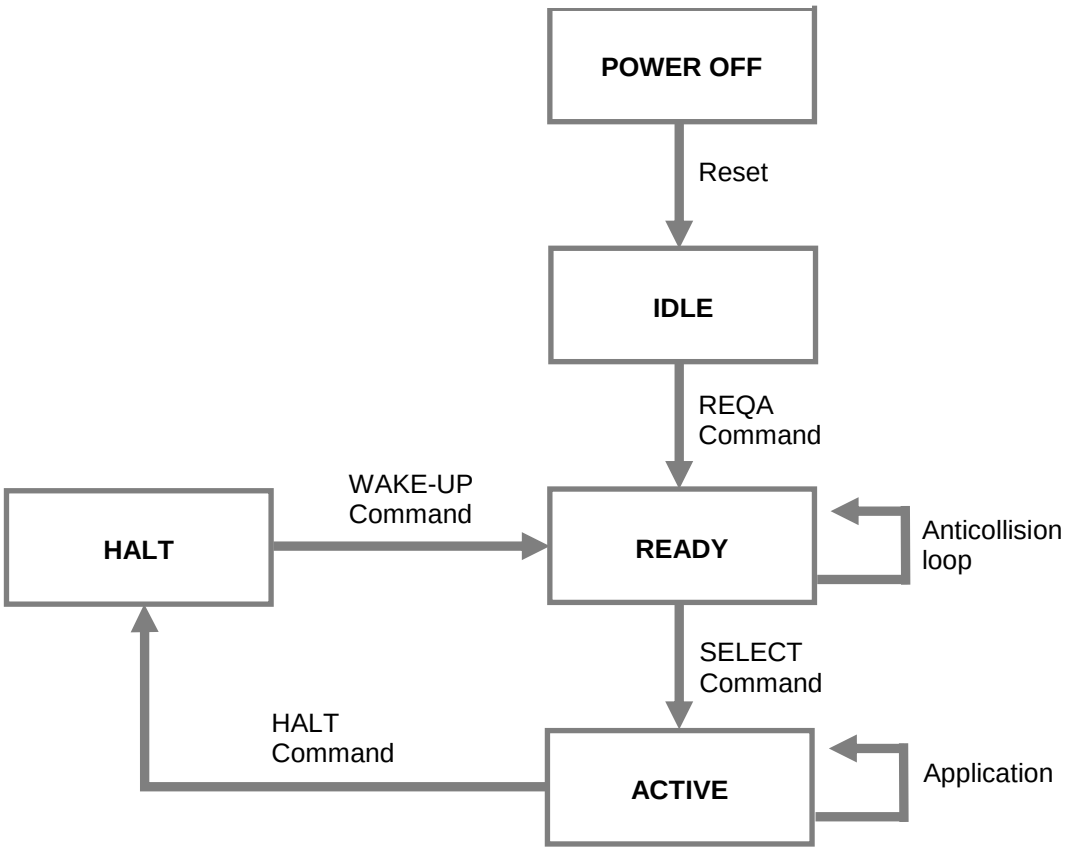
Existem dois tipos de interface de sinal de comunicação entre o PCD – *Proximity Coupling Device* (o leitor) e o PICC - *Proximity Integrated Circuit Card* (o cartão sem contato), o tipo A e o tipo B. Eles diferem entre si quanto à amplitude de modulação do sinal de transmissão, e ao tipo de codificação de dados e representação de bits. Assim, o leitor deve alternar entre os métodos de modulação quando estiver ocioso, para que possa detectar a presença de cartões tanto do tipo A quanto do tipo B. Sendo que, apenas um tipo de interface pode ser ativada durante uma sessão de comunicação, até a desativação pelo leitor ou a remoção do cartão.

Na comunicação *contactless*, surge uma preocupação que na comunicação por contato não existe. Podendo haver mais de um PICC no raio de alcance do PCD, como gerenciar a recepção de respostas de dois ou mais PICC's a comandos de energização no mesmo período de tempo? Esta situação é chamada de colisão.

1.2.2.1 Protocolo de anticolisão para PICC do tipo A

A ISO 14443-3 especifica o protocolo anticolisão para o tipo A, que detecta colisões no nível de bit de um pacote. Nele, existem cinco estados que um PICC pode estar, conforme apresentado na figura 4. No estado **POWER OFF** (desligado), o PICC não está energizado. Sendo energizado através de um comando Reset emitido pelo PCD, ele passa ao estado **IDLE** (ocioso), sendo assim capaz de reconhecer comandos REQA. O PICC, então, entra no estado **READY** (pronto) assim que recebe um comando REQA ou WAKE-UP válido. Quando ele é selecionado através de um comando SELECT, seu estado passa para **ACTIVE** (ativo). E, por fim, ele entra em **HALT** (parado) por um comando HALT ou por um comando específico da aplicação. Neste estado, ele apenas responde a comandos WAKE-UP, passando assim ao estado READY.

Figura 4. Diagrama de estados de um PICC.



Fonte: ISO/IEC 14443.

Os comandos usados pelo PCD para gerenciar a comunicação entre vários PICC's são:

REQA – enviados para detectar PICC do tipo A;

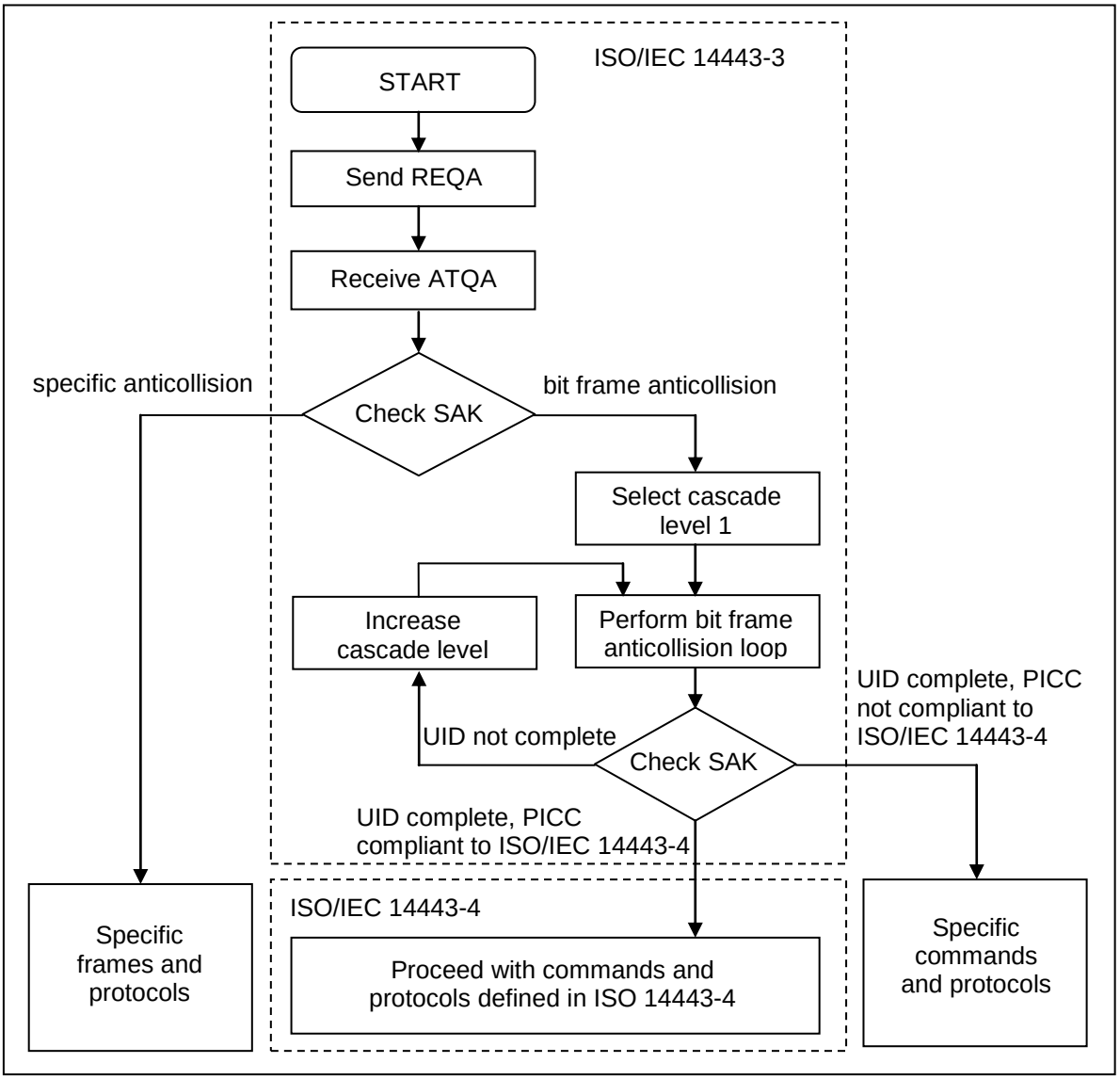
WAKE-UP – enviados para colocar o PICC que está em estado HALT em estado READY;

ANTICOLLISION e **SELECT** – estes são usados para a execução do protocolo anticolisão;

HALT – enviado para parar a comunicação com o PICC selecionado.

Para selecionar um PICC para iniciar uma comunicação, é realizada uma sequência seletiva através do UID – *Unique Identification* do PICC, conforme apresentado na figura 5 e detalhado mais adiante.

Figura 5. Fluxo de inicialização e anticolisão para o PCD.



Fonte: ISO/IEC 14443.

Quando um comando REQA é transmitido pelo PCD, todos PICC's que estão no seu raio de ação, e no estado IDLE, respondem com seus ATQA's e passam para o estado READY. O PCD, por sua vez, efetua a rotina anticolisão selecionando um PICC para iniciar comunicação (definida pela ISO/IEC 14443-4). Assim, este passa ao estado ACTIVE.

1.2.2.2 Protocolo de anticolisão para PICC do tipo B

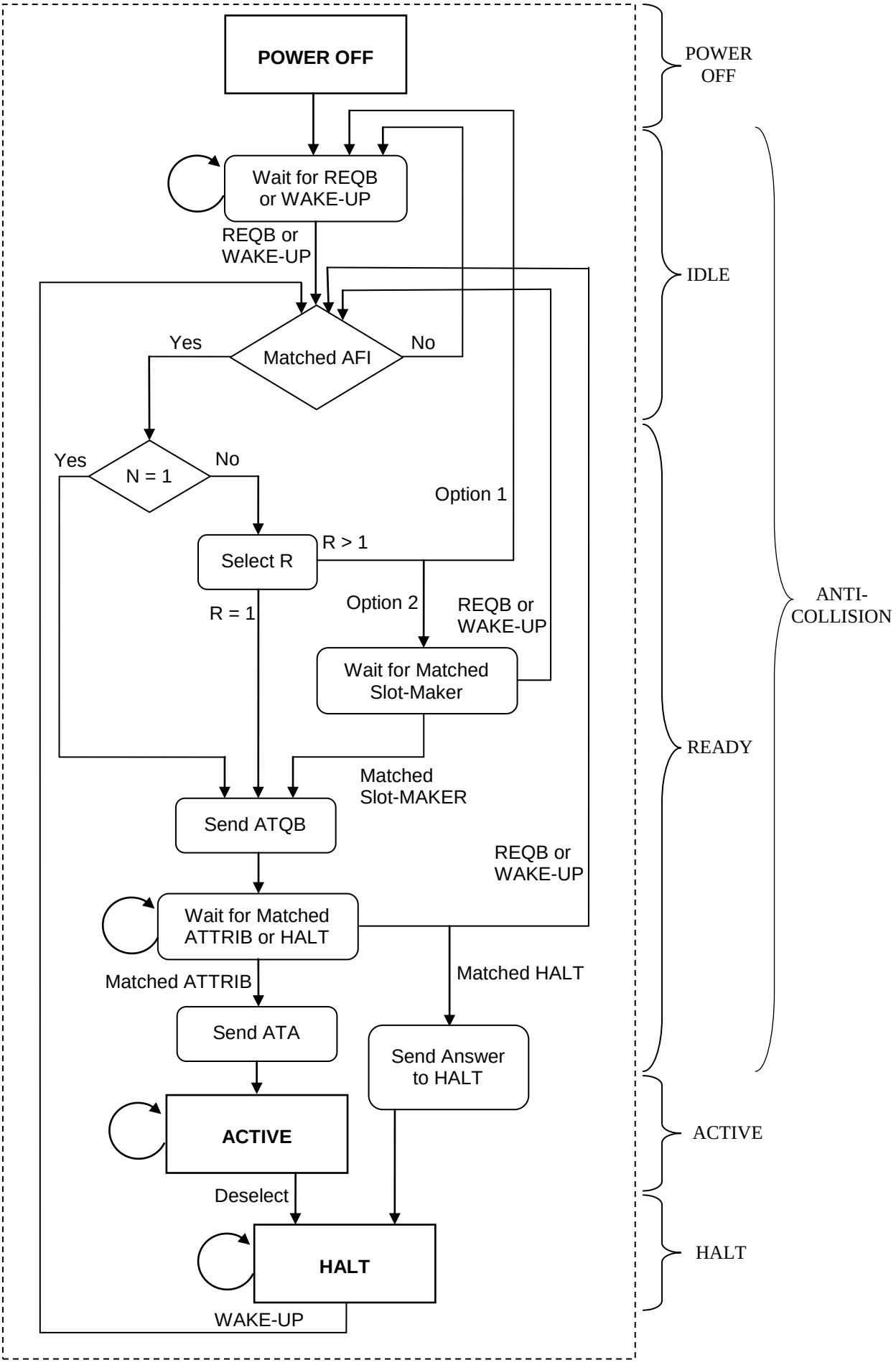
Como para o tipo A, a ISO 14442-3 também especifica protocolo de gerenciamento de colisão para os PICC's do tipo B. O esquema é baseado na definição de slots (fatias) de tempo em que os PICC's são convidados a responder com o mínimo de dados de identificação. Também, o número de slots é parametrizado e pode variar de 1 (um) a algum número inteiro, e a probabilidade do PICC responder em cada slot de tempo também é controlada.

Na sequência anticolisão, os PICC são autorizados a responder apenas uma vez. Consequentemente, mesmo no caso da presença de múltiplos PICCs no campo de ação do PCD, haverá provavelmente um slot em que apenas um PICC responda e esteja onde o PCD é capaz de capturar seus dados de identificação. Com base nestes dados o PCD é capaz de estabelecer um canal de comunicação com o PICC identificado.

Na figura 6, adiante, é apresentado o diagrama do fluxo de transições de estados de um PICC do tipo B. Onde, o PCD inicia o processo de anticolisão emitindo comandos REQB ou WAKE-UP que contém um valor N que indica o número de slot's atribuidos ao processo. Assim, os PICC's no campo de ação do PCD com o código AFI correspondente são afetados.

Se N for igual a 1, então todos os PICCs respondem com seu ATQB. Se for maior, então o PICC seleciona um número aleatório R em um intervalo de 1 a N. Se R for igual a 1, então o PICC responde com ATQB. Se o R for maior do que 1, então o PICC espera, silenciosamente, por um comando Slot MARKER (opção 1), e depois responde com ATQB. Por isso, o PCD everigua, periodicamente, todos os slots para verificar se algum PICC está presente no campo. Sendo premitido que o PICC responda em apenas um slot, dos N slots. Quando o PCD recebe

Figura 6. Fluxo de transição de estados de um PICC.



Fonte: ISO/IEC 14443-3.

a resposta ATQB, ele pode responder com um comando HALT correspondente para colocar o PICC em estado HALT (suspenso), ou pode responder com um comando correspondente ATTRIB, colocando-o no estado ACTIVE (ativo) e, assim, iniciar a transação.

Todos os pacotes trocados entre o PCD e o PICC contém um campo com um valor para conferência de integridade chamado CRC. Assim, quando o PCD recebe uma resposta ATQB com um erro de CRC, é assumido que uma colisão tenha ocorrido. Então, o PCD completa as transações com os outros PICCs no campo e, em seguida, coloca-os no estado de suspensão. Um novo comando REQB é emitido, fazendo com que cada PICC no campo que não tenha sido suspenso selecione um novo número aleatório R. Este procedimento resolve o problema dos PICC's que sofreram colisão na sua transmissão de dados.

Este processo continua até que todos os PICCs no campo tenham suas transações completadas. Qualquer comando recebido pelo PICC durante o processo de anticolisão com um erro de CRC ou erro de formato de quadro é ignorada.

1.2.3. MIFARE

MIFARE é uma marca registrada de chips produzidos pela NXP Semicondutores. Baseado no padrão internacional ISO/IEC 14443 – tipo A, seus *smart cards contactless* (sem contato) e leitoras do tipo *read/write* (leitura/escrita) trabalham a uma distância de até 10 cm, e possuem processamento criptográfico de chave pública (PKI), permitindo aplicações múltiplas (MIFARE.NET, 2013).

Os produtos fabricados pela MIFARE são: o *MIFARE Ultralight*™, o *MIFARE Ultralight™ C*, o *MIFARE™ Classic 1K*, o *MIFARE™ Classic 4K*, o *MIFARE Plus™ S 2K*, o *MIFARE Plus™ S 4K*, o *MIFARE Plus™ X 2K*, o *MIFARE Plus™ X 4K*, o *MIFARE DESFire™ EV1 2K*, o *MIFARE DESFire™ EV1 4K*, e o *MIFARE DESFire™ EV1 8K*. Nos quadros 6-a e 6-b, são apresentadas algumas das características técnicas dos diversos *chip's contacless* produzidos.

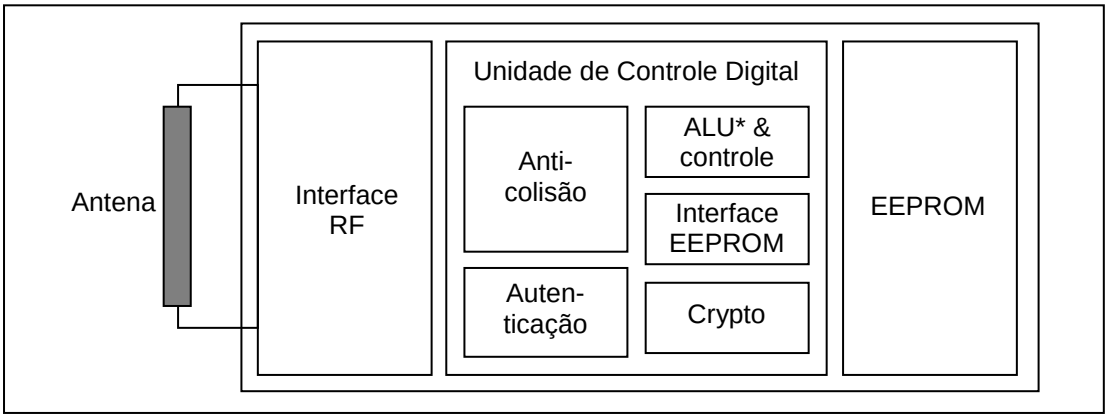
Tabela 6. Características técnica dos chip's contactless MIFARE.

Produtos/ Características	MIFARE Ultralight	MIFARE Ultralight C	MIFARE Classic 1K	MIFARE Classic 4K	MIFARE Plus S 2K	MIFARE Plus S 4K	MIFARE Plus X 2K	MIFARE Plus X 4K	MIFARE DESFire EV1 2K	MIFARE DESFire EV1 4K	MIFARE DESFire EV1 8K
	MF0 IC U1X	MF0 IC U2X	MF1 S50	MF1 S70	MF1 SPLUS 60	MF1 SPLUS 80	MF1 PLUS 60	MF1 PLUS 80	MF3 IC D21	MF3 IC D41	MF3 IC D81
Memória											
Tamanho do EEPROM (bytes)	64	192	1024	4096	2048	64	4096	4096	2048	4096	8192
Área OTP (bits)	32	32	-	-	-	32	-	-	-	-	-
Duração da escrita (ciclos)	10.000	10.000	100.000	100.000	200.000	10.000	200.000	200.000	500.000	500.000	500.000
Retenção de dados (anos)	5	5	10	10	10	5	10	10	10	10	10
Organização	16 páginas c/ 4 bytes	48 páginas c/ 4 bytes	16 setores c/ 64 bytes	32 setores c/ bytes e 8 setores c/ 256 bytes	32 setores com 64 bytes	16 páginas c/ 4 bytes	32 setores c/ 64 bytes e 8 setores c/ 256 bytes	32 setores c/ 64 bytes e 8 setores c/ 256 bytes	Sistema de arquivo flexível	Sistema de arquivo flexível	Sistema de arquivo flexível
RF-Interface											
Conformidade à ISO 14443[a]	Sim – até a camada 3	Sim – até a camada 3	Sim – até a camada 3	Sim – até a camada 3	Sim – até a camada 4	Sim – até a camada 4	Sim – até a camada 4	Sim – até a camada 4	Sim – até a camada 4	Sim – até a camada 4	Sim – até a camada 4
Frequência (MHz)	13,56	13,56	13,56	13,56	13,56	13,56	13,56	13,56	13,56	13,56	13,56
Taxa de trans-ferência (kbits/s)	106	106	106	106	106 ... 848	106	106 ... 848	106 ... 848	106 ... 848	106 ... 848	106 ... 848
Anticolisão	Bit a bit	Bit a bit	Bit a bit	Bit a bit	Bit a bit	Bit a bit	Bit a bit	Bit a bit	Bit a bit	Bit a bit	Bit a bit
Distância de operação (mm)	Até 100	Até 100	Até 100	Até 100	Até 100	Até 100	Até 100	Até 100	Até 100	Até 100	Até 100
Segurança											
Número Serial (bytes)	7 - UID	7 – UID	4 NUID ou 7 – UID	4 NUID ou 7 – UID	4 NUID ou 7 – UID	7 – UID	4 NUID ou 7 – UID	4 NUID ou 7 – UID	7 – UID	7 – UID	7 – UID
Gera Número Randômico	-	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Chave de acesso	-	1 chave	2 chaves por setor	2 chaves por setor	2 chaves CRYPTO1 ou AES por setor	2 chaves CRYPTO1 ou AES por setor	2 chaves CRYPTO1 ou AES por setor	2 chaves CRYPTO1 ou AES por setor	14 chaves por aplicação	14 chaves por aplicação	14 chaves por aplicação
Condições de acesso	Por página	Por página	Por setor	Por setor	Por setor	Por setor	Por setor	Por setor	Por arquivo	Por arquivo	Por arquivo
Segurança - MIFARE Classic (Crypto1)	-	-	Suportado	Suportado	Suportado a nível de segurança 1 e 2	Suportado a nível de segurança 1 e 2	Suportado a nível de segurança 1 e 2	Suportado a nível de segurança 1 e 2	-	-	-
Segurança DES & DES3	-	Autenticação	-	-	-	-	-	-	CMACing / Cifragem	CMACing / Cifragem	CMACing / Cifragem
Segurança AES 128	-	-	-	-	CMACing	CMACing	CMACing / Cifragem	CMACing / Cifragem	CMACing / Cifragem	CMACing / Cifragem	CMACing / Cifragem

Fonte: NXP (2013).

Os chips MIFARE são integrados a um cartão plástico que segue as especificações da ISO/IEC 7810, e é composto por três partes (NXP, 2013): a Interface de Radiofrequência, a Unidade de Controle Digital e a EEPROM - *Electrically-Erasable Programmable Read-Only Memory* (memória que pode ser programada e apagada várias vezes eletronicamente), conforme ilustrado na figura 7.

Figura 7. Estrutura de ICC MIFARE.



Fonte: SIMÕES, 2008.
** ALU – Arithmetic Logic Unit (unidade lógica aritmética).*

Pela Interface RF os dados (e energia) são recebidos e enviados. A capacidade de armazenamento da memória varia conforme o tipo do chip MIFARE. E, a unidade de controle digital é composta de cinco componentes:

- Anti-colisão – componente de controle de comunicação com vários cartões, para ser realizada de forma sequencial e sem interferência de dados;
- Autenticação – componente que efetua o processo de autenticação para acesso aos blocos de memórias que são protegidos por chaves criptográficas;
- Unidade Lógica Aritmética e controle – unidade que realiza, como o próprio nome diz, cálculos lógicos e aritméticos e controla suas operações;
- Interface EEPROM – componente que fornece acesso à memória;
- Crypto – componente de controle e cálculos criptográficos.

1.2.4. FeliCa

Patenteado e produzido pela Sony Corporation, o FeliCa – *Felicity Card*, é um sistema de *smart card contactless* semelhante ao MIFARE, usado em grande escala em muitos países asiáticos, principalmente em sistemas de bilhetagem de transporte público e em pagamentos eletrônicos (SONY GLOBAL, 2013).

Compatível com o padrão JIS: X6319-4 criado pela JICSAP - *Japan IC Card System Application Council* (conselho para desenvolvimento de sistemas para ICC japonês), que especifica implementação para smart cards, os smart cards FeliCa possuem memória não-volátil integrada e um chip de comunicação sem fio para troca de dados com um leitor compatível. Além de ser usada criptografia para proteção dos dados armazenados (NEARFIELDCOMMUNICATION.ORG, 2013).

2. O NFC – Near Field Communication

Segundo a definição apresentada pelo NFC FORUM (2013), o NFC é a tecnologia que torna a vida mais fácil e conveniente, simplificando transações, trocas de conteúdo digital e conexões entre dispositivos eletrônicos, com um toque ou a aproximação entre eles. A ideia é que os usuários desta tecnologia sejam capazes de realizar uma comunicação rápida e segura entre vários dispositivos sem ter que dispender esforços em configurações de redes.

O NFC nasceu da cooperação entre a Nokia Corporation, a *Royal Philips Electronics* e a *Sony Corporation*, em 2004, criando o Fórum NFC para "incentivar a implementação e a padronização da tecnologia NFC para assegurar a interoperabilidade entre dispositivos e serviços" (PHILIPS, 2013), e é padronizado pela ISO 18092 / ECMA 340 (NFCIP-1) que especifica a interface e o protocolo de comunicação de fio entre dispositivos acoplados.

Um celular com a tecnologia NFC pode ser usado em diversas aplicações:

- ✓ Pagamentos – usado como um cartão de crédito para efetuar pagamentos de compras em estabelecimentos comerciais, bastando apenas aproximar o aparelho de um POS[1] (*Point of Sale*) *contactless*;
- ✓ Transportes – usado como ticket, cartão de embarque, ou até mesmo cartão de fidelização para crédito de pontos, onde os viajantes aproximam seus celulares ao leitor NFC no momento do embarque;
- ✓ Serviços médicos – usado para armazenamento de informações médica sobre seu portador, como tipo sanguíneo e doenças, auxiliando em atendimentos de emergência, bem como o histórico médico, constando tratamentos realizados e os dados dos profissionais de saúde responsáveis;
- ✓ Capturas de informações de avisos e propagandas – sendo usado para ler informações contidas em *tags* afixados em propagandas em cartazes e em revistas, ou até mesmo disparar um aplicativo para requisição de um serviço on-line, a partir da leitura de uma *tag* contida em um anúncio, por exemplo, um pedido de entregas ou um taxi.

[1] POS – máquina de cartões presente em grande parte de estabelecimentos comerciais.

Tal variedade de aplicações se deve ao fato de que um dispositivo com a tecnologia NFC pode operar em três modos diferentes (KILÅS, 2009):

- **Emulador de cartão** – quando o dispositivo NFC se apresenta como um *smart card* ou um cartão de crédito *contactless*. Exemplo, usar um celular NFC para efetuar pagamentos de compras ou bilhetes de transporte público (figura 8-a).
- **Emulador de leitor** – quando o dispositivo se comporta como um leitor de dados de *tags* NFC. Quando se aproxima um celular de um pôster contendo uma *tag* e carrega seu conteúdo (figura 8-b), por exemplo.
- **Comunicador *Peer-to-Peer*** – quando o dispositivo NFC se comunica com outro dispositivo NFC, trocando dados entre eles (figura 8-c).

Ora seguindo os padrões da ISO 18092, ora seguindo a ISO 14443, considerando-se que o NFC é uma extensão da tecnologia dos cartões *contactless*, e que também utilizam a mesma infraestrutura. O comportamento varia dependendo da aplicação utilizada no momento.

Figura 8. (a) Dispositivo NFC operando como emulador de cartão; (b) Dispositivo NFC operando como emulador de leitor contactless; (c) Dispositivo NFC operando em comunicação Peer-to-Peer.

Fonte: SLASHGEAR; MOBILEPEDIA; LETSGOMOBILE; 2013.

No protocolo NFCIP-1, um dispositivo é identificado como *initiator ou target,* ou seja, aquele que inicia a comunicação e controla a troca de dados, ou aquele que responde às requisições do *initiator,* respectivamente. O protocolo apresenta, ainda, dois modos de operação: o **modo de comunicação ativa**, onde ambos dispositivos geram ondas eletromagnéticas para transportar dados, e o **modo de comunicação passivo**, onde um dos dispositivos gera as ondas enquanto o outro usa a modulação recebida para retransmitir dados. Quanto à velocidade de comunicação, a taxa de transferência de dados pode ocorrer em 106, 212 ou 424

kbits/s, sendo o dispositivo portador da aplicação o responsável pela determinação da velocidade inicial. Contudo, provavelmente, ela precise ser adaptada por necessidade da própria aplicação ou pelo ambiente da comunicação (ECMA – NFC WHITE PAPER, 2004).

Seguindo o protocolo citado no parágrafo anterior, a interface de operação do NFC é feita por radiofrequência, trabalhando em 13,56 MHz e com distâncias de até 10 cm. Por esta frequência não ser regularizada, não há restrições e nem é necessário licença para uso do NFC. Por isso, pode haver vários dispositivos em uma mesma área. Assim, a comunicação entre os dispositivos NFC deve ser *half-duplex*, o que significa que um dispositivo deve "escutar" o meio antes de iniciar uma transmissão, e assim fazê-lo apenas se nenhum outro já estiver transmitindo naquele período de tempo, para que não interfira no sinal emitido pelo outro dispositivo. Mas se ocorrer o caso de dois ou mais *targets* responderem a uma requisição de um *initiator* ao mesmo tempo exatamente, uma colisão é detectada pelo *initiator* através de um sistema anti-colisão. Maiores detalhamentos sobre o protocolo ECMA 340 (NFCIP-1) serão discutidos na próxima seção.

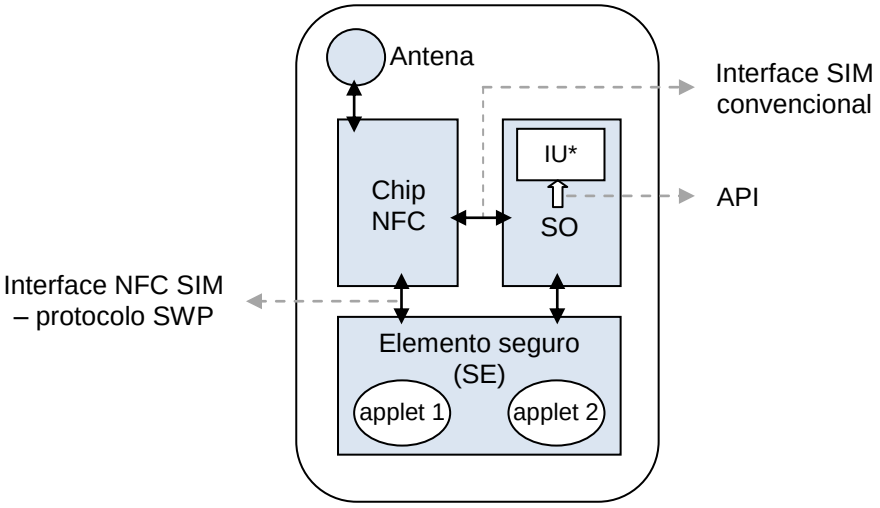
Apesar da possibilidade do NFC ser embarcado em dispositivos diversos como os notebooks, PDA's, TV's, tablet's e muitos outros, ele se apresenta principalmente em dispositivos celulares. Pois, além do potencial de processamento encontrado hoje nos dispositivos, o celular é um equipamento amplamente comercializado pelo mundo e possui um custo relativamente acessível na grande maioria dos países. Estima-se que, entre 2005 e 2011, houve um crescimento de 107% no número de brasileiros que possuem telefone celular (EXAME.COM, 2013).

A GSMA – *Groupe Speciale Mobile Association* é uma associação, formada em 1995, por operados de telefonia móvel e empresas relacionadas dedicadas a apoiar a padronização, implementação e promoção do sistema de telefonia móvel GSM. Ela apresenta a composição básica de um celular com o recurso NFC, o qual deve ser formado de um **chip controlador NFC** (com uma antena) e um **Secure Element – SE** (elemento seguro), conforme demonstrado através da figura 9. O elemento seguro contém um processador seguro, memória inviolável para armazenamento e memória de execução.

Há três tipos de elemento seguro selecionados pela GlobalPlataform Inc. (2009) para celulares NFC: o UICC – *Universal Integrated Circuit Card*, chip SIM

(Módulo de Identificação de Assinante) usado em telefones celulares em redes com a tecnologia 3G; o cartão de memória seguro, um micro SD, por exemplo; ou chip de memória segura já embarcado no dispositivo, como nos casos de celulares vendidos que possuem a função NFC embarcada (Galaxy SIII, no Brasil). Neles são armazenados os dados para os aplicativos NFC (*applets*) de forma segura, pois oferece tanto segurança física, como segurança lógica, permitindo que aplicativos NFC sejam executados em um ambiente seguro. Fornece também isolamento entre aplicações, e um canal seguro entre provedores de serviços e seus aplicativos. A vantagem de se optar pelo uso do chip SIM é a portabilidade de funcionalidades.

Figura 9. Arquitetura de um celular NFC.



** IU – Interface ao usuário*

Fonte: SIMÕES, 2008.

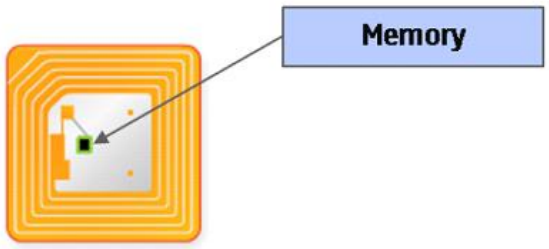
O chip NFC gerencia a comunicação entre o SE (elemento seguro), o sistema operacional do dispositivo, onde as aplicações estão sendo processadas, e a antenas que faz a transmissão dos dados através de radiofrequência. Na interface entre o SIM e o chip NFC é usado o protocolo SWP[2] – *Single Wire Protocol* (Protocolo de fio único).

[2] SWP – protocolo *full duplex* orientado a bit, ou seja, é possível a transmissão e a recepção de dados. Onde o chip NFC fornece energia, clock, dados e sinal para o gerenciamento do *bus* de dados. Sendo o chip NFC mestre e o UICC escravo.

O NFC Fórum (2008) define, ainda, três áreas necessárias para uma execução confiável de aplicações NFC em dispositivos celulares: o controlador NFC (chip NFC) que possui interface de transmissão e recebimento de dados entre as demais áreas que ainda serão definidas; a AEE - *Application Execution Environment* (ambiente de execução de aplicativos) que é a área comum para execução de aplicativos do celular, em geral como o discador, agenda, despertador; e a TEE – *Trusted Execution Environment* (ambiente de execução confiável) que é uma área segura para armazenamento de dados e aplicativos e sua execução. A TEE é provida por um SE contido no dispositivo, seja hardware (SIM e micro SD) ou software (alguma partição de memória protegida – Soft-SE)

As *tags* NFC são finos dispositivos eletrônicos (figura 10) que se assemelham a adesivos, e possuem uma antena e uma pequena memória, e são alimentadas ou lidas através de indução magnética (campo magnético). Estas podem ser incorporadas a qualquer tipo de produtos, como cartões de visitas, imãs de geladeira, pulseiras de identificação, chaveiros, etc...

Figura 10. Tag NFC.



Fonte: SHOWMETECH, 2013.

A NFC Fórum especifica quatro tipos de plataformas diferentes de *tags* para NFC, cada uma apropriada para cada tipo de tarefa e depende de como será usada (NOKIA DEVELOPER, 2012):

- **Tipo 1** – este tipo utiliza um modelo de memória simples, com uma capacidade física total de 120 bytes, mas apenas 96 bytes são disponíveis para alocação de dados dos usuários, e é dividida em blocos de 8 bytes cada. Baseada na norma ISO 14443-A, as *tags* são *read/re-writable* (leitura/regravável), mas os usuários podem

configurá-las para serem do tipo *read-only* (apenas leitura). Sua velocidade de comunicação é de 106 kbits/s e possui baixo custo.

- **Tipo 2** – este tipo é semelhante ao tipo 1, diferenciando-se apenas em seu tamanho de memória total de 64 bytes, com 48 bytes para dados de usuários, além de ser dividida em blocos de 4 bytes. Possui baixo custo.
- **Tipo 3** – este tipo não possui capacidade de memória definida, mas sua organização é disposta em blocos de 16 bytes. Este tipo é diferenciado dos demais, pois seus blocos não são endereçados diretamente, e sim relativamente ao *Service* relacionado, que são comparados aos arquivos em um sistema de arquivos. Cada *Service* possui um número de blocos de memória associado e podem ser endereçados pelo seu código que deve ser único em cada *tag*. Seu custo é alto.
- **Tipo 4** – possui sistema de arquivo flexível com diferentes tipos de arquivos e tipos de acesso, e inclui verificação de integridade e opção de cifragem como algumas de suas características principais. Além de ser totalmente compatível às normas ISO 14443-A e ISO 14443-B. Estas são pré-configuradas em fábrica para serem do tipo *read/re-writable* ou *read-only*. E sua capacidade de memória é variável de até 32 Kbytes e sua velocidade de comunicação chega a 424 kbits/s. Possui um custo relativamente alto.

Em comparação a outras tecnologias de comunicação, o RFID e o Bluetooth, por exemplo, a Infosys Research *apud* Agrawal e Bhuraria (2012) destacou o NFC como sendo a tecnologia mais avançada, levando-se em consideração o tempo de inicialização da comunicação entre dispositivos, o raio de alcance de operação, usabilidade, aplicação, necessidade de conhecimento técnico ou experiência para uso do consumidor e a conectividade com outros dispositivos.

O NFC se mostra vantajoso, tanto para consumidores como para comerciantes, por ser: intuitivo – não sendo necessário mais do que um simples toque para iniciar uma interação; versátil – podendo ser usado em vários ramos

industriais e ambientes; aberta e baseada em padrões – as camadas subjacentes da tecnologia NFC seguem padrões internacionais ISO, ECMA, e ETSI; capacitadora – possibilita conexões simples e rápidas de tecnologias sem fio, como o Bluetooth e o Wi-Fi; inerentemente seguro – pois as transmissões são de curto alcance; e interoperável – pois o NFC trabalha com a infraestrutura já existente dos cartões sem contato (NFC-FORUM, 2013).

Algumas empresas como a VISA (com o PayWave), a MasterCard (com o *PayPass*), e o Google (com o Google Wallet) já estão investindo em soluções de *mobile payment*, porém grandes parte das empresas não ingressaram no mesmo ritmo. Em um futuro não muito distante, estima-se que esta tecnologia domine o mercado, substituindo cartões e até dinheiro. Atualmente, um impedimento para a popularização desta tecnologia é a pequena opção de aparelhos a venda com NFC embarcado no país. No Japão, o NFC faz parte do dia a dia de grande parte da população. Em Tóquio, o sistema de catracas do metrô permite que as passagens sejam compradas com a aproximação do aparelho de telefone (TECMUNDO, 2013).

2.1. O Protocolo ECMA–340 (NFCIP–1)

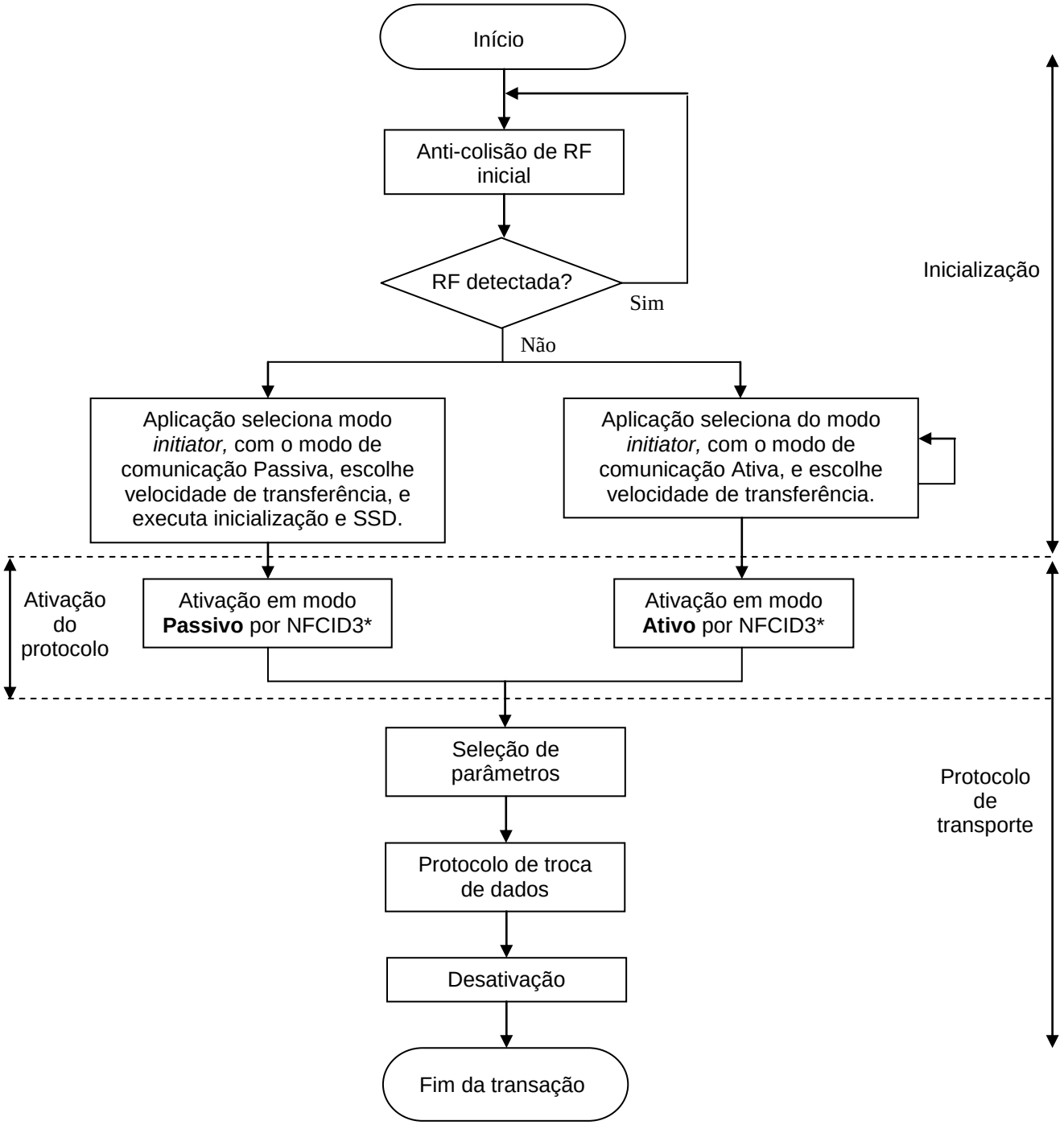
O ECMA – *European Computer Manufacturers Association* é uma organização internacional privada sem fins lucrativos de padronização de informações e sistemas de comunicação. O NFCIP–1 – NFC Interface and Protocol especifica a interface e o protocolo para comunicação sem fio simples entre dispositivos de acoplamente fechado, com velocidade de comunicação de 106, 212 e 424 kbps (ECMA-340, 2004).

O fluxo geral do protocolo NFCIP-1 (figura 11) é dividido em duas partes: a **inicialização** e o **protocolo de transporte**. A inicialização é a fase em que são realizados os processos de anti-colisão, onde o *initiator* escuta o meio antes de iniciar sua transmissão, a seleção do modo de comunicação com o *target* (ativa ou passiva), a eleição do dispositivo *target* da comunicação (SDD – *Single Device Detection*), e a escolha da velocidade de transmissão. O protocolo de transporte, por sua vez, subdivide-se em três partes: a ativação do protocolo, o protocolo de troca de dados e a desativação do protocolo.

O protocolo NFCIP-1 especifica como a comunicação entre dois dispositivos NFC é realizada, apresentando as seguintes ações consecutivas:

- o papel do dispositivo deve estar configurado, por default, como *target*, devendo o dispositivo permanecer dormente, aguardando por um comando de algum *initiator*;
- se requisitado pela aplicação do dispositivo, seu papel deve ser alterado para *initiator*. Assim, a aplicação determina, também, o modo de comunicação e a velocidade de transferência;
- como *initiator*, o dispositivo realiza uma varredura no campo de radiofrequência. Se nenhuma RF for detectada, ele pode ativar seu campo de RF, e, consequentemente, algum *target* ser ativado por ele;
- assim o *initiator* pode enviar comandos no modo de comunicação e velocidade selecionados previamente, bem como o *target* transmitir sua resposta no mesmo modo de comunicação e velocidade enviado pelo *initiator*.

Figura 11. Fluxo geral de inicialização e SDD.



** NFCID3 – Identificador randômico de ativação do protocolo de transporte.*
Fonte: ECMA-340, 2004.

É válido lembrar que, durante uma transação, o modo de comunicação (ativo ou passivo), bem como os papéis dos dispositivos na comunicação (*initiator* ou *target*), não muda até que a comunicação seja finalizada, ou seja, os aparelhos sejam afastados.

2.2. A Segurança no NFC

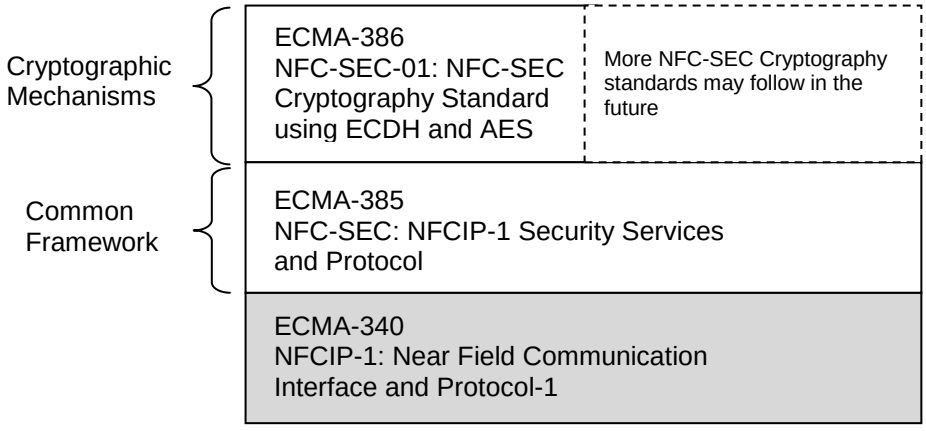
No Brasil, a maioria das pessoas ainda desconhece esta tecnologia emergente que é o NFC. E, apesar dele ser relativamente seguro pelo seu curto raio de ação, existem algumas vulnerabilidades que podem comprometer seu sucesso. Assim, nas próximas seções é apresentado o protocolo NFC-SEC e também os principais ataques à comunicação NFC conhecidos atualmente.

2.2.1. O NFC-SEC

O padrão NFCID-1 (ISO/IEC 18092), por si só, não oferece segurança ao NFC, pois não é especificado utilização de algum recurso que garanta a confidencialidade ou a integridade dos dados trafegados, como o uso da criptografia.

O NFC-SEC é uma pilha de protocolos que provê segurança à comunicação, independentemente de funcionalidades criptográficas específicas da aplicação, garantindo um bom equilíbrio entre segurança e performance. Porém, funciona apenas para o modo de comunicação NFC *peer-to-peer*, não servindo para o modo leitor ou para o modo emulador de cartões (COSKUN; OK; OZDENIZCI; 2012).

Figura 12. Pilha de protocolos NFC-SEC.

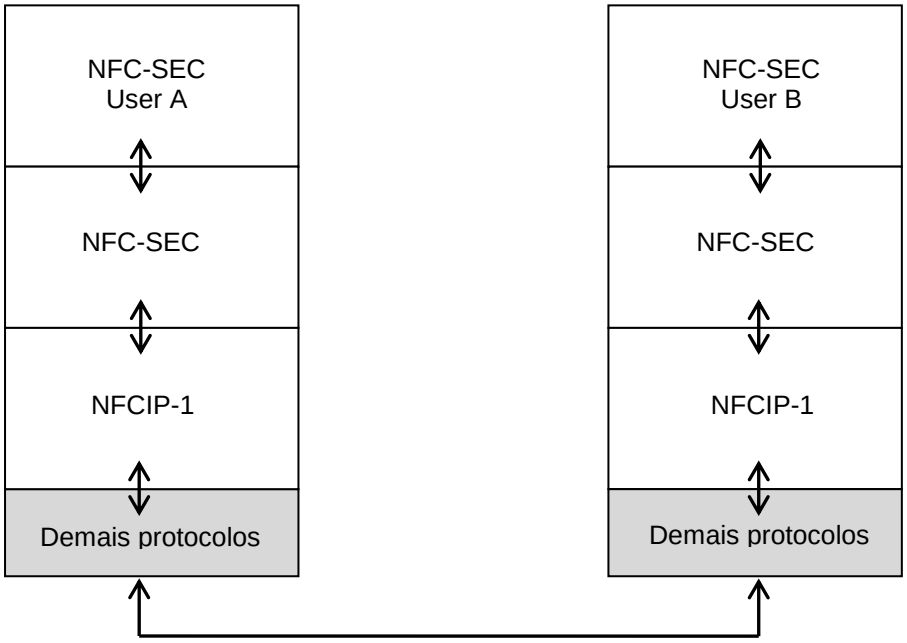


Fonte: COSKUN; OK; OZDENIZCI (2012).

A pilha NFC-SEC é composta de dois protocolos (figura 12). Na base, fica o NFC-SEC: NFCIP-1 *Security Services and Protocol*, que é especificado pela norma

ECMA-385 (2010) e tem como papel principal desempenhar a segurança contra a escuta e a modificação dos dados trafegados entre dispositivos NFC. Na camada acima, fica o NFC-SEC-01: NFC-SEC *Cryptography Standard using* ECDH *and* AES, especificado pela ECMA-386 (2010), que implementa mecanismos criptográficos usando algoritmo ECDH – Elliptic Curve Diffie-Hellman (curva elíptica de Diffie-Hellman) para troca de chaves e algoritmo AES – *Advanced Encryption Standard* para cifragem e verificação de integridade de dados. Outros tipos de algoritmos podem ser usados futuramente.

Figura 13. Aquitetura do NFC-SEC.

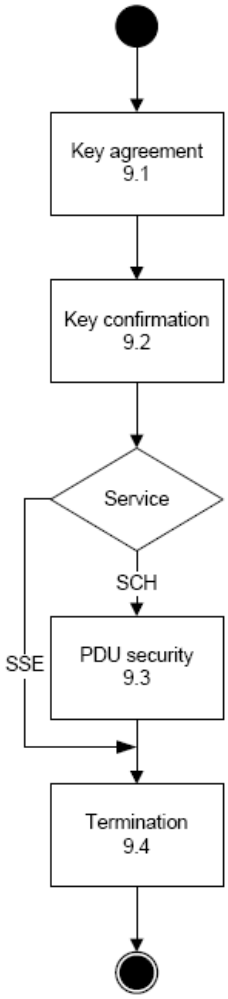


Fonte: Elaborado pela autora deste trabalho.

A arquitetura do NFC-SEC segue o modelo OSI especificado pela ISO/IEC 7498-1, conforme demonstrado na figura 13. E no protocolo são disponibilizados dois serviços ao NFC-SEC User: o SSE –*Shared Secret Service* e o SCH – *Secure Channel Service*. Através destes serviços, a transmissão entre os usuários é protegida por criptografia. No SSE, uma chave é compartilhada entre os NFC-SEC *Users,* assim podem usá-la conforme a necessidade da aplicação. No SCH, um canal seguro é estabelecido entre os NFC-SEC *Users*, passando a ser, toda a comunicação entre as aplicações, criptografada com a chave derivada a partir da chave compartilhada com o serviço SSE.

Os serviços NFC-SEC seguem uma sequência de execução de quatro etapas, conforme ilustrado na figura 14. Na etapa ***Key agreement*** (acordo de chaves), uma chave secreta é estabelecida entre os dispositivos comunicantes *peer-to-peer* utilizando algoritmo criptográfico de chave pública definido no NFC-SEC. Na ***Key confirmation*** (confirmação de chaves), a chave secreta compartilhada é verificada entre os NFC-SEC *Users*. A fase chamada ***PDU security*** (protocolo de unidade de dados seguro) é executada apenas no *SCH service*, quando os dados a serem trocados entre os NFC-SEC *Users* são protegidos, provendo assim confidencialidade, integridade e autenticidade dos dados. E, por fim, a fase *Termination* (finalização), quando os serviços SSE ou SCH são finalizados, quando o dispositivo NFC for desligado, a comunicação for finalizada (*Released*) ou perder a prioridade na comunicação (*Deselect*). Neste momento as chaves utilizadas são destruídas.

Figura 14. Fluxo geral dos serviços NFC-SEC.



Fonte: ECMA-358.

2.2.2. Tipo de ataques

Vulnerabilidades em novas tecnologias de formas de pagamentos e no setor bancário são alvos de interesse de *hackers* e organizações criminosas. Assim um ataque bem sucedido pode comprometer a reputação de um banco e até levar a perda de confiança da tecnologia. Assim, é necessário que se conheça suas vulnerabilidades e riscos, bem como se busque soluções para sanar ou minimizá-los.

A seguir, são apontados alguns tipos de ataques que ameaçam a comunicação entre dispositivos NFC:

Escuta de dados –

Pelo fato do NFC se comunicar por ondas de radiofrequência, apesar do raio de ação de sua onda ser pequeno (cerca de 10 cm), o protocolo é suscetível à ataques de captura indevida do sinal transmitido. Com uma simples antena instalada próxima a um terminal leitor NFC é possível interceptar os dados que são trafegados entre os dispositivos. Apesar disto, um ataque assim é mais difícil ocorrer em comunicações de modo passivo do que em comunicações de modo ativo, isso porque o *target* utiliza a energia da onda eletromagnética recebida do *initiator*, diminuindo assim o alcance da onda retransmitida em reposta, sendo necessário que os dispositivos quase se toquem. Uma prevenção a este ataque seria estabelecer um canal seguro entre as partes comunicantes, através de autenticação mútua, utilizando-se chaves criptográficas assimétricas (RSA, Curva Eliptica, etc...) e/ou simétricas (TDES ou AES).

Corrupção de dados –

Ao invés de “escutar” os dados trafegados entre os dispositivos NFC, um atacante poderia corrompê-los, interferindo no sinal transmitido. Segundo Haselsteiner e Breitfuβ (2006), os dados transmitidos por radiofrequência podem ser corrompidos, se dados também forem transmitidos em frequências e em tempo exatos. Com isso há uma interferência no sinal, fazendo com que o dispositivo receptor NFC fique sempre tentando buscar algum sinal válido, sem conseguir. Impossibilitando, assim, a realização de uma transação de pagamento com o NFC, por exemplo. Este tipo de ataque é conhecido como ***Denial of Service***. Contudo,

este tipo de ataque pode ser detectado pelo emissor, pois ele pode checar o campo de RF ao mesmo tempo em que ele realiza transmissão de dados.

Modificação de dados –

A alteração de dados que são transmitidos entre os dispositivos NFC, diferentemente à corrupção de dados, é um ataque muito difícil de ser realizado, pois depende da força da amplitude de modulação (CURRAN; MILLAR; GARVEY; 2012). Isto porque a decodificação do sinal é diferente para modulações 100% e 10%. Assim, Halselsteiner e Breitfuβ (2006) concluem que a alteração na codificação Miller com 100% ASK é possível em apenas alguns bits, e na codificação Manchester com 10% ASK é possível em todos os bits.

Como já citado no item anterior, enquanto o dispositivo NFC está transmitindo sinal, ele pode também realizar uma leitura do campo de RF. Assim é possível que este ataque seja detectado e a comunicação seja interrompida. Outra solução ainda melhor seria a apresentada no item 2.2.1, ou seja, por meio do uso de criptografia tornar o meio de comunicação mais seguro.

Inserção de dados –

A inserção de dados é feita durante a troca de mensagens entre os dispositivos NFC. Isso apenas vai ocorrer se o dispositivo levar muito tempo para responder à requisição, pois o atacante poderia enviar dados antes do dispositivo responder. Mas a inserção apenas ocorrerá com sucesso se a transmissão do sinal ocorrer anteriormente, pois, se for transmitido ao mesmo tempo, ocorrerá uma sobreposição, e assim a corrupção dos dados. Para essa modalidade de ataque a solução também seria tornar o canal de transmissão de dados seguro.

Man-in-the-Middle –

Neste tipo de ataque a comunicação é interceptada por um atacante. Este pode retransmitir os dados, bloqueá-los ou alterar algumas informações para o destinatário, isso sem que destinatário ou o remetente perceba sua ação, imaginando que estão conversando diretamente entre si. Mas, este ataque é praticamente impossível de se aplicar em uma comunicação NFC, conforme descrença tanto de Halselsteiner e Breitfuβ (2006) como de Curran, Millar e Garvey

(2012), pelo fato da impossibilidade de se alinhar perfeitamente dois campos de RF e, se acaso isso ocorresse o ataque seria reconhecido pelo emissor e a comunicação interrompida.

Clonagem –

Segundo Kilås (2009), um *smart card* pode ser reproduzido com o conteúdo idêntico ao original, caracterizando a clonagem. Mas alguns modelos mais avançado possuem dispositivos que previnem a leitura de conteúdos sensíveis e secretos, como chaves criptográficas, por exemplo.

Phishing –

O *phishing* é a fraude eletrônica onde o atacante se faz passar por uma pessoa ou empresa, através do fornecimento de informações falsas (geralmente, links em e-mails) que induzem ao usuário pensar que são verdadeiros, com a finalidade de capturar dados pessoais como senhas, números de cartões de crédito e códigos verificadores, ou seja, quaisquer dados que possam ser usados para facilitar outros tipos de crimes.

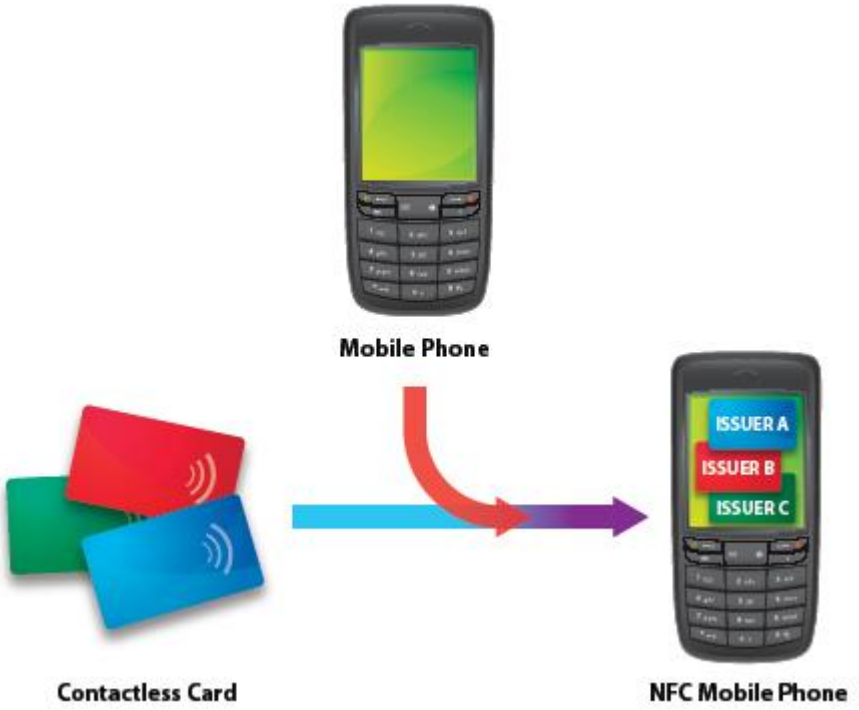
No NFC, Kilås (2009) aponta também o *phishing* como uma prática fraudulenta possível. Uma *tag* presente em um pôster de anuncio bancário, por exemplo, poderia ser substituído por outro contendo um link malicioso que direcione o usuário a um site idêntico ao verdadeiro, mas falso. Assim, quando o usuário digitar seus dados, como conta bancária e senha, por exemplo, estes são capturados, e após isso uma mensagem de erro comum pode ser apresentada ao usuário, e ele nem desconfiar o que acabou de ocorrer, imaginando que digitou a senha incorreta.

2.3. O NFC em pagamentos via dispositivos móveis

O *mobile payment*, ou *m-payment*, é uma nova forma de pagamento realizada através de um dispositivo celular NFC. Este serviço tem sido muito utilizado em diversos países europeus e no Japão (FAVORETTO, 2012), sendo utilizado em bilhetagem de transportes públicos, em entradas de estádios esportivos ou de eventos, estabelecimentos comerciais em geral, e muitos outros locais. Para

isso, combina-se à tecnologia dos celulares a tecnologia dos cartões *contactless* (figura 15). Assim, seus usuários se beneficiam de acessarem diversos serviços através de um único objeto, seu telefone celular.

Figura 15. Celular NFC usado no mobile payment.



Fonte: NFC-FORUM, 2008.

O *mobile payment* através do celular NFC também apresenta três características peculiares (NFC-FORUM, 2008):

- **Interatividade** – através das funções disponíveis no celular (teclado, tela sensível ao toque, sons, etc.) o usuário pode interagir com a transação, por exemplo, o usuário pode escolher a aplicação de uma determinada bandeira, dentre várias disponíveis, para realizar o pagamento de sua compra;
- **Gerenciamento Remoto de Multiplicação** – O gerenciamento de funções pode ser feito em tempo real remotamente. Sendo possível realizar download de aplicações, personalização e ativação/desativação de serviços no celular, bastando um termo assinado junto ao provedor do serviço (bancos, empresas

de recargas) para que o serviço seja disponibilizado imediatamente. Lançando, assim, o novo significado de "*anytime-anywhere*" ("a qualquer tempo e a qualquer lugar");

- **Gerenciamento Remoto de Usuário** – os provedores de serviços, com o consenso do usuário, podem recuperar registros de serviços utilizados e enviar a eles informações customizadas durante aquela transação ou em outras. Por exemplo, a apresentação de anúncios em compras futuras de produtos direcionados conforme o perfil de compra daquele consumidor.

Contudo, o celular NFC não é capaz de prover o *mobile payment* sozinho. Para isso, é necessário um sistema de servidores que se comunicam com o dispositivo NFC via rede móvel, para que seja possível prover aplicações de múltiplos serviços NFC remotamente. Toda esta estrutura forma o *NFC Mobile System* (sistema móvel NFC).

Figura 16. O sistema móvel NFC - canal de comunicação seguro.

Fonte: VANDERHOOF, 2012.

Conforme apresentado na figura 16, o sistema móvel NFC é composto por três entidades chave: o **provedor de serviço** (na figura, o *Issuance Institution*, que seria o banco, o emissor de serviço); o **TSM** – *Trusted Service Manager*; e o **MNO** – *Mobile Network Operators* (NFC-FORUM, 2008). Ainda são ilustrados o POS, que é a máquina da qual deve ser aproximado o celular NFC para o pagamento, localizada no estabelecimento comercial; a *Acceptance Institution*, que no caso de cartões de crédito é a empresa dona da bandeira do cartão (VISA, MasterCard, etc..) e o *Consumer's NFC Device*, que é o celular do usuário

O MNO é o responsável por manter a infraestrutura de rede móvel, por disponibilizar o serviço de conectividade de dados aos usuários, por autenticar o usuário para que possam se conectar à rede. O TSM provê um ponto de contato entre o servidor de serviço e o dispositivo NFC, sendo ele o responsável pelo gerenciamento remoto de multiplicação, apontado anteriormente neste capítulo. O papel do TSM é desenvolvido por empresas fabricantes de chips SIM, como a Gemalto e GD Burti (PAIVA, 2012).

Os padrões de comunicação utilizados entre as entidades do sistema móvel NFC, para garantir um canal de comunicação seguro para todo o sistema, também é descrita na figura 16. Entre o TSM, o *Issuance Institution*, e o *Acceptance Institution* o protocolo usado é o SSL/TLS ou a VPN. Entre o TSM, o MNO e o dispositivo do consumidor, o comunicação é feita segundo especificações do protocolo da GlobalPlataform ou também por SSL/TLS. Ainda entre o MNO e o dispositivo celular pode ser usado o formato de cifragem de dados via RAN - *Radio Access Network* (rede de acesso via rádio). Já, entre Dispositivo celular, o POS e a *Acceptance Institution*, são usadas as especificações da EMV e segurança dos protocolos NFC.

O protocolo de comunicação segura da GlobalPlataform[3] e as especificações EMV[4] não serão discutidos neste trabalho, pois não fazem parte de seu escopo, que busca o estudo do protocolo NFC e seu uso em pagamentos com dispositivos móveis.

[3] GlobalPlataform – organização independente e sem fim lucrativo que especifica uma infraestrutura padronizada para desenvolvimento, implantação e gerenciamento de *smart cards*.
[4] EMV – padrão desenvolvido pela Europay, MasterCard e Visa para inter-operação de cartões com chip, terminais POS e caixas eletrônicos, utilizado na autenticação de transações de cartões de crédito e débito.

3. O OpenNFC

Neste trabalho, um dos objetivos iniciais era o desenvolvimento de um sistema que utilizasse a infraestrutura NFC. Entretanto, houve uma grande dificuldade de se encontrar *tags* NFC e dispositivos que contivessem um chip controlador NFC embarcado ou algum dispositivo externo que desempenhasse esta funcionalidade. Assim, tendo em vista que pessoas podem passar pela mesma situação, apresentamos um emulador que pode ser o caminho para aqueles que buscam utilizar o auxilio da tecnologia NFC.

O OpenNFC (OPEN-NFC.ORG, 2013) é um conjunto de softwares criado pela Inside Secure© e implementa as funcionalidades do NFC emulando dois dispositivos NFC com suporte aos modos de operações: modo leitor, modo emulador de cartões e modo *peer-to-peer*. Suporta, também, a entrega de conexões como pareamento Bluetooth e Wi-Fi.

Com o OpenNFC são disponibilizadas API's para manipulação do hardware NFC, simplificando e acelerando assim o desenvolvimento de aplicativos com funcionalidades NFC. Havendo edições para WinCE 6.0 (compatível com o Windows™ Mobile 7), Linux 2.6, MeeGo e para plataforma Android.

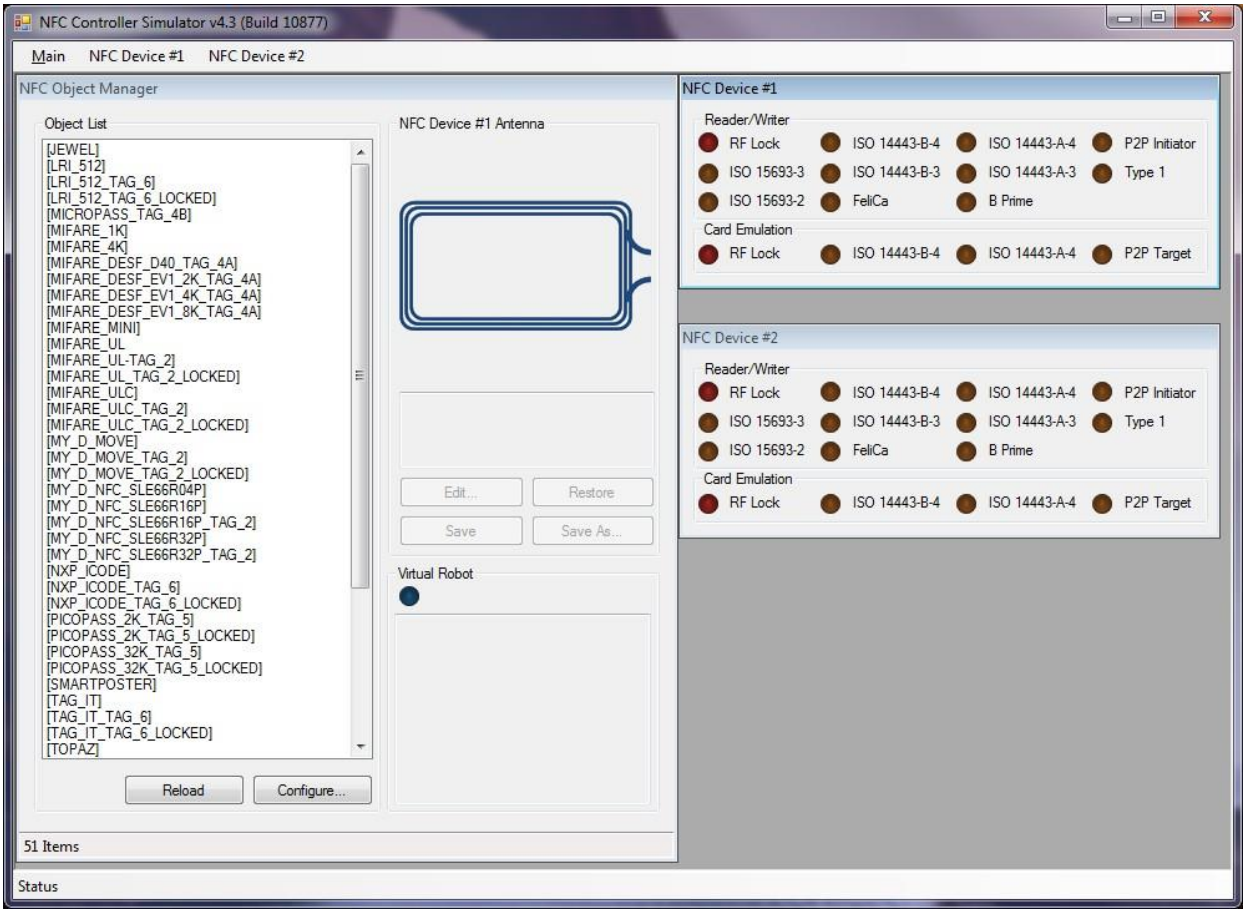
Os hardwares NFC desenvolvidos pela Inside Secure© são: o NFC Simulator, o MicroRead® e o SecuRead®. O MicroRead® é um chip controlador das funções NFC, e o SecuRead® se apresenta com um chip controlador NFC embarcado com um SE, eliminando assim a dependência da utilização de um UICC para o armazenamento seguro de informações. O NFC Simulator será o emulador de hardware NFC que será usado neste estudo da funcionalidade NFC com o OpenNFC.

O NFC Simulator (simulador NFC) é disponibilizado gratuitamente, com versão apenas para Win32 (Windows - 32 bits). Ele emula dois controladores NFC (#1 e #2) e um conjunto de cartões virtuais. Estes, bem como o segundo dispositivo NFC (#2), podem ser aproximados e removidos junto ao primeiro dispositivo (#1) virtualmente, simulando a ação real necessária para a comunicação NFC. Para sua instalação e execução, além de um computador com um bom processamento e um ambiente Win32, é necessário que o *.NET Framework runtime v.3.5* esteja instalado.

Contudo, ainda é preciso que o software *Connection Center*, disponibilizado com o pacote OpenNFC, também esteja sendo executado.

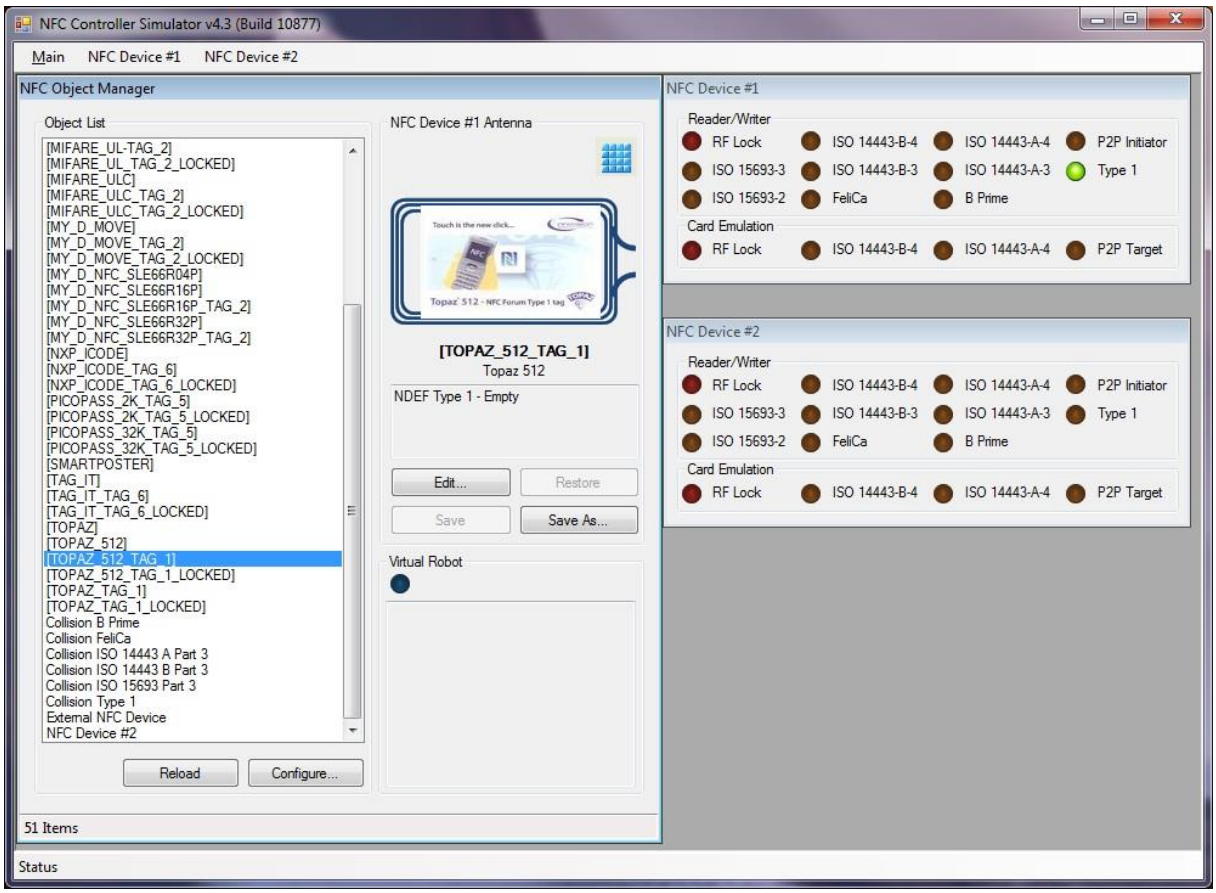
A figura 17 apresenta a tela inicial do simulador NFC, onde estão ilustrados três frames: *NFC Object Manager*, *NFC Device #1* e *NFC Device #2*. Os diferentes tipos suportados de cartões, *tags* e dispositivos NFC estão relacionados na lista de objetos disposta à esquerda da tela, e são emulados através de arquivos XML, que podem ser alterados e salvos. O conteúdo do arquivo XML representa os dados contidos no dispositivo.

Figura 17. Imagem da tela inicial do NFC Simulator.



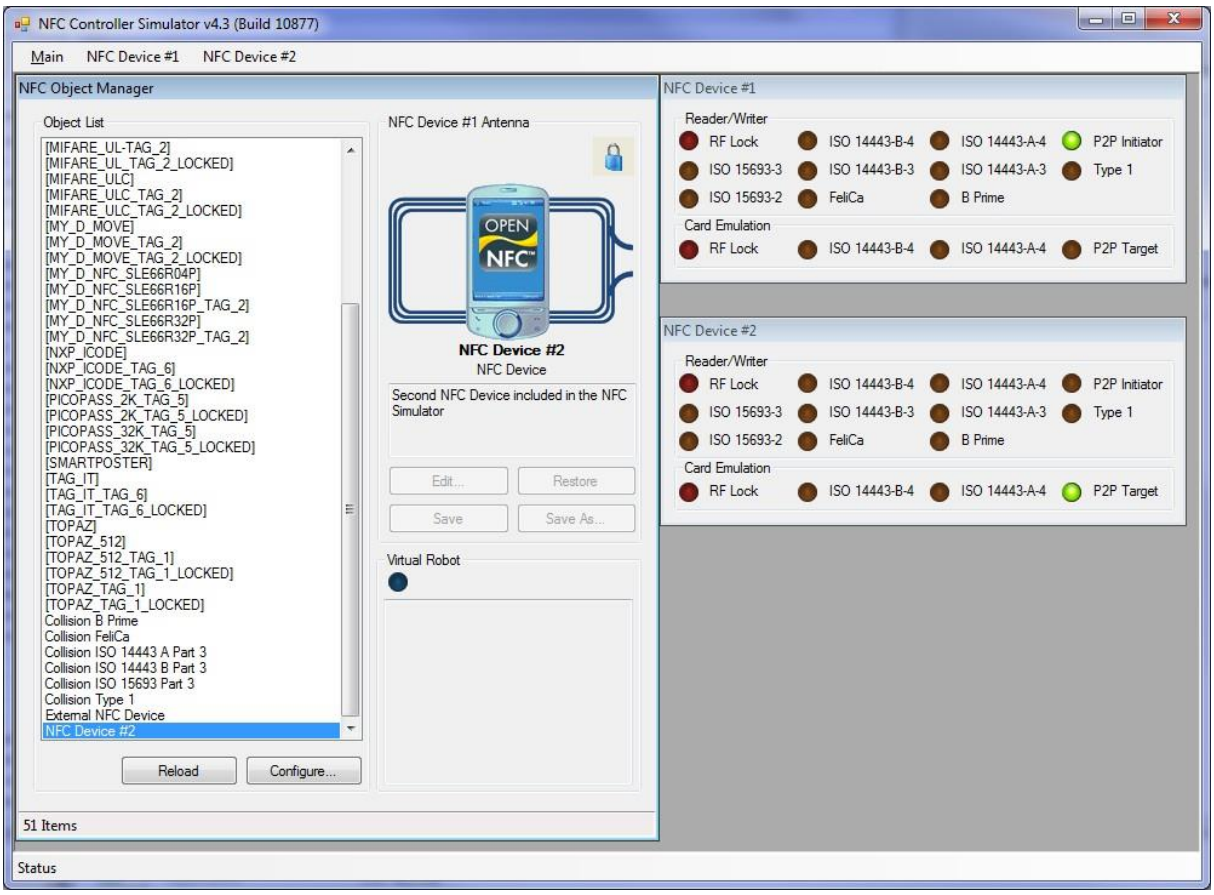
Fonte: OPEN-NFC.ORG, 2013.

Figura 18. Imagem da apresentação de cartão virtual – modo leitor de cartão.



Fonte: OPEN-NFC.ORG, 2013.

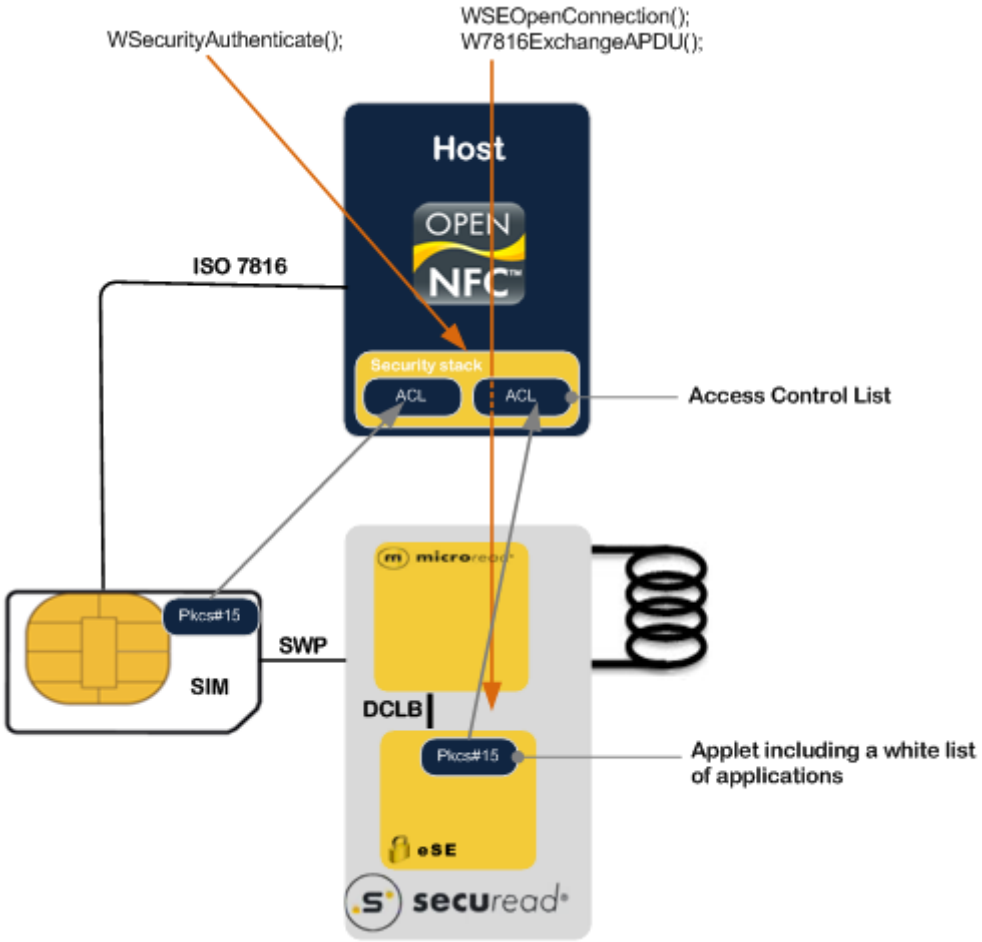
Figura 19. Imagem da apresentação de um segundo dispositivo NFC – modo peer-to-peer.



Fonte: OPEN-NFC.ORG, 2013.

Outra peculiaridade do OpenNFC é o gerenciamento do acesso ao *Security Element* - SE (o elemento seguro) no modo de operação em emulação de cartões. Esse gerenciamento é feito através da *Security Stack* (pilha de segurança) projetada para proteger o acesso das aplicações ao SE. Uma vez que um aplicativo mal intencionado (vírus, malwares, etc...) poderia enviar comandos ao SE repetidamente, com o intuito de provocar seu travamento e consequentemente uma falha de acesso as demais aplicações, um DoS – *Denial of Service*. Contudo, é importante ressaltar que a *Security Stack* apenas desempenha um gerenciamento de acesso ao SE, e não por si só garante a segurança deste.

Figura 20. Estrutura interna da Security Stack.



Fonte: OPEN-NFC.ORG, 2013.

Em uma solicitação de acesso a algum dado ou aplicativo armazenado na SE, a *Security Stack* busca no elemento seguro localizado um *applet* (miniaplicativos) PKCS#15[5] específico. Se este for localizado, seu conteúdo é verificado e utilizado. Caso não seja, a solicitação é rejeitada.

O OpenNFC, mais especificamente a Security Stack, mantém esquematicamente uma *white list* (lista de permissão), chamada ACL – Access Control List, com a relação de aplicações com acesso permitido a applets e emissão de comandos específicos no SE.

[5] PKCS#15 – estabelece um padrão que permite a usuários usar tokens criptográficos para identificar-se a aplicações críticas diversas (RSA LABORATORIES, 2013).

Com o intuito de facilitar o desenvolvimento e a portabilidade do OpenNFC, um módulo especial chamado NFC HAL - *Hardware Abstraction Layer* foi criado para comandar o dispositivo NFC especificado remotamente através de conexão TCP/IP. Esta conexão é gerenciada por uma ferramenta chamada **Connection Center**, disponibilizada com o OpenNFC para ambiente Win32. Assim, usando o OpenNFC com o *Connection Center NAL Module* (*Connection Center + NFC HAL Module*) ou com um dispositivos NFC real não há diferenças, isto é, o tipo de hardware utilizado é ignorado pela aplicação.

Quando o Connection Center é usado, a aplicação chama as API's do OpenNFC. Se um comando precisa ser enviado ao hardware NFC, o OpenNFC chama a interface do módulo NAL, que faz as intervenções necessárias (conversão de mensagens, por exemplo) e envia o comando resultante ao Connection Center via TCP/IP (o que significa que ele pode estar sendo executado em um dispositivo diferente). Este por sua vez direciona a mensagem para o dispositivo selecionado durante a inicialização, e faz o roteamento da reposta de retorno.

Portanto, uma estrutura de teste e apresentação da funcionalidade NFC pode ser montada dispondo de dois computadores (A e B) que se comunicam por TCP/IP. Na máquina A, deve ser instalado o emulador Android (*Android Reference Porting*), que já conterá a pilha OpenNFC e também o módulo Connection Center NAL. Na máquina B, instala-se o Connection Center e o NFC Simulator. De volta à máquina A, deve-se configurar o endereço IP da máquina B e ativar sua função NFC. Assim, a pilha OpenNFC na máquina A se conecta ao Connection Center que está sendo executado na máquina B, e este, por sua vez, inicializa a função NFC no NFC Simulator. Por fim, o simulador NFC pode então ser usado para apresentar tags ou outro dispositivo NFC ao aplicativo que está sendo executado no dispositivo com emulador Android (máquina A), simulando uma situação real.

Para dispositivos Android dotados com hardware NFC, basta que o módulo NAL seja substituído pelo endereço do local do chipset NFC real. Para as camadas superiores, inclusive a aplicação, não há mudança alguma.

CONCLUSÃO

O estudo sobre o NFC permitiu compreender que esta é uma tecnologia muito promissora e com aplicações múltiplas. Durante este estudo, percorremos os protocolos e produtos pertinentes e correlacionados ao assunto, explorando suas características, funcionalidades e peculiaridades. Com um embasamento teórico formado, partimos para o estudo do NFC. Foram apontadas suas aplicações mais conhecidas pelo mundo e seus modos de operações. Para aprofundar a pesquisa, foi estudado como o NFC opera seguindo a norma do padrão NFCIP-1.

No que ser refere à segurança, apesar do NFC ser relativamente seguro devido ao seu raio de comunicação ser bem curto, ele não provê proteção contra ataques do tipo *eavesdropping* ou modificação dos dados trafegados entre os dispositivos comunicantes. Fica a cargo do desenvolvedor a adoção de medidas de segurança na camada de aplicação como autenticação e troca de chaves entre aplicações dos terminais comunicantes para combater estes e outros tipos de ataque (VERMAAS, 2013). Para a comunicação no modo *peer-to-peer*, existe o protocolo de segurança NFC-SEC, na camada de transporte, que complementa o protocolo base NFCIP-1, do qual foi estudada sua estrutura interna e seu modo de funcionamento para tornar o canal de comunicação seguro. Mas para os modos de comunicação de emulador de cartão e de emulador de leitor não há protocolos especificados.

Ao dedicar um item de um capítulo ao estudo sobre o papel do NFC no *mobile payment*, pode-se concluir que entre as diversas tecnologias presentes no sistema, o NFC propicia a interface entre as duas entidades principais do sistema, o cliente e o estabelecimento comercial, atribuindo agilidade, conveniência e confiabilidade às transações de pagamento. Contudo, considerando-se a criticidade das transações comerciais, o NFC por si só não oferece segurança considerável ao sistema *mobile payment.* Sendo necessárias, assim, figuras importantes ao sistema como o TSM, responsável pelo gerenciamento da segurança (gerenciamento de chaves usadas para criptografia dos dados e atualização de *firmwares*), utilizada em todo o sistema.

Focando o mercado brasileiro, o uso do *mobile payment* é promissor, pois o país já conta com uma rede de POS (*point of sale*) *contactless* (figura 21) já

instaladas em diversos estabelecimentos comerciais, fornecidas por empresas administrados como a Cielo e a RedeCard, podendo ser usados em transações com cartões *contactless* bem como com dispositivos NFC, considerando-se que o *mobile payment* se baseia no NFC, e este, por sua vez, baseia-se no protocolo dos cartões *contactless.* O barateio de dispositivos com a tecnologia NFC embarcada é um fator que contribuiria para expansão do uso do celular como forma de pagamento. Outro fato importante é a normatização de sistemas de pagamento móvel pela MP 615/13 publicada pelo governo brasileiro em 20 de maio de 2013, cabendo ao Banco Central a regulamentação, onde cria-se margem para pagamentos móveis.

Figura 21. POS (maquineta) contactless.

Fonte: CONTACTLESS.INFO, 2013 e imagem elaborada pela autora deste trabalho.

Foi apresentado, também, o software OpenNFC, emulador NFC. Foi visto que com ele é possível que aplicativos com a funcionalidade NFC sejam desenvolvidos sem que seja necessária a utilização de dispositivos específicos com a função NFC, ainda de restrito acesso no Brasil.

Por isso, como trabalho futuro proponho que seja desenvolvido uma aplicação na área de *mobile payment*, e que seja feito uma pesquisa voltada para este assunto, focando os protocolos de comunicação da GlobalPlataform e o padrão EMV que garantem um canal seguro para o trafego de dados sensíveis e críticos para a segurança de todo o sistema. Proponho também que seja estudado mais a

fundo as função do TSM, detalhando seu funcionamento e até mesmo realizando um estudo de caso, por desempenhar um papel importante na segurança da estrutura do *mobile payment* como um todo.

REFERÊNCIAS

AGRAWAL, P.; BHURARIA, S. Near Field Communication: Collaboration beetween different stakeholders is of utmost importance to suceed in today's NFC-enabled world. SETLabs Briefings, v. 10, n. 1, 2012. Disponível em: <www.infosys.com/infosys-labs/publications/Documents/winning-it.pdf#page=69>. Acesso em: 04 mai 2012.

CARDWERK. ISO 7816. Disponível em: <www.cardwerk.com/smartcards/smartcard_standard_ISO7816-4_5_basic_organizations.aspx>. Acesso em: 09 mar 2013.

CONTACTLESS.INFO. Disponível em: <www.contactless.info/default.asp>. Acesso em: 02 jul 2013.

COSKUN, V.; OK, K.; OZDENIZCI, B. Near Field Communication (NFC): From Theory to Practice. 2 edição, 2012. Ed. Wisley. Disponível em: <books.google.com.br/books?id=-n3DZtCyFl8C&pg=PT406&lpg=PT406&dq=ECMA-385&source=bl&ots=AAjnG8sxtH&sig=hhc5T7N_sFMR2IIjme52_wCUAdU&hl=pt-BR&sa=X&ei=ucecUZntFKLz0gGbiYDQBg&ved=0CG4Q6AEwCQ>. Acesso em: 22 mai 2013.

CURRAN, K.; MILLAR, A.; MC GARVEY, C. Near Field Communication. Internetional Journal of Electrical and Computer Engineering, v. 2, n. 3, 2012. Disponível em: <www.iaesjournal.com/online/index.php/IJECE/article/view/234/pdf>. Acesso em: 04 mai 2012.

ECMA INTERNATIONAL. Standard ECMA-340, Near Field Communication Interface and Protocol (NFCIP-1). 2 edição, dez 2004. Disponível em: <http://www.ecma-international.org/publications/standards/Ecma-340.htm>. Acesso em: 18 jun 2012.

ECMA INTERNATIONAL. Standard ECMA-385, NFC-SEC: NFCIP-1 Security Services and Protocol. 2 edição, jun 2010. Disponível em: <http://www.ecma-international.org/publications/standards/Ecma-385.htm>. Acesso em: 21 mai 2013.

ECMA INTERNATIONAL. Standard ECMA-386, NFC-SEC-01: NFC-SEC Cryptography Standard using ECDH and AES. 2 edição, jun 2010. Disponível em: <http://www.ecma-international.org/publications/standards/Ecma-386.htm>. Acesso em: 21 mai 2013.

ECMA INTERNATIONAL. Near Field Communication – White Paper. 2004. Disponível em: <http://www.ecma-international.org/activities/Communications/2004tg19-001.pdf>. Acesso em: 11 julho 2012.

EMVCO. Specification. Disponível em: <www.emvco.com/specifications.aspx>. Acesso em: 02 mar 2013.

EXAME.COM. Número de brasileiros com celular cresce 107%, diz IBGE. Disponível em: <exame.abril.com.br/tecnologia/noticias/numero-de-brasileiros-com-celular-cresce-107-diz-ibge>. Acesso em: 21 mai 2013.

FAVORETTO JR, J. D. O que falta para o NFC decolar no Brasil. CPqD, jul 2012. Disponível em: <www.cpqd.com.br/imprensa-e-eventos/the-news/6411-o-que-falta-para-o-nfc-decolar-no-brasil.html>. Acesso em: 19 jun 2013.

FERRARI, J.; MACKINNON, R.; POH, S.; YATAWARA, L. Smart Card: A Case Study. International Technical Support Organization – IBM, 1 edição, out 1998. Disponível em: <http://www.redbooks.ibm.com/redbooks/pdfs/sg245239.pdf>. Acesso em: 27 fev 2013.

GLOBALPLATAFORM. GlobalPlatform's Proposition for NFC Mobile: Secure Element Management and Messaging, abr 2009. Disponível em: <www.paymentscardsandmobile.com/research/reports/GlobalPlatform_NFC_Mobile_White_Paper.pdf>. Acesso em: 17 mai 2013.

GSMA. Mobile NFC Infrastructure. V 1.0. Jul 2012. Disponível em: <www.gsma.com/mobilenfc/wp-content/uploads/2012/08/GSMA-Mobile-NFC-Infrastructure-v1-01.pdf > Acesso em: 15 abr 2013.

HASELSTEINER, E.; BREITFUβ, K. Security in Near Field Communication (NFC): Strength and Weaknesses. Philips Semiconductors, 6, Gratkorn, 2006. Disponível em: <http://ece.wpi.edu/~dchasaki/papers/Security%20in%20NFC.pdf>. Acesso em: 04 mai 2012.

HENDRY, M. Muti-Application Smart Cards. Jun 2007. Disponível em: <books.google.com.br/books?id=ieAkyyRnJrwC&printsec=frontcover&dq=Multi-application+Smart+Cards&hl=pt-BR&sa=X&ei=a-ksUcalHYLA8ATYj4GADQ&ved=0CDkQ6AEwAA#v=onepage&q=Multi-application%20Smart%20Cards&f=false>. Acesso em: 26 fev 2013.

ISO/IEC 14443-3. Identification cards — Contactless integrated circuit(s) cards — Proximity cards — Part 3: Initialization and anticollision. Disponível em: <www.waazaa.org/download/fcd-14443-3.pdf>. Acesso em: 13 mar 2013.

ISO/IEC 14443-4. Identification cards — Contactless integrated circuit(s) cards — Proximity cards — Part 4: Transmission protocol. Disponível em: <www.waazaa.org/download/fcd-14443-4.pdf>. Acesso em: 13 mar 2013.

KILÅS, M. Digital Signatures on NFC Tags. 2009. 53 f. Dissertação (Mestrado) Faculdade de Tecnologia da Informação e Comunicação da Suécia. Disponível em: <http://web.it.kth.se/~johanmon/theses/kilas.pdf>. Acesso em: 11 jul 2012.

LETGOMOBILE. Disponível em: <www.letsgomobile.org/en/5024/mobile-phone-payments/>. Acesso em: 02 jul 2013.

MIFARE.NET. Disponível em: <www.mifare.net/products/mifare-smartcard-ic-s>. Acesso em: 25 mar 2013.

MOBILEPEDIA. Disponível em: <www.mobilepedia.com.br/noticias/35-milhoes-de-celulares-com-nfc-serao-vendidos-esse-ano/attachment/celular-nfc>. Acesso em: 02 jul 2013.

MP 615/13. Medida Provisória nº 615. 17 mai 2013. Disponível em: <www.jusbrasil.com.br/legislacao/1034911/medida-provisoria-615-13>. Acesso em: 04 jun 2013.

NEARFIELDCOMMUNICATION.ORG. FeliCa Tecnology. Disponível em: <www.nearfieldcommunication.org/felica.html>. Acesso em: 27 mar 2013.

NFC FORUM. Disponível em: <www.nfc-forum.org>. Acesso em: 31 mar 2013.

NOKIA DEVELOPER. Differences among different NFC tags, 27 nov 2012. Disponível em: <www.developer.nokia.com/Community/Wiki/Differences_among_different_NFC_tags>. Acesso em: 17 mai 2013.

NXP – MIFARE smart cards IC's. Disponível em: <www.nxp.com/products/identification_and_security/smart_card_ics/mifare_smart_card_ics>. Acesso em: 20 mar 2013.

OPEN-NFC. Open NFC™ Developer Site. Disponível em: <open-nfc.org/wp/nfchal/simulator/features/>. Acesso em: 06 mai 2013.

PAIVA, F. M-payment à brasileira. Ed. #153 – ano 15 – abril/12. TELETIME. Disponível em: <www.teletime.com.br/4/2012/m-payment-a-brasileira/tt/281240/revista.aspx>. Acesso em: 01 jun 2013.

PHILIPS. As empresas Nokia, Philips e Sony estabeleceram o Fórum de Comunicação via Campo Próximo (Near Field Communication, ou NFC). Disponível em: <www.newscenter.philips.com/br_pt/standard/about/news/press/article-3017.wpd>. Acesso em: 04 abr 2013.

PRADO, E. Mobile Payment: Uma Guerra de Gigantes. **Convergência Digital**, fev 2012. Disponível em: <convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=29157&sid=15&tpl=printerview>. Acesso em: 24 jul 2012.

RANKL, W.; EFFING, W. Smart Card Handbook. John Wiley & Sons Ltd., Chichester, 1997. Disponível em: <books.google.com.br/books?id=C55-4kVUQ14C&pg=PT54&dq=history+of+smartcard&lr=&hl=pt-BR&source=gbs_toc_r&cad=4>. Acesso em: 02 mar 2013.

RFID JOURNAL. Disponível em: <www.rfidjournal.com>. Acesso em: 14 fev 2013.

RFIDBR. Disponível em: <www.rfidbr.com.br/index.php/leitora-reader.html>. Acesso em: 21 fev 2013.

ROBERTI, M. The History of RFID Technology. RFID Journal. Disponível em: <www.rfidjournal.com/article/view/1338/1/129>. Acesso em: 11 fev 2013.

RSA LABORATORIES. Disponível em: <www.rsa.com/rsalabs/node.asp?id=2141>. Acesso em: 21 mai 2013.

SAVI TECNOLOGY. Active and Passive RFID: Two Distinct, But Complementary, Technologies for Real-Time Supply Chain Visibility, A White Paper by Savi Tecnology, jan 2002. Disponível em: <logmgt.nkmu.edu.tw/news/articles /White%20Paper-Active%20and%20Passive%20RFID.pdf>. Acesso em: 14 fev 2013.

SHOWMETECH. Disponível em: <showmetech.com.br/guia-completo-sobre-nfc/blog-nfc-tag/>. Acesso em: 02 jul 2013.

SIMÕES, D. Sistema de Fidelização sobre NFC. 2008. 86 f. Dissertação (Mestrado) Universidade Técnica de Lisboa. 2008. Disponível em: <https://dspace.ist.utl.pt /bitstream/2295/232852/1/dissertacao.pdf>. Acesso em: 02 mar 2013.

SLASHGEAR. Disponível em: <www.slashgear.com/doubletwist-adds-airplay-support-and-doubletap-feature-for-nfc-enabled-devices-10151130/>. Acesso em: 02 jul 2013.

SONY GLOBAL. Felica Card User's Manual. Disponível em: <www.sony.net/Products/felica/business/tech-support/data/card_usersmanual_2.0 .pdf>. Acesso em: 25 mar 2013.

TECMUNDO. Onde e como a tecnologia NFC está sendo aplicada. Disponível em: <www.tecmundo.com.br/nfc/8173-onde-e-como-a-tecnologia-nfc-esta-sendo-aplicada.htm>. Acesso em: 17 abr 2013.

TELECO. Estatística de celulares no Brasil. 16/06/2013. Disponível em: <www.teleco.com.br/ncel.asp>. Acesso em: 24 jun 2013.

UFRJ. Disponível em: <www.gta.ufrj.br/grad/07_1/rfid/RFID_arquivos/Index.htm>. Acesso em: 11 fev 2013.

VANDERHOOF, R. Applying the NFC Secure Element in Mobile Identity Apps. Smart Card Alliance. 2012. RSACONFERENCE 2012. Disponível em: <365.rsaconference.com/servlet/JiveServlet/previewBody/3519-102-1-4620/>. Acesso em: 01 jun 2013.

VERMAAS, R. The Security Risck of Mobile Payment Applications Using Near-Field Communication. 2013. Dissertação (Mestrado). Erasmus University Rotterdam. 2013. Disponível em: <thesis.eur.nl/pub/13457/13457-Vermaas.pdf>. Acesso em: 01 jun 2013.

WIKIPEDIA. Disponível em: <pt.wikipedia.org/wiki/Cartão_inteligente>. Acesso em: 02 jul 2013.

WIZIACK, J. Governo prepara projeto para celular funcionar como cartão de banco. FOLHA.com, jul 2012. Disponível em: <www1.folha.uol.com.br/mercado/1118328-

governo-prepara-projeto-para-celular-funcionarcomo-cartao-de-banco.shtml>. Acesso em: 11 jul 2012.