PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
ESCOLA POLITÉCNICA
GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

ESTUDO DA APLICAÇÃO DA TECNOLOGIA NFC EM SISTEMAS DE PAGAMENTOS ELETRÔNICOS SEM CONTATO (*CONTACTLESS*)

THIAGO VIEIRA DI COIMBRA ROCHA

Goiânia
2022

THIAGO VIEIRA DI COIMBRA ROCHA

ESTUDO DA APLICAÇÃO DA TECNOLOGIA NFC EM SISTEMAS DE PAGAMENTOS ELETRÔNICOS SEM CONTATO (*CONTACTLESS*)

Trabalho de Conclusão de Curso apresentado à Escola Politécnica da Pontifícia Universidade Católica de Goiás, como parte dos requisitos para obtenção do título de Bacharel em Ciência da Computação.

Orientador:

Prof. Me. Rafael Leal Martins

Banca examinadora:

Prof.(a) Ma. Ludmilla Reis Pinheiro Dos Santos

Prof.(a) Ma. Angélica da Silva Nunes

Goiânia
2022

THIAGO VIEIRA DI COIMBRA ROCHA

ESTUDO DA APLICAÇÃO DA TECNOLOGIA NFC EM SISTEMAS DE PAGAMENTOS ELETRÔNICOS SEM CONTATO (*CONTACTLESS*)

Trabalho de Conclusão de Curso aprovado em sua forma final pela Escola Politécnica, da Pontifícia Universidade Católica de Goiás, para obtenção do título de Bacharel em Ciência da Computação, em _____/_____/_____

Orientador: Prof. Me. Rafael Leal Martins

Prof.(a) Ma. Ludmilla Reis Pinheiro Dos Santos
Coordenadora de Trabalho de Conclusão de Curso

Goiânia
2022

AGRADECIMENTOS

Ao Professor Rafael Leal Martins, orientador, por todo apoio, dedicação, colaboração e paciência.

A minha companheira Heloise Cardoso pelas conversas, inestimáveis sugestõ es, revisões de texto e por todo apoio.

RESUMO

A utilização de dispositivos móveis como meio de pagamentos está a crescer, tanto no Brasil quanto no mundo. Apesar de o uso das carteiras digitais ainda não ser amplamente empregada, seja pela falta de terminais que disponham da tecnologia NFC ou pelo simples fato de ainda haver uma certa resistência em seu uso pela população em geral, nota-se que gradativamente o uso desta forma de pagamento vem crescendo e que se trata de um meio seguro, prático e que tenta buscar reduzir os custos dos meios de pagamentos digitais. Este trabalho tem como objetivo apresentar informações a respeito das transações financeiras, com ênfase na utilização de *smartphones* como meio de pagamento e como a utilização de carteiras digitais tendem a ser um meio amplamente utilizado para pagamentos digitais. Objetiva-se ainda apresentar a tecnologia NFC, utilizada em pagamentos sem contato entre os dispositivos e expor o fluxo transacional desde o momento em que ocorre a captura pelo terminal utilizado pelo estabelecimento onde ocorre a aquisição de um bem ou serviço até o encerramento do processo na etapa de autenticação.

***Palavras-chave**: EMV, NFC, Carteira Digital, Pagamento Móvel, Pagamentos Digitais.*

ABSTRACT

The use of mobile devices as a means of payment is growing, both in Brazil and in the world. Although the use of digital wallets is still not widely used, either due to the lack of terminals that have NFC technology or the simple fact that there is still a certain resistance in its use by the general population, it is noticed that the use of this form is gradually payment method has been growing and that it is a safe, practical method that tries to reduce the costs of digital payment methods. This work aims to present information about financial transactions, with emphasis on the use of smartphones as a means of payment and how the use of digital wallets tends to be a widely used means for digital payments. The objective is also to present the NFC technology, used in contactless payments between the devices and to expose the transactional flow from the moment it is captured by the terminal used by the establishment where the acquisition of a good or service occurs until the end of the process in the authentication step.

***Keywords**: EMV, NFC, Digital Wallet, Mobile Payment, Digital Payments.*

LISTA DE FIGURAS

LISTA DE SIGLAS

ABECS	Associação Brasileira das Empresas de Cartões de Crédito e Serviços
APDU	*Application Protocol Data Unit*
ATM	*Automatic Teller Machine*
EFT	*Electronic Funds Transfer*
EMV	*Europay, MasterCard e Visa*
GHz	Giga Hertz
GSM	*Global System for Mobile Communications*
HCE	*Host Card Emulation*
IEC	*International Electrotechnical Commission*
IEEE	*Institute of Electrical and Electronics Engineers*
ISO	*International Organization for Standardization*
Kbits	Quilobits
MAC	*Message Authentication Code*
Mbit/s	Megabit por segundo
MHz	Mega Hertz
NDEF	*NFC Data Exchange Format*
NFC	*Near Field Comunication*
PAN	*Primary Account Number*
PIN	*Personal Identification Number*
POS	*Point of Sale*
QR Code	*Quick Response Code*
RFID	*Radio Frequence Identification*
SIM	*Subscriber Identity Module*
TSP	*Token Service Providers*
UICC	*The universal integrated circuit card*
UMTS	*Universal Mobile Telecommunication System*
URI	*Uniform Resource Identifier*
WIFI	*Wireless Fidelity*

SUMÁRIO

1 INTRODUÇÃO

A partir do século XXI, é dado início a era do dinheiro digital e da economia virtual, aonde não é necessário o uso de papel moeda e nem mesmo de um cartão em mãos para realizar a aquisição de bens ou serviços. Pode-se notar também o surgimento das carteiras digitais, que são aplicativos instalados em dispositivos móveis, como *smartphones*, relógios e pulseiras que substituem a utilização de dinheiro, cartões de débito ou crédito (PHAM; HO, 2015).

Conforme a tecnologia vem evoluindo é possível perceber a influência nos meios de pagamentos. Nota-se, na história do dinheiro, no surgimento da moeda, o desenvolvimento e implementação do papel-moeda, na criação e adoção do uso dos cartões de débito e crédito e mais recentemente, a partir de 2004 (AKANA; KE, 2020) no uso da tecnologia *Near Field Comunication* (NFC), que permite a troca de informação sem haver o contato físico entre os dispositivos, sendo esta tecnologia uma das alternativas mais utilizada, segundo a Associação Brasileira das Empresas de Cartões de Crédito e Serviços (Abecs) (2022, p.18), em pagamentos por aproximação, também conhecido pelo termo *contactless,* entre aparelhos e terminais *Point Of Sale* (POS).

Os pagamentos do tipo *contactless* estão se tornando cada vez mais comuns, à medida em que novos cartões de pagamento (também chamados de cartões “*tap and pay*”), *smartphones*, *tablets* e terminais POS são projetados para suportar a tecnologia NFC (Abecs, 2022).

Desde 2007, inovações vem ocorrendo em relação a ideias e implementações de carteiras digitas o que resultou na proliferação de modelos de carteiras, todas destinadas a melhorar a conveniência do consumidor, disponibilizar ofertas, alavancar dados, e reduzir o custo dos meios de pagamentos.

Outubro de 2014 marcou um momento seminal na história das carteiras digitais com o anúncio de Apple Pay. Ainda que o Google tenha anunciado a primeira carteira digital centrada em dispositivos móveis, a Google Wallet, em 2011, a indústria aguardava ansiosamente a versão de carteira digital da Apple.

1.1 Contextualização

O surgimento do cartão de crédito acontece em 1920, nos Estados Unidos, quando algumas empresas decidem criar meios para vender aos seus clientes no formato crédito. Em 1959 Frank McNamara teve a ideia de criar um cartão com sua identificação, para pagar sua conta após um tempo. Ele criou o Diners Club*,* usado inicialmente em poucos estabelecimentos e por um grupo restrito de pessoas. Com o tempo o uso do cartão foi ganhando mais adeptos e já era aceito por muitos locais. Inicialmente os cartões eram feitos de papel cartão e só no ano de 1955 surge o modelo de plástico. Em 1958 a empresa American Express*,* também nos Estados Unidos, lança seu cartão de crédito, em seguida, não muito tempo depois, o Bank of America, também dá início a seu cartão de crédito com o nome BankAmericard, tornando-se o precursor em todo os Estados Unidos, que mais tarde passou a se chamar Visa.

O Diners Club junto a American Express operava como responsável pelo pela cobrança e pagamento, essa operação é conhecida como *closed loop* (caminho fechado). Essas empresas possuíam contrato com os bancos emissores de cartões. Nesse modelo de transação financeira, o titular do cartão realizava a transação no estabelecimento, esse enviava os dados para o emissor, que aprovava a transação e envia os dados para o estabelecimento.

Em 1966 o Bank of America cria o primeiro cartão de crédito genérico, e a BankAmericard passa a ser utilizada em diversos bancos nos Estados Unidos. Na mesma época, outros bancos americanos se juntam para formam a Interbank Card Association.

Junto como essas novas empresas, um novo modelo financeiro é estabelecido, conhecido como *open loop* (caminho aberto) ou *four party*. Esse formato não precisa que o banco que emite o cartão seja o mesmo do usuário ou do estabelecimento comercia. As transações precisam ser processadas por um sistema centralizador, que efetua a transferência entre banco do estabelecimento, banco do usuário e banco do emissor. O titular faz o uso do cartão em determinado estabelecimento, e esse estabelecimento envia os dados do cartão em uso para o sistema do seu banco. O banco do estabelecimento envia a transação para a bandeira que valida o cartão, enviando a transação para o banco emissor validar a compra. Deste modo, o dono do cartão recebe um comprovante dessa transação e o banco do estabelecimento envia

essa transação para o estabelecimento, e a bandeira envia a aprovação para o banco do estabelecimento.

A ideia de comprar agora e pagar depois foi muito bem aceita. O cartão é muito popular, é um meio de pagamento quase indispensável. Essa forma imediata de crédito fornece inúmeras facilidades, como aquisição de produtos e serviços, flexibilidade de pagamento e saques emergenciais. Devido aos seus benefícios empresas tem se dedicado em criar propostas cada vez mais tentadoras para adesão de novos clientes. A instituição financeira emite um cartão com limite de crédito. O cliente por meio de um contrato de adesão se compromete a efetuar o pagamento das operações feitas entre o titular e credenciados. Esses cartões são feitos em instituições bancárias, mas diversos estabelecimentos, como lojas de departamento que fornecem aos seus clientes os *privates labels*, crédito para ser usado naquele estabelecimento.

Silva (2000, p. 63) afirma que “crédito, em sentido restrito e específico, como consistindo na entrega de um valor presente mediante uma promessa de pagamento”. Ou seja, uma venda feita no crédito se caracteriza pela entrega de um produto com pagamento que ocorre no futuro.

O cartão possibilita ao cliente um relacionamento de fidelização, com prazos, créditos e outros serviços financeiros. A modalidade de pagamento por crédito também é utiliza para automatizar financiamentos. Ele vem substituindo o pagamento à vista como um facilitador de transações. Nesse contexto é gerada uma política de crédito aplicada pelas instituições financeiras. Porém toda essa gama de benefícios pode levar as pessoas a não ter uma dimensão dos ricos financeiros, gerando dívidas e taxas de juros. Os cartões de crédito são emitidos com base no nível de renda do cliente, histórico do cliente O cliente deve pagar o seu ou suas dívidas durante o período de pagamento, caso contrário, os juros se acumularão.

Porém mesmo sendo um dos grandes responsáveis por estimular o consumo e impulsionar o desenvolvimento da economia, grande parte dos consumidores não conhece o funcionamento e os fatores que envolvem seus processos operacionais

1.2 Objetivo geral

O objetivo deste trabalho é realizar um estudo a respeito dos meios de pagamentos digitais utilizando a tecnologia NFC e apresentar as informações decorrentes do estudo sobre o funcionamento das transações financeiras através do uso da tecnologia NFC. É objetivo também deste trabalho apresentar algumas informações a respeito do funcionamento básico da tecnologia NFC e compreender o motivo pelo qual ela fora escolhida para a realização de transações financeiras sem a necessidade de contato entre dispositivos.

1.3 Objetivos específicos

Os objetivos específicos deste trabalho são:

- Descrever o funcionamento da tecnologia *wireless* NFC;
- Descrever o modelo de pagamento *Europay, MasterCard e Visa* (EMV), suas especificações e padrões para pagamentos;
- Apresentar com é possível a utilização da tecnologia NFC em pagamentos digitais utilizando os padrões EMV;

1.4 Justificativa

Acompanhando a evolução tecnológica, principalmente dos *smartphones*, várias alternativas para pagamento móvel vêm surgindo e sendo utilizadas. Assim, com a popularização de dispositivos móveis como, *tablets, smartwatches* e pulseiras. Nota-se o aumento em relação a quantidade dispositivos com tecnologia o suficiente capaz de oferecer o serviço de carteira digital. Boa parte, se não a maioria desses dispositivos permitem a utilização da tecnologia NFC o que permite a um dispositivo emular a funcionalidade de um cartão de crédito permitindo aos usuários desses dispositivos a aquisição de bens e serviços através de transações financeiras por meios digitais. Segundo um estudo realizado pela PWC Brasil, transações financeiras por meio digital devem crescer até 142% até 2030 (Rocha, 2022).

Diante do que fora exposto, a escolha do presente tema se deu em razão de haver a necessidade de disseminar o conhecimento da forma como os meios de

pagamentos vem evoluindo especialmente no que concerne ao uso de dispositivos móveis e cartões de crédito e débitos para realizarem pagamentos.

1.5 Metodologia

Para alcançar os objetivos apresentados neste trabalho foram necessários estudos em relação a tecnologia NFC, pagamentos digitais e os padrões de pagamentos EMV.

Foi utilizado como método de pesquisa bibliográfica o estado da arte na área em artigos científicos, livros e revistas associadas aos objetos de estudo. Durante o processo da pesquisa bibliográfica, é responsabilidade do autor se atentar quanto a qualidade das informações obtidas em suas pesquisas e a veracidade das mesmas, analisando possíveis contradições ou incoerências que elas possam apresentar (PRODANOV, 2013). Neste caso, o pesquisador assume o papel de avaliador e analista dos dados obtidos no decorrer do processo de sua pesquisa.

2 FUNDAMENTAÇÃO TEÓRICA

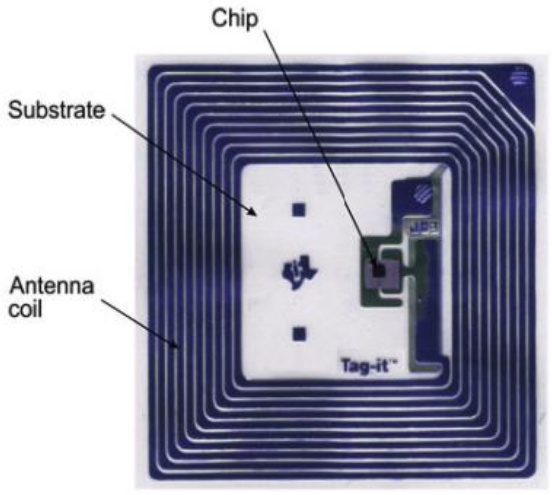
Este capítulo tem como propósito expor o estado da arte, como forma de mostrar o que já existe em relação a outros trabalhos realizados sobre o tema da pesquisa.

2.1 Tecnologia NFC

NFC é uma tecnologia de comunicação sem fio de curto alcance baseada em padrões aprovados e já utilizados por uma outra tecnologia chamada *Radio Frequence Identification* (RFID) e por *smart cards*. RFID, que fora introduzido na década de 1970, realiza identificação automática e transferência de dados via sinais de rádio eletromagnéticos normalmente por meio de um leitor ativo que está conectado a uma fonte de energia e uma etiqueta eletrônica passiva que é um transponder recebendo sua alimentação elétrica pelo leitor através de indução magnética.

Segundo (IGOE *et al.*, 2014), uma *tag* RFID, mostrada na Figura 1, é composta de uma antena, para receber e transmitir o sinal de rádio, e um circuito integrado para processar, armazenar a informação e para modular e demodular o sinal.

Figura 1 - Exemplo composição de uma *tag* RFID.



Fonte: (Mepits, 2014).

Em 2004 as empresas Nokia, Sony e *NXP Semiconductors* fundaram o *NFC Forum* (https://nfc-forum.org), uma associação sem fins lucrativos cuja organizações membros compartilham padrões de implementação, definem protocolos para interoperabilidade na troca de dados, aplicação e marketing para desenvolver as melhores soluções possíveis para o avanço do uso da tecnologia NFC.

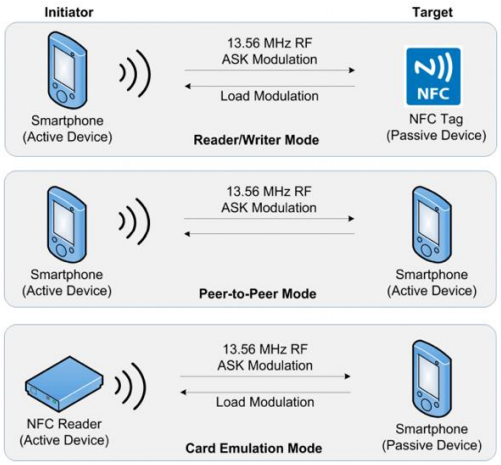
De acordo com (IGOE *et al.*, 2014), uma das maiores vantagens da NFC é o fato de a tecnologia ser compatível com a infraestrutura RFID já existente desde 1970, *tags* RFID e com os *smart cards contactless*. A tecnologia NFC foi construída tendo como base um subconjunto de padrões *International Organization for Standardization* (ISO) existentes, incluindo o padrão ISO/IEC 14443 que já é utilizado pela tecnologia RFID. O NFC opera na banda de radiofrequência de 13,56 Mega Hertz (MHz) com modulação *shift-keying* permitindo uma taxa de transferência de dados de até 424 Quilobits (Kbits) por segundo.

Em contraste com o convencional sistema RFID, na tecnologia NFC não há mais a distinção entre leitor e *transponder*. Um dispositivo compatível com NFC integra ambos os componentes, um *transponder* passivo e um leitor ativo permitindo assim não apenas ler e gravar dados de ou para uma *tag*, mas também receber e transmitir dados diretamente para outro dispositivo NFC. Segundo (Coskun, 2012), NFC suporta em geral três modos de operação, mostrado na Figura 2:

- Modo Leitura/Escrita: A capacidade do dispositivo NFC operar como um leitor ou escritor ativo. Assim que o dispositivo NFC se aproxima perto o bastante de uma tag RFID *transponder* passiva ou de um *smart card*, a energia é transferida a *tag* passiva via acoplamento magnético indutivo. Após a *tag* ter sido alimentada, uma comunicação *contactless* pode ser estabelecida. O dispositivo NFC é então capaz de não apenas ler as informações armazenadas na *tag*, mas também escrever/gravar dados na memória da *tag*;
- Modo *Peer-to-Peer:* Apenas pelo fato de se manter dois dispositivos NFC perto um do outro, esse modo permite facilmente a troca de dados entre esses dois dispositivos;
- Modo emulação de cartão*:* Neste modo o dispositivo NFC age como um *smart card* permitindo que outros dispositivos NFC possam ler os seus dados. Esse modo de operação é usado para pagamentos ou para prover controle de

acesso. O dispositivo NFC faz as vezes de um cartão de crédito ou um cartão de identificação permitindo assim a eliminação do objeto físico correspondente;

Figura 2 - Modos de interação e operação de dispositivos NFC

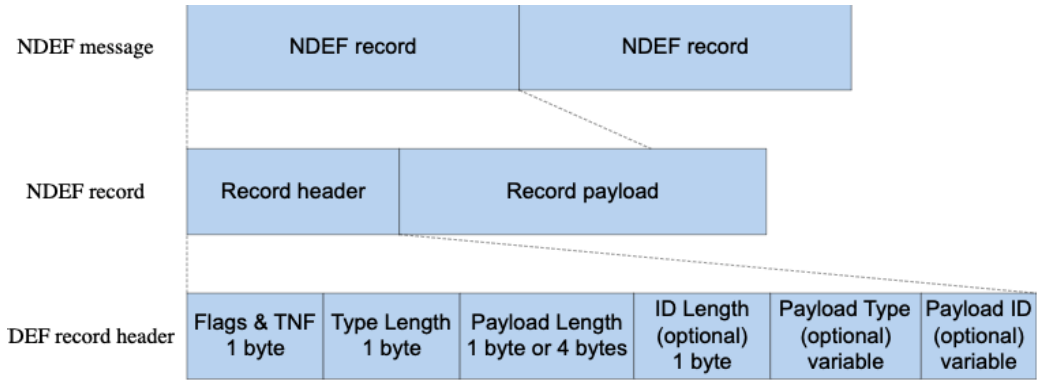


Fonte: COSKUN V.; OZDENIZCI B.; OK K (2015, p. 13352).

Independente do modo de operação (leitura/escrita, *peer to peer* ou emulação de cartão) a troca de dados entre dois dispositivos NFC utiliza um *NFC Data Exchange Format* (NDEF) que é um formato simples de mensagem binária definida pela norma ISO/IEC 18092, *Near Field Communication – Interface and Protocol* (NFCIP-1). Esta norma define uma interface de comunicação assim como um protocolo para interconexão sem fio de dispositivos acoplados operando a 13,56MHz. Este formato de mensagem é utilizado tanto na troca de dados entre dispositivos NFC quanto entre dispositivo NFC e uma *tag* NFC.

Uma mensagem NDEF é composta por um ou mais registros NDEF que encapsulam os dados do usuário da camada de aplicação. O registro NDEF é formado por um cabeçalho e por um *payload* que armazena os dados do usuário, conforme a Figura 3.

Figura 3 - Estrutura de uma mensagem NDEF



Fonte: (Nordic. 2018).

O cabeçalho de um registro NDEF é composto pelos campos:

- *Flags and TNF*: O campo Flags e TNF, mostrado na Figura 4, contém os flags:
  - ***MB*** *(Message Begin) e* ***ME*** *(Message End):* Especifica a posição do registro NDEF dentro da mensagem. O *flag* **MB** é definido para o primeiro registro na mensagem. Da mesma forma, o sinalizador **ME** é definido para o último registro da mensagem. Se em uma mensagem houver apenas um registro, ambos os *flags* serão definidos;
  - ***CF*** *(Chunk Flag):* Usado para *payloads* particionados (um *payload* que é particionada em vários registros). Definido em todas as partições do registro, exceto na última;
  - **SR** (*Short Record*): Usado para determinar o tamanho do campo que armazena o valor responsável por definir o tamanho do *payload*. Se este *flag* estiver definido, o campo ***Payload Lenght*** ocupa 1 byte; caso contrário, ele tem o tamanho de 4 bytes;
  - **IL** (*ID Length present*): Indica se um campo ***ID Length*** existe no cabeçalho. Se este *flag* estiver definido, significa que o campo ***ID Length*** existe no cabeçalho;
  - **TNF** (*Type Name Format*): Especifica a estrutura do campo ***Payload Type*** e como interpretá-lo;
- *Type Length*: Especifica o tamanho do campo (***Payload Type***) responsável por armazenar o tipo do *payload*. É um campo obrigatório no cabeçalho, mas seu valor pode ser zero;

- *Payload Length*: Especifica o tamanho do *payload*. Pode ter tamanho de1 byte ou 4 bytes, a depender do flag **SR**. É um campo obrigatório no cabeçalho, mas seu valor pode ser zero;
- *ID Length*: Se torna um campo obrigatório no cabeçalho se o flag **IL** estiver sido definido. Especifica o tamanho do campo ***Payload ID***;
- *Payload Type*: Se torna um campo obrigatório no cabeçalho se o campo ***Type Length*** contiver um valor maior do que zero. Especifica o tipo de *payload* do registro NDEF;
- *Payload ID*: Se torna um campo obrigatório no cabeçalho se o flag **IL** estiver sido definido e se o campo ***ID Length*** conter um valor maior do que zero. Especifica o ID do *payload* do registro NDEF;

Figura 4 - Estrutura do campo *Flags and TNF*

Fonte: (Nordic. 2018).

O campo do cabeçalho de maior notoriedade é o *Payload Type* que descreve o tipo e o formato dos dados do registro podendo ser um tipo de mídia *MIME*, descrevendo uma composição de, por exemplo, imagens, conteúdo textual e quaisquer outros tipos de informações ou um dos tipos de registros predefinidos, *NFC record type definitions* (RTD). Em contraste com os tipos de mídia MIME, as últimas especificações (NFCForum, 2006) do NDEF definem não apenas a estrutura de dados, mas também a forma como os dados devem ser eventualmente processados e apresentado no receptor do dispositivo NFC de saída. Alguns tipos de RTD:

- *Text Record Type*: permite encapsular informações textuais sobre o esquema de codificação dos caracteres e o idioma do texto;
- *Signature Record Type*: oferece um mecanismo de segurança fornecendo a possibilidade de através de um certificado, assinar digitalmente todo um NDEF. O *software* que recebe a mensagem NDEF assinada pode verificar sua autenticidade e integridade juntamente a Autoridade Certificadora

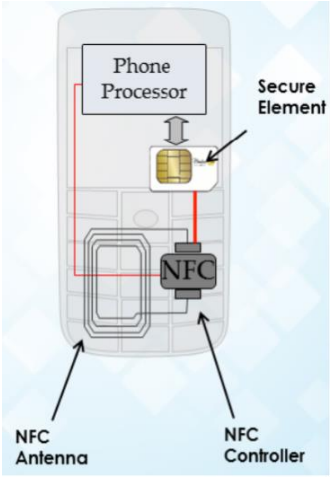
responsável pela emissão do certificado digital utilizado na assinatura da mensagem NDEF;

- *URI Record Type*: pode conter uma *Uniform Resource Identifier* (URI), por exemplo um endereço de um site ou um endereço de *e-mail*. O *software* que recebe este registro NFC pode, por exemplo, ser programado para processar automaticamente essas informações para um navegador *web* ou um *software* de *e-mail*;

Conforme (Want, 2011), quando há a necessidade de transferência de grande quantidade de dados a uma grande distância ou em alta velocidade entre o emissor e o receptor dos dados, a capacidade ordinária da tecnologia NFC de transferência de dados pode não ser o suficiente para atender tais requisitos. Em teoria, a tecnologia NFC também fornece um mecanismo para transferir o fluxo da conexão e transferência dos dados para outra tecnologia sem fio com taxas de transferências mais altas como *Wireless Fidelity* (WIFI) ou *Bluetooth*. Essa troca de contexto de estabelecimento de comunicação e transferência de dados envolvendo outras tecnologias sem fio envolve um grande esforço de configuração. Neste caso, o simples princípio de tocar e conectar, empregado pelo NFC, é utilizado apenas para trocar os parâmetros de configuração necessários para o estabelecimento da conexão entre o emissor e o receptor. Essa troca de parâmetros deve seguir a especificação técnica fornecida pelo *NFC Forum* para que seja possível ativar um novo canal de comunicação, entre o emissor e o receptor, permitindo assim uma assertiva transferência de contexto de comunicação.

De acordo com (Sabella, 2016), para que seja possível um *smartphone* utilizar a tecnologia NFC quatro componentes básicos de *hardware* são necessários: um controlador de *host* (*phone processor*), um controlador NFC, uma antena NFC e um elemento de segurança responsável por prover um ambiente de execução seguro, ilustrados na Figura 5.

Figura 5 - Anatomia dos componentes NFC em um *smartphone*



Fonte: SABELLA, MUELLER (2016, p. 30).

O controlador de *host* atua como a espinha dorsal de todos os *smartphones*, sendo necessário não apenas para executar o sistema operacional do aparelho, mas também para gerenciar a interface com o usuário, o modem *Global System for Mobile Communications* (GSM)/*Universal Mobile Telecommunication System* (UMTS) e atua também como um ambiente de execução de aplicativos. É a base para outros componentes NFC no sistema do *smartphone* tendo, portanto, um papel essencial para integrar a funcionalidade NFC ao *smartphone*.

A Antena NFC é necessária para receber e transmitir sinais de rádio adequados. O controlador NFC prove suporte aos três modos de operação, modula, demodula e processa os sinais, de acordo com as especificações NFC.

A arquitetura NFC fornece um elemento seguro, *Secure Element*, que serve como um ambiente de execução confiável. Pelo fato de muitas vezes lidar com dados críticos e sensíveis, muitos sistemas NFC, portanto, precisam de um ambiente seguro para persistir dados e executar aplicações estando protegido de uso indevido e manipulação de dados.

O elemento responsável por prover esse ambiente seguro pode ser integrado ao *smartphone* de diversas maneiras. Pode ser um chip dedicado sendo parte integrante do hardware do smartphone ou poderia ser um chip em formato de cartão sendo possível sua troca e/ou remoção. Uma outra forma, talvez, mais razoável, de se ter um elemento que possa prover esse ambiente seguro, seria a utilização de um cartão do tipo *The universal integrated circuit card* (UICC). Este cartão já é fornecido pelas operadoras de rede de telefonia móvel para seus clientes, e não é de utilização

exclusiva do módulo *Subscriber Identity Module* (SIM), mas também pode ser utilizado como uma plataforma multifuncional segura, podendo inclusive prover um módulo de segurança para várias aplicações.

2.2 Comparação NFC com outras tecnologias sem fio

Existem outras tecnologias que permitem comunicação sem fio e fornecem recursos semelhantes aos apresentados nas tecnologias RFID e NFC.

Uma tecnologia que também pode ser integrada a smartphones e opera a curto alcance é o *Bluetooth* (IEEE Standard 802.15.1-2002). Operando em uma faixa de frequência mais alta, 2.4 Giga Hertz (GHz), consegue permitir taxas de transferência mais altas, podendo chegar até 2 Megabit por segundo (Mbit/s) o que o torna uma opção mais eficaz quando se trata de transferência de grandes quantidades de dados. Outra característica do *Bluetooth*, e o que torna de certa forma menos seguro do que o NFC, é a grande área de cobertura do seu sinal, entre 10 e 100 metros, em relação a área de cobertura do sinal do NFC, o que acaba facilitando a interceptação do sinal por terceiros e permitindo um possível roubo de dados.

Um ponto que difere o *Bluetooth* do NFC consiste na forma como a conexão entre os dispositivos é estabelecida, enquanto no NFC em questão de frações de segundos a conexão entre os dispositivos é estabelecida no *Bluetooth* outras definições de configuração são necessárias, muitas vezes há também necessidade da interação com o usuário ou o emparelhamento dos dispositivos.

Outra tecnologia utilizada para comunicação sem fio é o Wi-Fi (IEEE 802.11). Opera nas frequências 2,4 GHz e/ou 5,0 GHz, mas com maior potência, permite taxas de transferências de dados ainda mais altas, podendo chegar a 600 Mbits/s a depender do padrão utilizado na família IEEE 802.11, e com alcance de até 100 metros. *Bluetooth* e Wi-Fi não se comunicam com dispositivos passivos que não possuem uma fonte de alimentação de energia elétrica, como as *tags* passivas, o que é possível com o NFC.

Com propriedades similares com as das *tags* NFC existe ainda o *Quick Response Code (QR Code)* (ISO/IEC 18004:2006), ilustrado na Figura 6. É um código de barras óptico de duas dimensões, codificado em padrão preto e branco com a capacidade de armazenar vários tipos de dados ou até centenas de milhares de caracteres, sendo esse limite definido pelo tamanho da *tag* e do nível de correção de

erros. Podem ser impressos em diferentes tipos de superfícies, muito comum de ser encontrado em embalagens de produtos e anúncios em cartazes.

Figura 6 - Exemplo *QR Code*

Fonte: (USP, 2018).

Para que o conteúdo de uma *tag QR Code* seja lido é necessário o uso do sensor de uma câmera. Em contraste com as *tags* NFC, as *tags QR* podem ter a leitura de seu conteúdo comprometida, devido ao fato de o processo de leitura sofrer interferência direta da luminosidade e a posição do leitor. *Tags QR Code* são mais baratas do que *tags* NFC, mas o processo de leitura de uma *tag QR Code*, utilizando a câmera de um *smartphone*, é mais demorado e demanda mais processamento do que a leitura de uma *tag* NFC.

Em certos casos, pode-se observar que o uso da tecnologia NFC realmente traz mais benefícios em detrimento ao uso de outras tecnologias, mas também nota-se que essas tecnologias podem além de coexistirem em um mesmo dispositivo, podem se complementar muito bem como alternativas de comunicação sem fio.

2.3 Sistema de Pagamento EMV

Antes da implementação do uso de cartões inteligentes com chip, os cartões com tarja magnética eram usados para as transações de débito/crédito, onde os dados sobre a conta são lidos e registrados para em seguida ser solicitado ao portador do cartão uma assinatura para autenticação.

Após o cartão ser passado no terminal, um recibo é impresso uma vez que os detalhes da conta são verificados pelo sistema, e o cliente tinha que assinar o recibo

e devolvê-lo ao vendedor/atendente. Em seguida, o vendedor deveria verificar a assinatura no recibo e se correspondia à assinatura no verso do cartão para autorizar a transação (EMVCo, 2011). Entretanto, esse sistema possui certas falhas de segurança, como a possibilidade de que o cartão possa ser roubado e que a assinatura poderia ser falsificada para realizar as transações.

Com o avanço da tecnologia, havia equipamentos disponíveis no mercado negro aonde os dados podiam ser lidos e gravados nas tarjas magnéticas, facilitando a clonagem dos cartões originais e seu uso sem o conhecimento do titular do cartão (EMVCo, 2011). Com todos esses cenários possíveis de fraude foi introduzido o EMV que poderia lidar com tais questões e fornecer segurança para as transações com cartão.

EMV foi lançado em 1994 como um padrão para trazer mais segurança na utilização de cartões como meio de pagamento. O EMV usa cartões inteligentes com circuitos integrados que guardam as informações do leitor de cartões. Esta implementação, inclusive, necessita de dispositivos de hardware específicos que aceitam os cartões EMV para realizar as transações. Este foi um grande passo, pois a um custo dispendioso, todo o sistema de pagamento utilizando cartões fora atualizado. A intenção dessa troca de tecnologia tinha como foco três áreas principais: Redução de Fraude, Redução de Custos de Telecomunicações e Gestão de Risco de Crédito.

Segundo (EMVCo, 2014), EMV é um padrão global e uma tecnologia de pagamento para processamento seguro de pagamentos usando cartões inteligentes/chip, mostrado na Figura 7. O aplicativo de pagamento do usuário está embarcado em um chip, que contém um microprocessador, que pode armazenar de forma segura, informações sigilosas e realizar processamento criptográfico.

Figura 7 - Exemplo de um cartão com *chip*/circuito integrado

Fonte: (“Mastercard EMV Chip Technology | EMV Chip Card Solutions for Issuers”, [s.d.]).

Com o propósito de garantir a interoperabilidade mundial e mitigar o risco de fraudes, foram estabelecidas as especificações EMV que descrevem o comportamento dos terminais e os protocolos de comunicação entre os terminais e o ICC (*Integraded Circuit Card*) embutido no cartão. As especificações EMV são mantidas pela EMVCo para as tecnologias: *EMV Contact*, *EMV Contactless*, *EMV Tokenization*, *EMV Card Personalization Specification* etc. A primeira versão das especificações foi publicada em 1996 e conhecido como EMV'96. Em seguida veio a versão EMV v3.1.1 publicada em 1998, EMV v4.0 (também conhecido como EMV2000) publicado em 2000, EMV v4.1 publicado em 2004, EMV v4.2 publicada em 2008 e a versão mais recente v4.3 publicada em 2011.

Há uma diferença fundamental entre uma transação feita por um cartão que utiliza tarja magnética e uma transação feita por um cartão que utiliza um chip EMV. Para tarja magnética, o cartão é simplesmente um dispositivo de armazenamento de dados que é lido pelo terminal, não havendo a necessidade do uso do cartão até o fim do fluxo transacional. O terminal realiza todo processamento e aplica as regras de pagamento (EMVCo, 2014). O armazenamento inalterado de dados, portanto, tornam os cartões de tarja magnética mais vulneráveis a fraudes possibilitando a que quem quer que tenha acesso a esses dados também consiga acessar as informações confidenciais do titular do cartão necessárias para realizar transações de tarja magnética.

As transações com cartão através do uso de chip contêm dezenas de informações a serem intercambiadas entre o cartão, o terminal e a instituição adquirente da transação. Isso é possível, pois o terminal realiza o processamento dos

dados do cartão e autenticação criptográfica antes que uma transação seja concluída com sucesso. O uso da tecnologia EMV não impede que as violações e roubo de dados ocorra, mas torna muito mais difícil para os fraudadores terem acesso aos dados.

A implementação da tecnologia EMV encontrou vários desafios incluindo; alto custo envolvido na atualização da infraestrutura de pagamento, como a rede ATM (*Automatic Teller Machine*), rede de pontos de venda e *switch EFT* (*Electronic Funds Transfer*) bancário. Há também altos custos de aquisição dos cartões integrados com chip, personalização do cartão de pagamento e realizar a conscientização dos usuários sobre a necessidade de mudança (VIJAYAN, 2014).

As transações EMV basicamente se dividem em dois tipos, contato(*contact*) e sem contato(*contactless*). O que define o tipo de transação é a forma como o chip entra em contato com o terminal. Na transação do tipo *contact* o chip do cartão deve entrar em contato físico com o leitor de chip do terminal POS para que seja feita a leitura dos dados do cartão do cliente, conforme ilustrado na Figura 8. Na transação EMV do tipo *contactless* o usuário deve tocar o cartão no terminal POS ou apenas aproximar o cartão a uma distância de no máximo 10 cm do terminal, permitindo assim que o terminal forneça energia ao cartão através do uso da tecnologia NFC, e os dados do cartão possam ser lidos pelo terminal, conforme ilustrado na Figura 9.

Figura 8 - Exemplo de transação com contato (*contact*)

Fonte: (BDO Unibank, 2020).

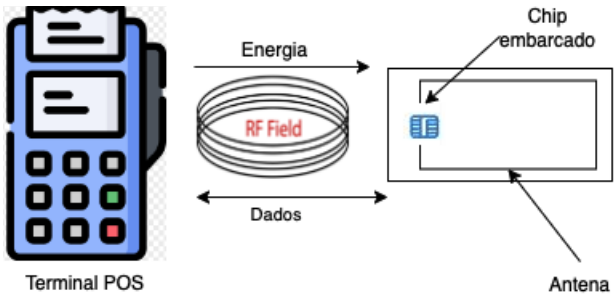
Figura 9 - Exemplo de transação sem contato (*contactless*)

Fonte: (BDO Unibank, 2020).

Por padrão, um cartão que permite realizar transações *contactless* inclui um chip NFC e uma antena incorporados durante a fabricação do cartão. Este chip foi projetado para ser compatível com o padrão ISO/IEC 14443 (ISO/IEC 14443-4, 2018) que define os circuitos integrado para cartões usados para identificação e o padrão ISO/IEC 7816 (ISO/IEC 7816-4, 2013) usado na especificação dos protocolos de transmissão para comunicação entre cartões *contactless* e seus *hosts*.

Conforme ilustrado na Figura 10, todos os cartões de pagamento *contactless* são alimentados com energia elétrica através de um campo magnético gerado por um leitor de cartão compatível com NFC ou terminal POS localizado a uma distância de até 10 cm.

Figura 10 - Arquitetura cartão *contacless*



Fonte: Figura adaptada do: (ALESS et al, 2016) com conteúdo desenvolvido pelo autor deste trabalho.

Para evitar que haja o furto de dados o chip NFC, embutido nos cartões *contactless*, protege os dados contra decriptação e permite apenas a leitura seletiva dos dados armazenados em sua memória (ISO/IEC 7816-4, 2013). Além disso, cada

chip NFC é projetado para autenticar os dados da transação usando um MAC (*Message Authentication Code*) que é calculado com a chave simétrica embutida no cartão *contactless* e o banco emissor do cartão. Os mecanismos de segurança e recursos de proteção de dados usados em cada cartão de pagamento *contactless* são especificados pelas diferentes redes emissoras de cartões, como Pay Wave da VISA, ExpressPay da American Express e PayPass da Mastercard, entre outros.

As carteiras digitais (também conhecidas como *e-wallet)* habilitadas para NFC permitem que os usuários façam pagamentos por transações emulando a funcionalidade de um cartão de pagamento *contactless*. Assim como os cartões de pagamento *contactless*, as carteiras digitais também seguem as normas ISO/IEC 14443 (ISO/IEC 14443-4, 2018) e ISO/IEC 7816 (ISO/IEC 7816-4, 2013). Enquanto o padrão ISO/IEC 14443 define como o chip NFC deve ser incorporado a um cartão *contactless*, também definem como os *smartphones* ou terminas POS processam os parâmetros necessários para transmissão de dados, o padrão ISO/IEC 7816 define a estrutura da APDU (*Application Protocol Data Unit*) que é usada pelo chip NFC para comunicação com outros chips NFC no perímetro próximo. As três carteiras digitais habilitadas para NFC mais populares no mercado hoje são Apple Pay, Android Pay e Samsung Pay.

Para que seja possível realizar pagamentos utilizando essas carteiras digitais, os usuários devem primeiro registrar os dados de seu cartão de pagamento *contactless* na carteira. Após a aprovação do registro dos dados do cartão na carteira digital pelo banco emissor do cartão, o usuário poderá, então, realizar pagamentos aproximando seu *smartphone* em qualquer terminal POS que possua a tecnologia *contactless*, assim como faria com um cartão de pagamento *contactless*. O terminal POS, em seguida, prossegue para iniciar e processar a transação comunicando-se com o processador de pagamento (ou adquirente), a rede emissora do cartão, bem como o banco emissor, respectivamente.

2.3.1 Infraestrutura de pagamentos do método contactless

De acordo com (SVIGALS, 2014), devido a uma aceitação massiva dos consumidores pela utilização de cartões que possuem chip e se utilizam da autenticação PIN (*Personal Identification Number*), os bancos e as redes emissoras de cartões têm aproveitado a infraestrutura já existente, para essa forma de

pagamento, como base para a implantação de pagamentos via débito e crédito com cartões *contactless*. Com isso, vem ocorrendo uma queda vertiginosa no uso da tecnologia de tarja magnética em cartões de crédito e débito.

Baseado nas normas ISO/IEC 14443 (ISO/IEC 14443-4, 2018) e ISO/IEC 7816 (ISO/IEC 7816-4, 2013) as Especificações *EMV Contactless Specifications for Payment Systems* definem os padrões mais proeminente para transações de pagamento *contactless*. São gerenciadas pelo consórcio EMVCo, todos os membros deste consórcio usam um símbolo comum para identificar a aceitação de pagamento *contactless* baseado nas diretrizes estipuladas na norma ISO/IEC 14443 (ISO/IEC 14443-4, 2018) para indicar aceitação de pagamentos *contactless* em terminais POS globalmente.

2.3.2 Tokenização

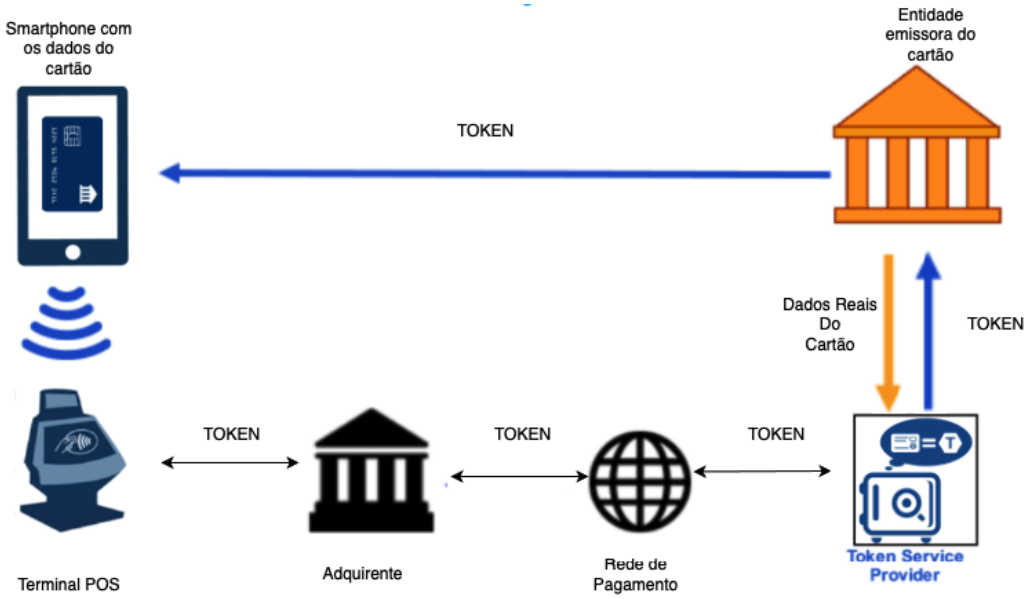
Tokenização é o processo no qual o número do cartão de crédito ou de débito, do inglês PAN *(Primary Account Number*), é substituído por um número gerado aleatoriamente com a mesma quantidade de dígitos do número original do cartão. Esse número gerado aleatoriamente é referido como o token de pagamento ou PAN temporário e é armazenado em um servidor centralizado e altamente seguro conhecido como cofre de *tokens*. Na Figura 11, é ilustrado como os *tokens* de pagamentos são gerados dentro da infraestrutura de pagamentos *contactless*.

A especificação *EMV - Payment Tokenisation Specification* (EMVCo, 2020) fornece as estruturas e diretrizes para garantir que as instituições que possuem certificações para atuarem como TSPs (*Token Service Providers*) possam gerar *tokens* de pagamento que estão em conformidade com um formato interoperável uniforme antes de serem usados em transações de pagamento *contactless*.

Ainda conforme mostrado na Figura 11, as instituições TSP são as entidades dentro de uma infraestrutura de pagamentos *contactless* certificadas, o que a permite ser responsável para gerar, emitir, atribuir e gerenciar o ciclo de vida de tokens de pagamentos. Esses *tokens* de pagamentos só podem ser usados em um domínio específico, como por exemplo fazer pagamentos via smartphones.

O principal objetivo do processo de tokenização é proteger o portador do cartão de fraudes e roubo de dados. Dois exemplos de instituições TSP são a American Express Token Service e a VISA Token Service.

Figura 11 - Fluxo e infraestrutura de tokenização



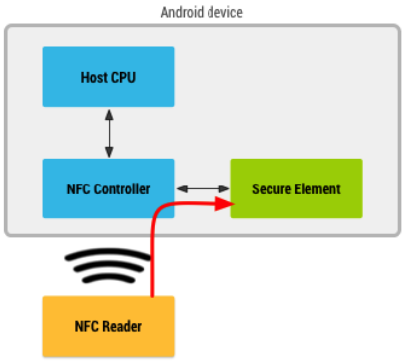
Fonte: Figura adaptada do: (“Bank Islam Brunei Darussalam Chooses Rambus to Secure Mobile Payments”, 2018)

2.3.3 Elemento Seguro

Conforme ilustrado na Figura 12, tradicionalmente as credenciais do cartão utilizadas para pagamentos móveis estão armazenadas dentro de um hardware referido como elemento seguro. O elemento seguro, trata-se de um chip inviolável e independente capaz de armazenar com segurança dados e chaves criptográficas, assim como realizar o processamento de transações sensíveis (“Host-based card emulation overview | Android Developers”, 2019). Devido ao fato de o elemento seguro possuir em sua estrutura um processador criptográfico, operações criptográficas e autenticações de transações como controle de acesso em edifícios, bilhetagem de transporte, entre outros, são possíveis.

Quando um usuário aproxima seu *smartphone*, com a funcionalidade NFC habilitada, de um terminal POS ou um leitor NFC, o controlador NFC automaticamente encaminha todas as mensagens do terminal POS ou leitor NFC para a aplicação correspondente instalada no elemento seguro, sem passar pelo sistema operacional do *smartphone*.

Figura 12 - Emulação NFC de cartão com elemento seguro



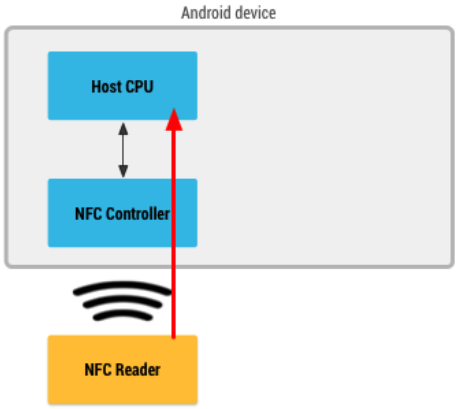
Fonte: (“Host-based card emulation overview | Android Developers”, 2019)

2.3.4 Host Card Emulation

HCE (*Host Card Emulation*), trata-se de uma tecnologia que envolve o uso de software para emular a funcionalidade de um cartão de pagamento *contactless* em aparelhos que possuem um dispositivo NFC e que seguem os padrões da especificação ISO/IEC 14443 (14443-4, 2018**)**. Devido ao fato de o recurso HCE tipicamente ser implementado como um serviço, não há a necessidade de existir uma interface com o usuário possibilitando assim sua execução em segundo plano (“Host-based card emulation overview | Android Developers”, 2019). Esse recurso é vital para uma gama de aplicativos NFC como, por exemplo, um aplicativo de emissão de bilhetes de um sistema de transporte coletivo, onde basta o usuário aproximar seu smartphone do leitor de pagamentos *contactless* para que seja dado início ao processo da transação responsável por efetuar o pagamento do bilhete.

Antes da introdução do recurso HCE, todos os dados recebidos pelo controlador NFC eram roteados diretamente para o elemento seguro. Atualmente, com a rápida proliferação do recurso HCE nas carteiras digitais, os dados são transmitidos para a CPU do dispositivo habilitado para NFC, que se torna responsável por transferi-los ao aplicativo correspondente através do sistema operacional como representado na Figura 13. Todas as credenciais necessárias para dar suporte à funcionalidade NFC estão salvas em um ambiente *secure cloud storage.*

Figura 13 - Emulação NFC de cartão sem elemento seguro



Fonte: (“Host-based card emulation overview | Android Developers”, 2019)

3 FLUXO TRANSACIONAL UTILIZANDO O PADRÃO EMV

Neste capítulo será abordada a forma como ocorre um fluxo transacional, seguindo os padrões EMV, tanto para transações do tipo *contact* quanto para o tipo *contacless*.

3.1 Etapas de autorização de uma transação por meio digital

Uma transação financeira eletrônica, seja ela realizada através de um dispositivo, como por exemplo um *smartphone*, ou um cartão é composta pelos seguintes componentes: emissor, adquirente, portador e estabelecimento.

Segundo (“Dicionário do Cartão | ABECS”, [s.d.]), emissores podem ser instituições financeiras responsáveis por emitir e administrar cartões, tanto de débito quanto crédito, sejam esses cartões próprios da instituição ou de terceiros e o financiamento é concedido diretamente por elas aos portadores dos cartões. Essas instituições financeiras são comumente chamadas de bandeiras. No Brasil, as principais bandeiras atuantes são Diners*, Visa,* American Express e Mastercard. Há ainda as administradoras, que também podem ser consideradas emissores, que são empresas não financeiras que administram e emitem os cartões, tanto de terceiros quanto próprios, mas o financiamento não é concedido diretamente os clientes. Essas empresas representam os portadores junto as instituições financeiras com o intuito de obtenção de financiamento.

Adquirentes são as empresas ou companhias atuantes na efetuação de transações financeiras e são responsáveis por prover a comunicação entre o banco emissor e o *e-commerce*, por fim enviar ao comércio (conhecido também como estabelecimentos) a resposta vinda do emissor. As companhias atuantes como adquirentes são obrigadas a possuir um certificado de *PCI Compliance*, reconhecida internacionalmente como uma das maiores soluções em segurança e sendo necessário para todos as empresas que realizam armazenamento, transmissão de dados de cartões pela web e processamento de transações. Alguns exemplos de adquirentes no Brasil são Pagseguro, Cielo, Redecard e GetNet.

Ao consumidor final que tem interesse em adquirir serviços e/ou bens usando como meio de pagamento o dispositivo móvel ou o cartão de crédito é atribuído o identificador de portador.

As empresas e lojistas são estabelecimentos que prestam serviços ou vendem bens, que podem ser pagos através dos meios eletrônicos de pagamentos utilizando por exemplo, um terminal POS. Aos estabelecimentos cabe o papel da solicitação da autorização de pagamento junto ao banco emissor do portador.

3.2 Fluxo transacional

Transações realizadas com cartões de crédito ou débito, podem ser processadas por diversas plataformas como dispositivos móveis, lojas físicas e do comércio eletrônico e terminais com e sem fio. Em poucos segundos, todo o fluxo da transação é processado, desde o momento em que a transação é capturada no terminal POS até a impressão do comprovante contendo o código da autorização (PAPADIMITRIOU, 2020).

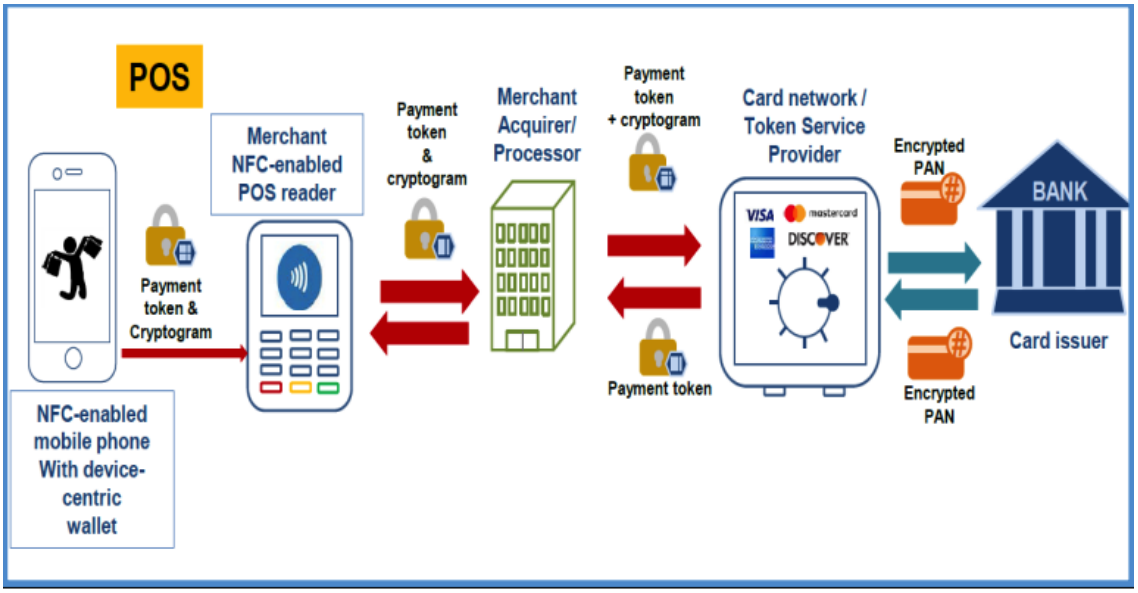
Para que haja a autorização de transações comerciais algumas normas devem ser respeitadas. Em princípio, o estabelecimento comercial deve ter a transação aprovada juntamente ao banco emissor e o portador deve apresentar o dispositivo/cartão a fim de realizar um pagamento através de um terminal POS pertencente ao estabelecimento.

Em pagamentos do tipo *contact*, o cartão é inserido no terminal POS, os dados do cartão são lidos e enviados ao banco adquirente através de uma linha telefônica ou conexão com a internet. Em sequência, o processador ou adquirente envia os dados do cartão a rede de cartões de débito ou crédito e realiza a solicitação de autorização do pagamento ao banco emissor do cartão. A solicitação de autorização deve ser composta pelos componentes: número do cartão, código de segurança, endereço de cobrança (este será validado pelo sistema de verificação de endereço) e a data de expiração do cartão.

No processo de autenticação, os dados do cartão como: senha, data de validade, código de segurança, limite ou saldo do cliente, são verificados pelo banco emissor. Nesta etapa também é realizada uma análise de risco utilizando ferramentas de proteção contra fraudes. Após o emissor receber a requisição, validar os dados do cartão, realizar a análise de fraude, ele nega ou aprova a transação e envia o retorno para o estabelecimento. Se a transação for aprovada, o banco emissor sensibiliza o saldo ou o limite do portador do cartão abatendo o valor da compra.

A Figura 14 ilustra o fluxo de uma transação utilizando um *smartphone* como forma de pagamento. Em transações realizadas através de *smartphones* a comunicação é feita com um terminal POS que possui a tecnologia NFC utilizando o aplicativo de pagamento (este aplicativo pode ser uma carteira digital). O aplicativo de pagamento envia um *token* que representa os dados do cartão. A instituição financeira é quem gera o *token* quando o usuário registra seu cartão no aplicativo de pagamento em seu *smartphone* (EMVCo, 2020).

Figura 14 - Fluxo de uma transação *contactless* utilizando um *smartphone*



Fonte: Federal Reserve Bank of Boston (2017, p.8)

4 CONSIDERAÇÕES FINAIS

O padrão global de pagamentos interoperável EMV foi introduzido em 1996 com o objetivo de mitigar fraudes e reduzir custos operacionais. Implementar o padrão EMV ao mesmo tempo em que ocorre uma disseminação do uso da tecnologia NFC faz bastante sentido. As três formas de pagamentos: EMV *contact*, EMV *contactless* e NFC no modo emulação de um cartão *contactless* são baseados em padrões e são interoperáveis dentro de uma bandeira de cartão.

Nem todos os consumidores adotarão o método de pagamento NFC via *smartphone* imediatamente. Para aqueles que o fizerem, os aplicativos de pagamento NFC via *smartphone* normalmente são oferecidos como uma opção complementar aos tradicionais cartões de plástico, para garantir a aceitação universal em estabelecimentos comerciais que não utilizam terminais capazes de realizar transações *contactless*. Os aplicativos de pagamento EMV via NFC disponíveis para *smartphones* são compatíveis com a mesma infraestrutura utilizada para pagamentos *contactless* EMV utilizando cartões plásticos.

O uso de carteiras digitais é uma opção mais segura do que carregar cartões físicos. Essa segurança reside no fato de os aplicativos de carteira digital, como o Apple Pay, converterem todos os seus dados bancários em algo que não pode ser acessado ou usado pelos fraudadores. Todos os seus cartões de crédito e outros dados sigilosos permanecem protegidos, mesmo que seu smartphone seja roubado.

Os sistemas de pagamento NFC são muito mais rápidos comparados aos pagamentos feitos com cartões de tarja, chip e em dinheiro. A agilidade é decorrente do fato de que em pagamentos NFC o usuário precisa apenas aproximar o cartão ou o *smartphone* do terminal POS para que seja dado início a transação. Para o comerciante também é bastante conveniente, pois não é necessário aguardar o cliente inserir seu PIN ou retirar e contar o dinheiro de sua carteira. Através do uso da tecnologia NFC os pagamentos podem ser feitos em segundos.

A conveniência pode ser considerada uma das maiores vantagens no uso de pagamentos via NFC, pois para o usuário ficou bastante prático fazer pagamentos utilizando seu *smartphone* ou *tablet*. A forma como todo o processo de pagamento ocorre é bem fácil de usar e entender, isso permite ao usuário realizar pagamentos apenas aproximando seu dispositivo móvel do terminal POS.

A tecnologia NFC proporciona diversos benefícios, mas há um custo para esses benefícios. Para algumas empresas esse custo pode ser muito alto. Grandes corporações e empresas multinacionais, por exemplo, conseguem integrar com sucesso a tecnologia NFC em seus sistemas, no entanto para pequenas e médias empresas a integração NFC pode causar um grande impacto no faturamento e impossibilitar o aumento nos lucros. Todo esse impacto é em decorrência do alto custo de instalação de *software* e *hardware* juntamente com a contração de mão de obra especializada para a implantação.

A tecnologia NFC é mais segura quando comparada com a tecnologia tradicional *contact* de pagamento via cartões, mesmo assim ela não está livre de riscos. Sempre é possível notar que a rápida inovação e evolução na tecnologia traz consequências positivas e negativas. A invasão a *smartphones* tornou-se um fenômeno comum e os *crackers* sempre estão inovando em novas maneiras de enganar os usuários, obtendo acesso aos seus dados financeiros. Isso acaba por tornar todo o sistema NFC propenso a golpes e fraudes, o que pode acabar desencorajando os usuários, tanto clientes quanto comerciantes, a utilizarem essa tecnologia para pagamentos.

Pagamentos utilizando a tecnologia NFC via *smartphones* é uma forma de pagamento móvel inovadora que permite consumidores transformem seus celulares em carteiras digitais. Esta inovação está alinhada com a tendência do mercado onde o número de usuários de *smartphones* vem crescendo significativamente e os serviços móveis estão se tornando cada vez mais parte do dia a dia dos consumidores, principalmente no que diz respeito a pagamentos.

Tanto as empresas que atuam no desenvolvimento de *smartphones* quanto as bandeiras de cartões possuem um grande desejo em aumentar a aceitação e a implementação desta modalidade de pagamento, tendo em vista que, esta, deverá ser a tecnologia de pagamento do futuro e ainda possibilitando criar uma variedade de novas oportunidades de negócios. Mas, por trás de todo esse otimismo, a implantação de pagamento móvel baseado em NFC é ainda muito limitada, os consumidores ainda têm dúvidas sobre a adoção desta modalidade de pagamento.

Em outros palavras, o desenvolvimento da inovação de pagamentos via NFC está experimentando uma condição paradoxal, onde por um lado pesquisadores e empresas de pagamento móvel baseadas em NFC estão altamente otimistas sobre

essa inovação, enquanto, por outro, alguns consumidores ainda estão hesitantes em usar esta modalidade de pagamento móvel.

Devido ao fato de quase não haver bibliografias na língua portuguesa que tratem do tema EMV e boa parte das bibliografias na língua inglesa serem pagas, acabou por impor certas barreiras para o desenvolvimento do trabalho.

4.1 Sugestões de trabalhos futuros

Como sugestão para trabalhos futuro fica o aprofundamento nos estudos e possíveis implementações para mitigar alguns já conhecidos ataques a modalidade de pagamento via NFC como, *Relay Attack*, *Cloning Attack e Man-in-the-Middle* e o aprofundamento nos estudos e possíveis sugestões de melhorias para as falhas de segurança do padrão EMV.

REFERÊNCIAS

ALESS et al. **NFC (Near Field Communication) – Aplicações e uso**. Disponível em: <https://www.embarcados.com.br/nfc-near-field-communication/>. Acesso em: 30 abr. 2022.

AKANA, T.; KE, W. Contactless Payment Cards: Trends and Barriers to Consumer Adoption in the U.S. **Discussion Papers (Federal Reserve Bank of Philadelphia)**, maio 2020.

Balanço do setor de meios eletrônicos de pagamento RESULTADOS 1T22. [s.l: s.n.]. Disponível em: <https://api.abecs.org.br/wp-content/uploads/2022/05/Apresenta%C3%A7%C3%A3o-1T22.pdf>. Acesso em: 18 jun. 2022.

Bank Islam Brunei Darussalam Chooses Rambus to Secure Mobile Payments. Disponível em: <https://www.businesswire.com/news/home/20181205005205/en/Bank-Islam-Brunei-Darussalam-Chooses-Rambus-to-Secure-Mobile-Payments>. Acesso em: 30 abr. 2022.

COSKUN, V.; OZDENIZCI, B.; OK, K. The Survey on Near Field Communication. **Sensors**, v. 15, n. 6, p. 13348–13405, 5 jun. 2015.

Dicionário do Cartão | ABECS. Disponível em: <https://www.abecs.org.br/dicionario-do-cartao>. Acesso em: 6 maio. 2022.

EMVCo - Contactless Specifications for Payment Systems Book A Architecture and General Requirements. [s.l: s.n.]. Disponível em: <https://www.emvco.com/wp-content/uploads/2017/05/Book_A_Architecture_and_General_Rqmts_v2_6_Final_20160422011856105.pdf>. Acesso em: 28 abr. 2022.

EMVCo - Integrated Circuit Card Specifications for Payment Systems,: Book 1: Application Independent ICC to Terminal Interface Requirements, Version 4.3, EMVCo, Novembro (2011)

EMVCo - Integrated Circuit Card Specifications for Payment Systems,: Book 2: Security and Key Management, Version 4.3, EMVCo, Novembro (2011)

EMVCo - Integrated Circuit Card Specifications for Payment Systems,: Book 3: Application Specification, Version 4.3, EMVCo, Novembro (2011)

EMVCo - Integrated Circuit Card Specifications for Payment Systems,: Book 4: Cardholder, Attendant, and Acquirer Interface Requirements, Version 4.3, EMVCo, Novembro (2011)

EMVCo, LLC A Guide to EMV Chip Technology Version 2.0 A Guide to EMV Chip Technology Version 2.0. [s.l: s.n.]. Disponível em: <https://www.emvco.com/wp-content/uploads/2017/05/A_Guide_to_EMV_Chip_Technology_v2.0_20141120122132753.pdf>.

EMVCo - Payment Tokenisation Specification. [s.l: s.n.]. Disponível em: <https://www.emvco.com/wp-content/uploads/2020/09/EMV-Payment-Tokenisation-Specifciation-Technical-Framework-v2.1-Full-FAQ-updated.pdf>. Acesso em: 29 abr. 2022.

First & Merchants BankAmericard Visa. Disponível em: <https://americanhistory.si.edu/collections/search/object/nmah_1444151#:~:text=The%20BankAmericard%20was%20introduced%20by>. Acesso em: 02 mai. 2022.

Google Inc. 2017. Host-based card emulation overview | Android Developers. Disponível em: <https://developer.android.com/guide/topics/connectivity/nfc/hce>. Acesso em: 30 abr. 2022.

Host-based card emulation overview | Android Developers. Disponível em: <https://developer.android.com/guide/topics/connectivity/nfc/hce>. Acesso em: 30 abr.

IGOE, T.; COLEMAN, D.; JEPSON, B. **Beginning NFC : near field communication with Arduino, Android, and Phonegap**. Beijing: O'reilly, 2014.

ISO/IEC 14443-4:2018. Cards and security devices for personal identification — Contactless proximity objects — Part 4: Transmission protocol. Disponível em: <https://www.iso.org/standard/73599.html>. Acesso em: 24 abr. 2022.

ISO/IEC 18092:2004. Information technology – telecommunications and information exchange between systems–Near Field Communication–interface and protocol (NFCIP-1). (2004). Disponível em: <https://www.iso.org/standard/38578.html>. Acesso em: 24 abr. 2022.

ISO/IEC 7816-4:2013. Information technology – telecommunications and information exchange between systems – Near Field Communication interface and protocol (NFCIP-2). (2005). Disponível em: <https://www.iso.org/standard/54550.html>. Acesso em: 24 abr. 2022.

M. Reveilhac and M. Pasquet, "**Promising secure element alternatives for nfc technology,"** in Near Field Communication, 2009. NFC '09. First International Workshop on, fev. 2009, pp. 75 –80.

Mastercard EMV Chip Technology | EMV Chip Card Solutions for Issuers. Disponível em: <https://sea.mastercard.com/en-region-sea/business/issuers/products-and-solutions/payment-innovations/chip-emv.html>. Acesso em: 18 jun. 2022.

nRF5 SDK v15.0.0: NDEF message and record format. Disponível em: <https://infocenter.nordicsemi.com/topic/com.nordic.infocenter.sdk5.v15.0.0/nfc_ndef_format_dox.html>. Acesso em: 31 mar. 2022.

PAPADIMITRIOU, Odysseas. **How Credit Card Transaction Processing Works: Steps, Fees & Participants**. Disponível em: <https://wallethub.com/edu/cc/credit-card-transaction/25511>. Acesso em: 6 maio. 2022.

PHAM, T.-T. T.; HO, J. C. The effects of product-related, personal-related factors and attractiveness of alternatives on consumer adoption of NFC-based mobile payments. **Technology in Society**, v. 43, p. 159–172, nov. 2015

Point-of-Sale Terminals. Disponível em: <https://www.bdo.com.ph/POSTerminals>. Acesso em: 18 jun. 2022.

PRODANOV, Cleber Cristiano; FREITAS, Ernani Cesar de. **Metodologia do trabalho científico: Métodos e Técnicas de Pesquisa e do Trabalho Acadêmico**. 2.ed. Novo Hamburgo-Rio Grande do Sul: Universidade FEEVALE, 2013.

QR codes. Disponível em: <https://sites.usp.br/comcirp/qr-codes/>. Acesso em: 18 jun. 2022.

REYNOLDS, F. Whither Bluetooth? **IEEE Pervasive Computing**, v. 7, n. 3, p. 6–8, jul. 2008.

RFID | Electronic Tutorials | Mepits | Mepits. Disponível em: <https://www.mepits.com/tutorial/239/basic-electronics/rfid-a-technology-better-than-barcodes>. Acesso em: 25 mar. 2022

ROCHA, Daniel. Transações financeiras feitas digitalmente devem crescer 142% até 2030. **Estadão. 2022**. Disponível em: <https://einvestidor.estadao.com.br/comportamento/pix-transacao-financeira-digital-crescimento>. Acesso em: 27 maio. 2022.

SABELLA, R.; JOHN PAUL MUELLER. **NFC for dummies**. [s.l.] Hoboken, Nj John Wiley Et Sons, Inc, 2016.

SCHILIT, B. N.; SENGUPTA, U. Device ensembles ubiquitous computing. **Computer** , v. 37, n. 12, p. 56–64, dez. 2004.

SILVA, José P. **Gestão e Análise de Risco de Crédito**. 3. ed. São Paulo: Atlas, 2000.

SVIGALS, J. The long life and imminent death of the mag-stripe card. **IEEE Spectrum**, v. 49, n. 6, p. 72–76, jun. 2012.

Universidade de Aveiro › SWEET. Disponível em: <http://sweet.ua.pt/andre.zuquete/Aulas/IRFID/11-12/docs/NFC%20Data%20Exchange%20Format%20(NDEF).pdf>. Acesso em: 31 mar. 2022.

VEDAT COSKUN; OK, K.; BUSRA OZDENIZCI. **Near field communication : from theory to practice.** Reino Unido: John Wiley & Sons, 2012.

VIJAYAN, J. **5 issues that could hamper EMV smartcard adoption in the U.S.** Disponível em: <https://www.computerworld.com/article/2487581/5-issues-that-could-hamper-emv-smartcard-adoption-in-the-u-s-.html?page=2>. Acesso em: 22 abr. 2022.

WANT, R. Near field communication. **IEEE Pervasive Computing**, v. 10, n. 3, p. 4–7, 2011.