

UNIVERSIDADE FEDERAL DE UBERLÂNDIA

FACULDADE DE ENGENHARIA ELÉTRICA

PÓS-GRADUAÇÃO EM ENGENHARIA ELÉTRICA



**UM SISTEMA PARA PAGAMENTOS MÓVEIS UTILIZANDO
COMUNICAÇÃO POR PROXIMIDADE DE CAMPO.**

SÉRGIO HENRIQUE VITAL DE CARVALHO SILVA

AGOSTO

2013

SÉRGIO HENRIQUE VITAL DE CARVALHO SILVA

UM SISTEMA PARA PAGAMENTOS MÓVEIS UTILIZANDO
COMUNICAÇÃO POR PROXIMIDADE DE CAMPO.

Dissertação apresentada ao Programa de Pós-Graduação em Engenharia Elétrica da Universidade Federal de Uberlândia, como requisito parcial à obtenção do título de Mestre em Engenharia de Telecomunicações.

Área de pesquisa: Processamento digital de sinais.

Orientadora: Professora Dra. Edna Lúcia Flôres

Uberlândia

AGOSTO 2013

SÉRGIO HENRIQUE VITAL DE CARVALHO SILVA

UM SISTEMA PARA PAGAMENTOS MÓVEIS UTILIZANDO
COMUNICAÇÃO POR PROXIMIDADE DE CAMPO.

Dissertação apresentada ao Programa de Pós-Graduação em Engenharia Elétrica da Universidade Federal de Uberlândia, como requisito parcial à obtenção do título de Mestre em Engenharia de Telecomunicações.

Área de pesquisa: Processamento digital de sinais.

Banca Examinadora

Profª. Dra. Edna Lúcia Flôres (Orientadora – UFU)

Prof. Dr. Rodrigo Pinto Lemos - UFG

Prof. Dr. Paulo Sérgio Caparelli – UFU

Prof. Dr. Antônio Cláudio Paschoarelli Veiga – UFU

Uberlândia, agosto de 2013

UM SISTEMA PARA PAGAMENTOS MÓVEIS UTILIZANDO COMUNICAÇÃO POR PROXIMIDADE DE CAMPO.

SÉRGIO HENRIQUE VITAL DE CARVALHO SILVA

Dissertação apresentada à Universidade Federal de Uberlândia, como requisito parcial à obtenção do título de Mestre em Engenharia de Telecomunicações.

Sr. Sérgio Henrique Vital de Carvalho Silva
Mestrando

Profa. Dra. Edna Lúcia Flôres
Orientadora

Prof. PhD Dr. Edgard A. Lamounier Júnior
Coordenador da Pós-Graduação

AGRADECIMENTOS

À minha mãe, obrigado pela vida, educação e incentivo constantes ao longo da vida.

Ao meu pai pela sua dedicação e por ser meu herói.

À minha irmã pelo seu exemplo de irmandade, amizade verdadeira, apoio e amor.

À minha namorada pela companhia constante, compreensão, carinho e amor.

À toda minha família e verdadeiros amigos, que nunca me abandonaram, pelo eterno apoio, motivação e exemplo.

À Professora Edna Lúcia Flôres, primeiramente por ter acreditado no meu trabalho e na minha capacidade, pela sua confiança, amizade e principalmente orientação em me guiar durante todo o caminho.

Obrigado a Deus e ao Senhor, que me deram a fé necessária para acreditar, a força para não desistir, a inteligência para escolher o melhor caminho e o amor para seguir em frente.

“Afinal, ter problemas não é tão desesperador assim. Desesperador é não ter coragem de lutar contra eles. Homens fortes, homens criadores, que realizam grandes obras, acham que os problemas são para a mente como o exercício é para os músculos: desenvolvem nela a resistência necessária a uma vida construtiva e feliz. Agradeço a DEUS hoje pelos problemas que consegui vencer com minha coragem e determinação. Quando alguém disser para você que não será possível, que você não conseguirá, pare e reflita mas continue seguindo em frente, e lembre-se: se você conseguiu chegar até aqui, você pode realizar o que quiser, basta ter fé!”

RESUMO

A Comunicação por Proximidade de Campo do inglês Near Field Communication (NFC) e os pagamentos móveis são duas áreas em constante desenvolvimento no mercado atual. Hoje ao utilizar a carteira são encontradas cédulas de diferentes valores, moedas, cartões de débito e de crédito de um ou dois bancos, cartões fidelidade de restaurantes e recibos de compras. Mesmo que esses itens encontrados na carteira tenham um valor simbólico de utilidade, eles estão se tornando ultrapassados, como uma infinidade de plástico e papel que não fará muito sentido em um futuro próximo. A revolução dos pagamentos móveis é iminente e já está acontecendo. No lugar das carteiras estão entrando os celulares com dispositivos NFC em seu hardware e software que os transformam em uma carteira digital (e-wallet). O que interessa não são mais os papeis e os cartões, mas sim estar conectado com sua conta da e-wallet que possui seus dados bancários. O principal objetivo desta dissertação é apresentar o desenvolvimento de um sistema de pagamentos móveis denominado sistema S-Wallet, utilizando como base a tecnologia NFC. Este trabalho também inclui o desenvolvimento de um protocolo de pagamentos móveis, o protocolo SWEP, que realiza todo o processo de troca de mensagens, troca de dados e execução do pagamento. Além da App S-Wallet, uma aplicação com interface android para os usuários utilizarem. Assim como uma conta que armazena os dados dos usuários remotamente, denominada conta S-Wallet. Como parte da avaliação do sistema S-Wallet, foram realizados testes de integração das entidades desse sistema. Esses testes mostraram que o sistema S-Wallet proporciona usabilidade, segurança e privacidade aos usuários. Além disso foram realizados testes de usabilidade com usuários que mostraram que o sistema S-Wallet é fácil de usar e que pode ser indicado para o cenário pesquisado: pagamento entre dois usuários do inglês peer-to-peer (P2P) e máquinas de venda do varejo. Este trabalho mostra que a tecnologia NFC é segura para pagamentos móveis e é de grande utilidade para a expansão da mesma no setor comercial.

Palavras-chave: Comunicação por proximidade de campo, carteira digital, pagamentos móveis, segurança, usabilidade.

ABSTRACT

The Near Field Communication (NFC) and mobile payments are two areas in constant development in current market. Today when we use the wallet, we can found cash of different values, coins, debit and credit cards of one or two banks, loyalty cards from restaurants and shopping receipts. Even though these items found in the wallet have a symbolic value of utility, they are becoming outdated, as a plethora of plastic and paper that will not make much sense in the near future. The revolution of mobile payments is imminent and is already happening. Instead of wallets, we have mobile phones with NFC on their hardware and software that transform them into a digital wallet (e-wallet). What matters now are not the papers and cards, but stay connected to your e-wallet account's that has your bank details. The main objective of this dissertation is to present the development of a mobile payment system called S-Wallet system, using the technology of NFC. This work also includes the development of a protocol for mobile payments, the protocol SWEP, which performs the whole process of message exchange, data exchange and payment execution. Besides the App S-Wallet, an application interface to android users use. In addition, an account that stores users data remotely, called S-Wallet account. As part of the evaluation of the S-Wallet, we perform tests of integration of all the entities of the system. These tests showed that the S-Wallet provides usability, security and privacy to users. Further, we had performed usability tests with users showing that the S-Wallet system is easy to use and we had indicated it for the real scenario studied: payment between two users, peer-to-peer (P2P) and retail vending. This work shows that the NFC technology is secure for mobile payments and is very useful for its expansion in the commercial sector.

Keywords: Near field communications, digital wallet, mobile payments, security, and usability.

SUMÁRIO

AGRADECIMENTOS	v
RESUMO.....	6
ABSTRACT	7
LISTA DE FIGURAS.....	6
LISTA DE TABELAS.....	8
LISTA DE ABREVIATURAS.....	9
Capítulo 1 INTRODUÇÃO	10
1.1 Introdução	10
1.2 E-Wallets: Pagamentos Móveis	12
1.3 Motivação Deste Trabalho	13
1.4 Proposta Deste Trabalho	14
1.5 Estrutura da Dissertação	16
1.6 Considerações Finais Deste Capítulo	17
Capítulo 2 TECNOLOGIAS ATUAIS	18
2.1 Introdução	18
2.2 Código de Barras	18
2.3 Tarja Magnética	21
2.4 Identificação por Radiofrequência (RFID)	23
2.5 Smart Cards.....	27

2.5.1	ISO/IEC 7816	28
2.5.2	ISO/IEC 14443	31
2.6	MiFare.....	32
2.7	MiFare classic	33
2.7.1	Interface de radiofrequência.....	34
2.7.2	Organização da memória.....	35
2.7.3	Unidade de Controle Digital	36
2.8	FeliCa.....	37
2.9	Considerações finais deste capítulo	37
Capítulo 3 COMUNICAÇÃO POR PROXIMIDADE DE CAMPO		38
3.1	Introdução	38
3.2	Modos de operação	40
3.3	Topologia e Comunicação	41
3.4	Codificação e Modulação	41
3.4.1	Código Manchester	42
3.4.2	Código Miller modificado	43
3.5	Prevenção de Colisão.....	43
3.6	Fluxo Geral do protocolo	44
3.7	Aspectos de Segurança	46
3.7.1	Escutas (<i>Eavesdropping</i>).....	47
3.7.2	Destruição de dados	49
3.7.3	Modificação dos dados.....	49

3.7.4	Inserção de dados	51
3.7.5	Man-in-the-middle-attack.....	51
3.8	Aplicabilidade	53
3.9	Considerações Finais deste Capítulo	54
Capítulo 4 ARQUITETURA DO SISTEMA S-WALLET		55
4.1	Introdução	55
4.2	Principais Características do Sistema S-Wallet	56
4.3	Estrutura do Sistema S-Wallet	56
4.3.1	Sistema Cliente.....	60
4.3.2	Sistema varejista (loja)	63
4.3.3	Conta S-Wallet	64
4.3.4	Operações da S-Wallet:	64
4.3.5	Comunicações do sistema S-Wallet	82
4.4	Protocolo SWEP	85
4.5	App S-Wallet	90
4.6	Considerações Finais deste Capítulo	91
Capítulo 5 MÉTODO PROPOSTO		93
5.1	Introdução	93
5.2	Hardware utilizado.....	95
5.3	Interfaces de Comunicação	96
5.4	Applets Java – Procotolo SWEP.....	97
5.5	Conta S-Wallet – Base de Dados/Cloud Computing	100

5.6	Componente Java Micro Edition (App S-Wallet).....	101
5.6.1	Camada de apresentação	102
5.6.2	Camada de execução	103
5.6.3	Camada de comunicação	104
5.7	Sistema Varejista	105
5.8	Considerações Finais deste Capítulo	106
Capítulo 6	RESULTADOS OBTIDOS	107
6.1	Introdução	107
6.2	Desempenho do Protocolo SWEP	107
6.3	Custo do Hardware	110
6.4	Testes de Integração.....	111
6.4.1	Primeiro teste: inicialização da conta S-Wallet.....	111
6.4.2	Segundo teste: conexão inicial entre dois usuários.	112
6.4.3	Terceiro teste: realização e execução de pagamento.....	115
6.4.4	Quarto teste: usabilidade da App	117
6.4.5	Sexto Teste: segurança do sistema S-Wallet.....	120
6.5	Testes Qualitativos.....	121
6.6	Soluções existentes na literatura	122
6.6.1		126
6.7	Conclusões	127
Capítulo 7	CONCLUSÕES E CONTRIBUIÇÕES DESTE TRABALHO E TRABALHOS FUTUROS	130

7.1	Introdução	130
7.2	Conclusões	130
7.3	Contribuições deste Trabalho	131
7.4	Trabalhos Futuros	133
<i>REFERÊNCIAS</i>		134

LISTA DE FIGURAS

Figura 2-1 - Três variações de intensidade de códigos de barra.....	19
Figura 2-2 - Um exemplo de codificação de um código de barras 2D.....	21
Figura 2-3 – Tarja magnética aplicada a um cartão de plástico, conforme o padrão.	22
Figura 2-4 – Códigos devolvidos por uma resposta APDU [13].....	31
Figura 2-5 – Estrutura do IC com um cartão MiFare	34
Figura 3-1 – Etiqueta RFID passiva colada em um cartão de ônibus.....	41
Figura 3-2 - Código Manchester.....	43
Figura 3-3 - Código Miller modificado	43
Figura 3-4 – Inicialização geral e protocolo de transporte	45
Figura 3-5 – Modificação de bit da codificação de miller modificada.....	50
Figura 4-1 – Entidades participantes do ciclo de pagamentos da S- Wallet.	57
Figura 4-2 – Fluxo da operação de Crédito	67
Figura 4-3 – Ações que ocorrem durante o fluxo da operação de Crédito.....	68
Figura 4-4 – Fluxo da operação de pagamento.....	70
Figura 4-5 – Ações executadas durante a operação de seleção de pagamento.....	71
Figura 4-6 – Ações durante a função de pedido de conexão	73
Figura 4-7 – Ações executadas durante a inicialização do SWEF.	73
Figura 4-8 – Ações executadas durante a verificação do ID e inicialização da eNota...	75
Figura 4-9 – Ações executadas durante a transferência de dados.	76
Figura 4-10 – Ações executadas durante a confirmação do pagamento.....	77
Figura 4-11 – Ações executadas pelas Apps durante o encerramento da conexão	78
Figura 4-12 – Fluxo da operação de depósito e débito.....	79
Figura 4-13 – Fluxo de ações da operação de débito ou depósito.....	80
Figura 4-14 – Fluxo da operação de verificação de histórico/saldo.	81

Figura 4-15 – Ações realizadas pela operação de verificação de histórico/saldo.	82
Figura 4-16 – Estrutura do sistema S-Wallet.....	91
Figura 5-1 – Fases do desenvolvimento	93
Figura 5-2 – Arquitetura do protótipo de testes do sistema desenvolvido neste trabalho.	96
Figura 5-3 – Layout da operação de identificação do sistema S-Wallet	103
Figura 5-4 – Layout de uma execução de pagamento.	104
Figura 5-5 – Layout de solicitação de conexão para pagamento P2P.	105
Figura 6-1 – Tela de cadastro do sistema S-Wallet no smartphone.	112
Figura 6-2 – Taxa de conexão inicial entre dois usuários.	114
Figura 6-3 – Taxa de velocidade nas conexões realizadas com eficácia.....	114
Figura 6-4 – Número de conexões realizadas no teste.	116
Figura 6-5 – Porcentagem de acerto nas tentativas de conexão e envio de dados.	117
Figura 6-6 - Respostas dos participantes do teste de usabilidade.....	118
Figura 6-7 – Gráfico dos testes de acompanhamento da rede pelo teste de análise de pacotes (sniffer).	121

LISTA DE TABELAS

Tabela 2-1 – Diferenças técnicas e funcionais entre as tecnologias de RFID ativa e passiva [30].....	26
Tabela 2-2 – Estrutura de um comando APDU [33].	29
Tabela 2-3 – Especificação de um comando APDU [33].....	29
Tabela 2-4 – Estrutura de uma resposta APDU [12].	30
Tabela 2-5 – Especificações de uma resposta APDU [12].....	30
Tabela 2-6 – Partes constituintes da especificação do padrão ISO/IEC 14443.....	32
Tabela 2-7 - Principais características de acordo com a ISO 14443-tipo A.....	34
Tabela 3-1 - Codificação e modulação em diferentes velocidades de transferência [41]	42
Tabela 6-1 – Desempenho do sistema S-Wallet.....	108
Tabela 6-2 – Desempenho do sistema de segurança criptográfico da S-Wallet.....	109
Tabela 6-3 – Comparação do Sistema S-Wallet com protocolos de pagamentos da literatura.....	125

LISTA DE ABREVIATURAS

DSL - Digital Subscriber Line.

CDMA - Code Division Multiple Access.

HSDPA+ - High Speed Downlink Pocket Access Plus.

LTE - Long Term Evolution.

WAP - Wireless Application Protocol

P2P - Person-to-Person (peer-to-peer).

P2B - Person to Business.

NFC - Near Field Communication.

SWEP - Smart Way for Easy Payments.

RFID - Radiofrequency Identification.

ASK - Amplitude-Shift Keying

GPRS - General Packet Radio Service

IMEI - International Mobile Equipment Identity

POS - Point of Sale

JCOP - Java Card Open Platform

Capítulo 1

INTRODUÇÃO

1.1 *Introdução*

Atualmente, a sociedade tem presenciado novas formas de relacionamento comercial se comparados aos métodos de compra e pagamento do século IX. O homem mudou totalmente sua forma de interação com a sociedade a partir do desenvolvimento e da popularização da internet ocorrida em 1994 [1]. Após a introdução de protocolos de segurança [2] e de tecnologia como o *Digital Subscriber Line* (DSL) [3], a rede mundial de computadores tem sido utilizada de forma mais contínua e no ano 2000 ocorreu a chamada "bolha da internet" [4].

Na “bolha da internet”, inúmeras empresas do mundo real sejam elas operadoras de telecomunicações, instituições financeiras ou emissoras de TV patrocinaram e investiram no desenvolvimento de portais Web para a interação com os internautas [5]. Surgiram nesse período os primeiros portais de comércio eletrônico (e-commerce) [6], seja ele realizado por plataformas como navegador web ou por outros tipos de dispositivos que possibilitam o acesso à rede mundial de computadores. As trocas comerciais passaram nessa etapa por uma reformulação, onde o indivíduo utiliza os meios de pagamento tais como cartões de crédito ou “*internet banking*” para efetuar os pagamentos.

Paralelamente a essa novidade na maneira de interação do homem em sociedade, ocorreu também uma evolução das tecnologias de telecomunicações. As redes de transmissão de voz e de dados evoluíram desde o Sistema Global para Comunicações Móveis (GSM) do inglês *Global System for Mobile Communications* [7] e o Acesso

Múltiplo por Divisão de Código (CDMA) do inglês *Code Division Multiple Access* [8], do sistema de redes 2G, para as redes 3G com o *High Speed Downlink Pocket Access Plus*, (HSDPA+) [9], possibilitando a rápida transmissão de dados entre os celulares, até a atual rede *Long Term Evolution* (LTE) [10]. O celular evoluiu de um simples aparelho para a comunicação sonora entre duas pessoas, ou até mesmo grupos de pessoas, para um dispositivo multifuncional, com sistema operacional embarcado, hoje conhecido como “*smartphone*” [11].

Inteligente no nome e eficiente em suas funcionalidades, a integração de um sistema operacional ao *smartphone* possibilitou a reinvenção da forma como o ser humano lida com a internet, com os meios de comunicação e com os dados. Com a capacidade de apenas um toque dos dedos, pode-se ter acesso a inúmeras aplicações dentro da plataforma Android (sistema criado pela empresa Google) [12] ou da plataforma IOS (sistema desenvolvido pela Apple) [13].

Essas aplicações possibilitam a interação do usuário com as redes sociais, leitura de *feeds* de notícias, revistas e jornais. As evoluções do celular e das redes de telecomunicações possibilitaram ao ser humano a capacidade de ter o controle sobre sua vida financeira, social e profissional apenas pela utilização de um dispositivo conectado em rede.

Nesse ambiente de desenvolvimento tecnológico, pode-se citar então o nascimento de uma nova modalidade de formas de pagamento. Com a grande penetração do *smartphone* no mercado (hoje existem cerca de 258 milhões de aparelhos celulares no Brasil, destes 49 milhões com utilização de plano de dados 3G) [14] e a popularização do *e-commerce* (espera-se um faturamento total de R\$ 22,5 bilhões em 2013) [15] surge assim o mercado das *e-wallets* [16] e do *m-commerce* [17].

Este capítulo apresenta os pagamentos móveis, a motivação, a proposta e a estrutura desta dissertação.

1.2 *E-Wallets: Pagamentos Móveis*

Define-se *m-commerce* como *Mobile Payment* ou *m-payment*, onde o usuário realiza os pagamentos de compras de produtos, serviços ou contas via celular ou *smartphone*. Esse tipo de pagamento aumenta a velocidade das trocas financeiras realizadas pelos dispositivos, possibilita ao varejo personalizar o atendimento ao cliente e reduz os custos para os varejistas e para as instituições financeiras. Pode-se considerar ainda o *m-commerce* como sendo um subgrupo do comércio eletrônico, porém com uma interação real entre o usuário e o comerciante e virtual na forma como o dinheiro é representado.

Define-se também *e-wallets* ou *Mobile Wallets* como um software de aplicação para realizar *m-payment* que está embarcado no *smartphone* com detalhes do usuário (possivelmente dados da sua conta bancária ou cartão de crédito). Esse software permite realizar pagamentos utilizando esse tipo de dispositivo. Os usuários podem integrar no *smartphone* vários instrumentos de débito ou crédito em uma mesma aplicação.

O dinheiro que antes era utilizado apenas por meio de papel moeda e cartões de plástico com tarja magnética ou micro chip, se digitalizou. Assim, grandes empresas de tecnologia, que realizam pagamentos como Google e Paypal e instituições financeiras como Mastercard e Visa vêm desenvolvendo projetos no setor de pagamentos móveis que movimentou U\$ 172 bilhões em 2012 [18].

Os pagamentos móveis se dividem em dois tipos: pagamentos móveis remotos e pagamentos móveis por proximidade [19]. No pagamento móvel remoto os usuários efetuam suas transações de qualquer lugar, por meio do envio de *Short Message Service*

(SMS) entre as partes ou de uma plataforma *Wireless Application Protocol* (WAP). As transações podem ser *Person to Person* (P2P) ou *Person to Business* (P2B) [20].

O pagamento móvel por proximidade, conhecido como *contactless payment*, ocorre quando um usuário possui um celular com tecnologia *Near Field Communication* (NFC). A NFC embarca um chip e uma antena na estrutura de hardware do dispositivo. Essa tecnologia permite armazenar as informações do usuário e realizar a comunicação com leitores em lojas e estabelecimentos varejistas. Para efetuar o pagamento é necessário o usuário aproximar o aparelho a alguns centímetros do leitor e, por meio de um padrão de comunicação sem fio, é efetuada a compra. Esse tipo de pagamento é apresentado nesta dissertação, onde é utilizada a tecnologia NFC para o desenvolvimento de um protocolo que possa fornecer segurança as transações financeiras entre os dois dispositivos, boa usabilidade e interação com o usuário.

1.3 *Motivação Deste Trabalho*

Ao utilizar a carteira pessoal pode-se encontrar cédulas de diferentes valores, moedas, algumas folhas de talão de cheque, cartões de débito e de crédito de um ou dois bancos, cartões-fidelidade de restaurantes, cafeterias e lojas, recibos de compras e muitos papéis de pagamentos e compras.

Por mais útil que pareça, a carteira hoje é um objeto ultrapassado, com vários itens de plástico e papel substituídos atualmente por sua forma digital. Com o tempo, as carteiras perderão sua exclusividade na hora de realizar pagamentos ou transferências. Em seu lugar são utilizados os celulares.

Os dispositivos móveis têm sofrido uma evolução contínua ao longo dos anos. Sua capacidade computacional aumentou, assim como a qualidade e a tecnologia das

telas sensíveis ao toque. Além das características básicas, os dispositivos vêm embarcados com tecnologias como o *bluetooth*, câmera digital, *wi-fi* e a NFC.

Essa capacidade computacional, associada às tecnologias embarcadas, possibilita o desenvolvimento de sistemas como os para pagamentos móveis. Um sistema para pagamentos móveis não oferece uma funcionalidade nova, apenas uma nova forma de desempenhá-la. Assim, para que o pagamento móvel se mostre necessário o sistema deve apresentar vantagens em relação às alternativas existentes.

Além disso, para a utilização da carteira eletrônica pelos usuários, são importantes três fatores: segurança, conveniência e a integração entre os bancos e as operadoras. O sistema tem ainda que lidar com a inexistência de padrões (*standards*) da tecnologia e dos serviços nesta área, resultando em uma falta de interoperabilidade nos sistemas atuais.

Levando-se em consideração a tecnologia em evolução, a inovação dos meios de pagamento e a necessidade de um padrão de protocolo e sistema, desenvolve-se nesta dissertação uma proposta para um sistema de pagamentos móveis. Essa proposta é apresentada a seguir, com alguns objetivos determinados para este trabalho.

1.4 *Proposta Deste Trabalho*

Esta dissertação apresenta o desenvolvimento de um protocolo de pagamentos móveis em conjunto com uma aplicação para a plataforma móvel Android, utilizada para realizar pagamentos com um *smartphone*. A finalidade desse desenvolvimento é definir a comunicação entre as partes dentro do protocolo e desenhar um prototipo das comunicações realizadas entre o protocolo e a aplicação.

Baseado na evolução dos pagamentos móveis mencionada nesta dissertação, é desenvolvido neste trabalho um sistema que integra o protocolo e a aplicação para o

usuário final realizar os pagamentos com seu dispositivo celular. Esse sistema é denominado nesta dissertação de Carteira Inteligente do inglês *Smart Wallet* (S-Wallet). O objetivo da S-Wallet é fornecer aos usuários de *smartphone* uma solução completa para os pagamentos *peer-to-peer* (P2P) e ponto de venda do inglês *Point of Sale* (POS).

A **S-Wallet** é composta por um protocolo de pagamentos móveis denominado neste trabalho de Pagamentos fáceis de forma inteligente do inglês **Smart Way for Easy Payments** (SWEP). Ela possui também uma conta na nuvem (*cloud computing*) [21] denominada **Conta S-Wallet** que estabelece o contato entre as instituições financeiras ou empresas de telecomunicações para a aquisição de créditos e de uma aplicação (App) para a plataforma Android.

Para cumprir com os requisitos de software e hardware que existem no mercado, estipulou-se alguns objetivos durante o desenvolvimento deste trabalho, para que fossem seguidos de forma a maximizar a qualidade do sistema S-Wallet. Os objetivos para o desenvolvimento da S-Wallet são:

- Desenvolver um protocolo que **maximize a eficiência na transferência** dos pagamentos móveis;
- **Facilitar o acesso** dos usuários aos pagamentos móveis;
- **Simplicidade:** o sistema deve possuir uma interface para aprendizado rápido, tornando a utilização fácil por parte dos usuários;
- **Interoperabilidade:** O sistema deve ter uma integração com outros meios de pagamentos digitais, assim como a integração com os meios de pagamento tradicionais. Ele também deve funcionar em qualquer marca de dispositivos eletrônicos;
- **Universalidade:** O sistema deve incluir a possibilidade de pagamentos de diferentes tipos, seja ele P2P, POS ou pagamentos *off-line*; e

- **Segurança:** o sistema deve apresentar um ambiente estável e seguro, fornecendo confiabilidade nas trocas de dados e segurança na execução dos pagamentos.

Além disso, são definidos alguns requisitos adicionais para o desenvolvimento do protocolo de pagamentos móveis e da aplicação para o sistema S-Wallet:

- **Privacidade:** o conteúdo das transações efetuadas pelo sistema S-Wallet deve ser privado, sem possibilidades de consultas públicas;
- **Anonimato:** os dados pessoais dos usuários devem permanecer seguros junto ao sistema S-Wallet, onde as transações são associadas a um identificador (ID);
- **Custo:** o custo da implantação do sistema S-Wallet deve ser minimizado, de maneira que os pagamentos móveis se disseminem no mercado; e
- **Rapidez:** O pagamento móvel deve ser pelo menos tão rápido quanto os meios de pagamento tradicionais.

1.5 *Estrutura da Dissertação*

Esta dissertação é composta por 7 capítulos.

Este capítulo apresenta os pagamentos móveis, a motivação, a proposta e a estrutura desta dissertação.

O Capítulo 2 descreve todas as tecnologias que se comportam do mesmo modo que a *Near Field Communication* (NFC), mas com suas características. São apresentadas as tecnologias do código de barras, as bandas magnéticas, os *smart cards*, terminando com uma análise da tecnologia escolhida para realizar este trabalho, NFC.

O Capítulo 3 apresenta os modos de operação, a topologia e a comunicação, a codificação e a modulação, a prevenção de colisão, o fluxo geral do protocolo, os aspectos de segurança e a aplicabilidade da comunicação por proximidade de campo.

O Capítulo 4 mostra as principais características do sistema S-Wallet, a estrutura desenvolvida para esse sistema, com as explicações sobre a conta S-Wallet, as operações e as comunicações que ocorrem no fluxo do pagamento móvel e o protocolo SWEP. Finalmente, é apresentada a App S-Wallet.

O Capítulo 5 descreve a desenvolvimento do sistema S-Wallet e do protocolo SWEP e algumas considerações sobre as funcionalidades desse sistema.

O Capítulo 6 apresenta os resultados obtidos nos testes realizados utilizando o sistema S-Wallet para verificar o desempenho, a integração e a qualidade desse sistema. Também são apresentados os custos com hardware para o desenvolvimento do sistema S-Wallet.

Finalmente, o capítulo 7 apresenta as conclusões e as contribuições deste trabalho e os trabalhos futuros que poderão ser realizados a partir desta dissertação.

1.6 Considerações Finais Deste Capítulo

Este capítulo apresentou os pagamentos móveis, a motivação, a proposta e a estrutura desta dissertação.

O próximo capítulo descreve todas as tecnologias que se comportam do mesmo modo que a *Near Field Communication* (NFC), mas com suas características. São apresentadas as tecnologias do código de barras, as bandas magnéticas, os *smart cards*, terminando com uma análise da tecnologia escolhida para realizar este trabalho, NFC.

Capítulo 2

TECNOLOGIAS ATUAIS

2.1 *Introdução*

Este capítulo apresenta a evolução das tecnologias utilizadas nas transações de pagamentos e que se comportam de alguma maneira do mesmo modo que o *Near Field Communication* (NFC) e suas respectivas características. São apresentadas as tecnologias do código de barras, as bandas magnéticas, os *smart cards*, terminando com uma análise da tecnologia escolhida para realizar este trabalho, NFC. Embora cada tecnologia seja distinta, tanto na forma de funcionamento quanto na sua capacidade de transferência e armazenamento de dados, a maioria delas atualmente é utilizada como meio de pagamento ou em programas de fidelização. Por outro lado, a identificação por radiofrequência (RFID) é estudada nesta dissertação por ser uma tecnologia em que se baseia o NFC, em vez de a sua utilização como auxílio a projetos de meio de pagamento.

2.2 *Código de Barras*

O código de barras é uma tecnologia que apareceu na década de 40 nos EUA, quando alguns comerciantes solicitaram o desenvolvimento de um sistema que pudesse efetuar a leitura dos produtos no caixa automaticamente. Tradicionalmente, os códigos de barras armazenam dados na forma de linhas paralelas em diferentes larguras, e são conhecidos por código de barras 1D. Estes códigos podem apenas codificar números e podem variar em largura (intensidade) [43]. Existem vários padrões (*standards*) de códigos de barras, embora apenas alguns sejam utilizados de uma forma global. Desde a

sua primeira utilização há 30 anos, os códigos de barras servem a quase todo tipo de aplicação.

A Figura 2.1 mostra três variações de largura (intensidade) de códigos de barras 1D para dois padrões.



Figura 2-1 - Três variações de intensidade de códigos de barra.

A informação armazenada em um código de barras é lida por um leitor que reconhece por meio de um detector de fotocélula, quando a luz que emite foi refletida. Esta luz é depois convertida em um sinal elétrico, possibilitando a identificação da informação que o código de barras armazena [23].

As vantagens e desvantagens dos código de barras 1D são:

- **Vantagens:**
 - A informação é representada em um formato visual;
 - Baixo custo;
 - O processo de criação de um código de barras é rápido e fácil;

- A informação é facilmente armazenada, transferida, processada e validada, sem recorrer a um teclado; e
- Ajuda a eliminar o erro humano;

- **Desvantagens:**

- Sujeito a deterioração ou erros de impressão, levando a erros de leitura; e
- Toda a computação é realizada do lado do leitor (esses códigos apenas fornecem um identificador (ID) que permite acessar a informação do item que está armazenada na base de dados do lado leitor);

A sua forte dependência do processamento realizado no lado do leitor, que corresponde a 95% do controle sobre o sucesso ou o fracasso de uma aplicação que use códigos de barras 1D [24], bem como a necessidade de armazenar mais dados em um código de barras, levaram ao desenvolvimento dos códigos de barras 2D. Estes tipos de códigos permitem armazenar grandes quantidades de informação em pouco espaço, permitindo assim distribuir e detectar informação sem necessidade de acesso a uma base de dados por parte do leitor.

A Figura 2.2 mostra um exemplo de codificação de um código de barras 2D [67].



Figura 2-2 - Um exemplo de codificação de um código de barras 2D.

O código de barras 2D é utilizado principalmente nas comunicações móveis e seus dispositivos. Praticamente todos os celulares atuais possuem uma câmera fotográfica, que pode ser utilizada como leitor de código de barras 2D, tornando o uso global desse tipo de códigos de barras possível para praticamente qualquer pessoa.

2.3 *Tarja Magnética*

A tarja magnética não é uma tecnologia muito recente e tem estado presente desde os anos 60. Nessa década, essa tecnologia foi utilizada principalmente em redes de transportes públicos, primeiramente em Londres e em seguida em São Francisco [68]. Ela existe em uma grande variedade de aplicações, e é familiar a todas as pessoas: trata-se da tarja preta ou castanha existente na face traseira de muitos cartões utilizados hoje em dia. A Figura 2.3 mostra a tarja magnética aplicada a um cartão de plástico conforme o padrão.

Atualmente todas as entidades financeiras que recorrem a tecnologia da tarja magnética seguem o ISO/IEC 4909 [67], com a finalidade de garantir compatibilidade a

nível mundial. Além das entidades financeiras, as entidades relacionadas com transportes são também grandes consumidores dessa tarja.

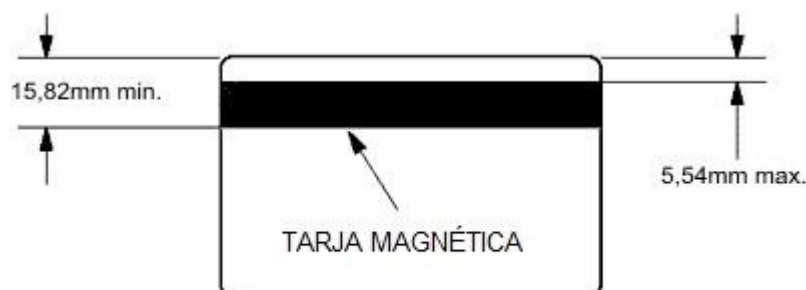


Figura 2-3 – Tarja magnética aplicada a um cartão de plástico, conforme o padrão.

A tecnologia da tarja magnética apresenta desvantagens em face a outras tecnologias que têm surgido. No entanto, a criação de um padrão para a alta coercibilidade, ou seja, a capacidade de um elemento em resistir a reorientação de suas partículas, aliada às técnicas de segurança vieram fornecer um novo alento a essa tecnologia. Assim, é pouco provável que a tecnologia da tarja magnética se torne obsoleta nos próximos 10 anos.

Por exemplo, a tarja magnética permite armazenar e modificar dados associados a um cartão de crédito. Esses dados são gravados no cartão por meio da modificação das pequenas partículas de ferro, que existem na tarja magnética. Essas tarjas são lidas por meio do contato direto com o leitor, e são passadas por uma cabeça de leitura.

As vantagens e desvantagens da tarja magnética são [48]:

- **Vantagens:**

- Os dados podem ser modificados ou reescritos;
- Alta capacidade de dados comparativamente com os códigos de barras;
- Segurança adicional por não ser um formato humanamente legível;
- Imune a contaminação por sujeira, água, etc;
- Fisicamente robusta;
- Padrões bem definidos; e
- Custo extremamente baixo.

- **Desvantagens**

- Não funciona à distância, necessitando de contato com o leitor;
- Sujeita a deterioração devido ao movimento de passagem pelos leitores;
- Os dados podem ser danificados por proximidade com campos magnéticos; e
- O fato de não ser um formato humanamente legível pode ser um empecilho em algumas aplicações (por exemplo, não é possível efetuar qualquer transação com um cartão de tarja magnético sem o respectivo sistema de leitura).

2.4 Identificação por Radiofrequência (RFID)

A identificação por radiofrequência (RFID), do inglês *Radio Frequency Identification*, vem se desenvolvendo cada vez mais nas últimas décadas pelas vantagens e aplicações quase ilimitadas que apresenta. Essa tecnologia tem se tornado parte integrante do cotidiano das pessoas e está presente nas mais variadas áreas. A RFID aumenta a conveniência e a produtividade e por essa razão é aplicada à prevenção de roubos, ao pagamento de pedágios em estradas, à gestão de tráfego, ao controle de acessos para pessoas e automóveis, à gestão de bens, à monitoração de produtos em armazéns e lojas e muitas outras situações.

Tendo como base tecnologias como os sinais de rádio de onda contínua e os radares, a identificação por radiofrequência resultou de um projeto desenvolvido pelos aliados na Segunda Guerra Mundial [28].

O conceito adjacente a RFID permite dois modos distintos: as etiquetas RFID se ativam quando recebem um sinal e o refletem (modo passivo) ou emitem um sinal próprio (modo ativo).

Existem diferentes métodos para identificar objetos por meio de RFID, mas o mais comum é armazenar um identificador unívoco (número de série) que permita identificar o produto, e talvez outra informação, em um circuito integrado que está ligado a uma antena [29]. Um sistema RFID é constituído pela antena, pelos emissores/receptores equipados com decodificadores e por etiquetas. Cada etiqueta é programada com a informação que identifica o objeto.

A tecnologia RFID apresenta vantagens e desvantagens:

- **Vantagens:**

- Possibilidade de etiquetar cada item univocamente com informação relativa ao mesmo;
- A informação de cada item pode ser apenas de leitura (*read-only*) ou de leitura e escrita (*read-write*);
- Possibilidade de identificar o objeto no sistema sem necessidade de contato, podendo esse ser identificado a alguns metros de distância (esta depende da especificação utilizada); e
- Possibilidade de saber onde está um determinado objeto dentro do sistema, desde que este esteja ao alcance dos leitores/scanners do sistema.

- **Desvantagens:**

- Os sinais de dois leitores podem interferir um no outro, não permitindo que as etiquetas respondam efetivamente aos dois pedidos de leitura;
- Se existirem muitas etiquetas em uma área, pode se tornar complicado para os leitores lerem todas as etiquetas. Este problema pode ser contornado lendo uma etiqueta de cada vez; e
- As etiquetas contêm informação estática, assim toda a manipulação de informação em um sistema RFID é realizada ao lado dos leitores.

Existem três tipos de etiquetas RFID: as ativas, as passivas e as semi passivas. Desses três tipos, apenas as etiquetas ativas e as passivas apresentam diferenças relevantes. As semi passivas, como o próprio nome indica, são apenas uma variação das etiquetas passivas. A diferença entre elas é que as ativas recorrem à energia da sua bateria interna para enviar as ondas de rádio. As semi passivas apresentam determinadas vantagens e desvantagens de acordo com a aplicação. O principal fator em que as etiquetas diferem é na forma como recebem a energia.

As etiquetas ativas têm uma fonte própria de energia que as alimenta continuamente (mesmo quando se encontram fora do alcance dos leitores). Tal fato permite não só que a etiqueta receba sinais com intensidades muito baixas, mas ainda que esta responda ao leitor com um sinal de intensidade alta a partir da sua própria fonte de energia. Esta capacidade permite ainda que as etiquetas ativas tenham um alcance muito grande (100 metros ou mais).

Ao contrário das etiquetas ativas, as etiquetas passivas não têm uma fonte de energia própria. Essas obtêm a energia necessária para seu funcionamento a partir da

energia que é transmitida do leitor para elas por meio de radiofrequência (RF). Essas etiquetas podem refletir o sinal que recebem do leitor ou então absorver uma pequena quantidade de energia que lhes permita enviar uma resposta rápida posteriormente. Em ambos os modos, a etiqueta necessita de receber sinais de elevada intensidade do leitor e responder com uma mensagem cuja intensidade do sinal é fraca, o que limita o alcance das mesmas a 3 metros ou menos (dependendo da frequência e do fornecedor pode mesmo chegar apenas a alcançar poucos centímetros). As principais características para isso ocorrer são: para que a etiqueta possa se ativar e possa enviar a resposta, é necessário que se encontrem não somente ao alcance dos leitores, mas que esteja próxima o suficiente para que alguma energia seja fornecida a ela.

A Tabela 2.1 apresenta as várias características de cada tipo de etiqueta, que devem ser consideradas quando se pretende instalar um sistema RFID.

Tabela 2-1 – Diferenças técnicas e funcionais entre as tecnologias de RFID ativa e passiva [30].

	Ativo	Passivo
Fonte de energia da etiqueta	Interna à etiqueta	Energia transferida a partir do leitor via RF.
Bateria	Sim	Não
Disponibilidade da energia	Contínua	Apenas no campo de alcance do leitor.
Força do sinal necessária (leitor -> etiqueta)	Baixa	Alta (tem de ser suficiente para fornecer energia à etiqueta)
Força do sinal criado (etiqueta -> leitor)	Alta	Baixa
Alcance de comunicação	Longo alcance (100 metros ou mais)	Curto alcance (3 metros ou menos).
Leitura multi-etiqueta	Um único leitor lê milhares de etiquetas em um raio de várias dezenas de metros.	Um único leitor lê centenas de etiquetas em um raio de 3 metros.
Armazenamento de dados	Grande capacidade de armazenamento	Pequena capacidade de armazenamento

2.5 *Smart Cards*

Smart card é uma tecnologia que foi introduzida na Europa há pouco mais de uma década e que nasceu de uma “parceria” entre a Motorola e uma empresa de computadores francesa, a Bull. Essa nova tecnologia trouxe as seguintes vantagens: o aumento substancial de conveniência e segurança em uma transação; o armazenamento selado de dados de identidade; o aumento de segurança de um sistema, assegurando privacidade aos dados importantes e evitando ataques ao sistema. Atualmente, os *smart cards* são utilizados em uma grande variedade de aplicações, tais como [31]:

- **Cartão de crédito** – crédito estendido eletronicamente para efetuar compras;
- **Cartão de débito** – permite aos utilizadores efetuarem pagamentos ou sacarem dinheiro, tipicamente em um ponto de venda, em um caixa ATM, ou por meio de um PIN;
- **Cartão de valor armazenado** – o passo inicial para uma sociedade sem dinheiro “vivo”. Um valor fixo é colocado eletronicamente no cartão. Por meio de um leitor apropriado os comerciantes podem deduzir o valor do cartão. Estes cartões podem ser recarregáveis ou descartáveis, ficando inutilizados quando o seu valor chega a zero;
- **Cartão para gestão de informação** – contém informação pessoal (dados médicos do utilizador, ...); e
- **Cartão de fidelização** – acumula pontos ou crédito de forma a proporcionar algum tipo de recompensa ao utilizador (descontos, produtos, serviços, ...).

Smart cards consistem em um cartão de plástico com circuito integrado (IC) incorporado. O IC pode ser um micro controlador (CPU/MPU) com um chip de memória interna e controlado por um Sistema Operativo, ou apenas um chip de

memória com lógica não-programável. O cartão com microprocessador permite adicionar, apagar e manipular a informação que armazena, enquanto o cartão só com um chip de memória (por exemplo, os cartões de telefone pré-pagos) apenas pode efetuar operações pré-definidas [32].

A capacidade de processamento e execução de operações pré-definidas sobre a informação que armazenam e a grande capacidade de armazenamento são características que tornam a utilização dos *smart cards* vantajosa. No entanto, são os seus elevados níveis de segurança e privacidade que servem como justificativa para o uso acentuado dessa tecnologia cada vez mais.

Uma das características mais importantes dos *smart cards*, quando associada à capacidade de manipulação dos dados que armazenam, é a capacidade desses cartões poderem ser utilizados em uma ampla variedade de aplicações. De fato, um único *smart card* pode funcionar como cartão de crédito, cartão de débito, cartão de condução, cartão de acesso, cartão de saúde e cartão de fidelização. Tudo isso com os mecanismos de segurança dos *smart cards* individuais para cada uma dessas aplicações.

Uma das principais diferenças nos *smart cards*, além de terem ou não um micro controlador, reside nos mecanismos de comunicação: podem ser de contato ou sem contato (*contactless*). Estes últimos, à semelhança das etiquetas RFID passivas, não possuem uma fonte de energia própria. A energia que necessitam para funcionar é retirada do campo magnético que se gera quando está na proximidade de um leitor compatível.

2.5.1 ISO/IEC 7816

O padrão ISO/IEC 7816 [33] é uma extensão do ISO/IEC 7810 que define 4 formatos para as características físicas dos cartões de identificação. O ISO 7816 é

constituído por quinze partes que especificam aspectos como as características físicas, aspectos de segurança e comandos de comunicação dos *smart cards*. O ISO/IEC 7816-4 é importante para este trabalho pois é ele que especifica a organização, a segurança e os comandos para a troca de dados.

No ISO/IEC 7816-4 a comunicação é realizada por meio de comandos *Application Protocol Data Units* (APDU), que podem conter um comando ou uma resposta. Um comando APDU está dividido em um cabeçalho mandatório e em um corpo opcional. As Tabelas 2.2 e 2.3 mostram a estrutura de um comando APDU e descrevem cada um dos seus parâmetros, respectivamente.

Tabela 2-2 – Estrutura de um comando APDU [33].

Comando APDU						
Cabeçalho (mandatório)				Corpo (opcional)		
CLA	INS	P1	P2	[Campo Lc]	[Campo Dados]	[Campo Le]

Tabela 2-3 – Especificação de um comando APDU [33].

Código	Nome	# 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.
[Campo Lc]	Comprimento	Igual o	Número de bytes presentes em [Campo

		Lc	Dados]
[Campo Dados]	Dados	Igual ao Lc	Array de bytes com dados do comando
[Campo Le]	Comprimento	De 1 a 3	Máximo bytes no [Campo Dados] na resposta APDU

A Tabela 2.4 mostra a estrutura de uma resposta. Estas mensagens são respostas a mensagens de comando.

Tabela 2-4 – Estrutura de uma resposta APDU [12].

Resposta APDU		
Corpo (opcional)	Trailer (mandatório)	
[Campo Dados]	SW1	SW2

A Tabela 2.5 descreve cada um dos parâmetros das mensagens do APDU.

Tabela 2-5 – Especificações de uma resposta APDU [12]

Código	Nome	#Bytes	Descrição
[Campo Dados]	Dados	Variável	Array de bytes com dados de resposta
SW1	Estado 1	1	Estado de processamento do comando
SW2	Estado 2	1	Qualificador do processamento do comando

A Figura 2.4 ilustra os códigos de resposta devolvidos a um comando APDU.

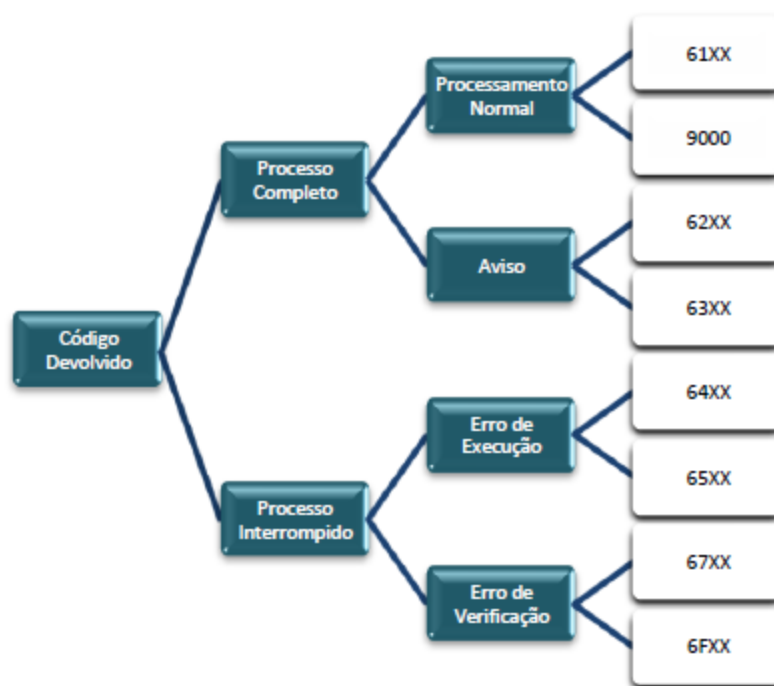


Figura 2-4 – Códigos devolvidos por uma resposta APDU [34].

2.5.2 ISO/IEC 14443

O ISO 14443 é o padrão internacional para cartões de identificação, cartões de circuito(s) integrado(s) sem contato e cartões de proximidade. Finalizado em 2001, este padrão foi criado inicialmente para dinheiro e bilhetes eletrônicos [35]. No entanto, ele serve atualmente como padrão para cartões de identificação sem contato.

O ISO 14443 opera a uma frequência de 13,56 MHz e suporta dois protocolos de comunicação: tipo A e tipo B. A frequência de operação escolhida para esse padrão é considerada a mais apropriada para um acoplamento indutivo de proximidade eficiente, ela é compatível com a regulação *Eletromagnetic Compatibility* (EMC). Essa frequência se encontra alocada para uma banda *Industrial, Scientific and Medical* (ISM) e apresenta uma baixa absorção pelos tecidos humanos.

Atualmente, é exigido por parte das entidades que controlam o padrão ISO 14443 total compatibilidade com as 4 partes desse, como mostrado na Tabela 2.6, tanto nos leitores *Proximity Coupling Device* (PCD) como nos cartões *Proximity Integrated Circuit Cards* (PICC). Assim, o ISO 14443 é suportado por praticamente todos os fornecedores de *smart cards*: VISA e Mastercard incluíram nas suas especificações para identificação sem contato (*contactless*).

Tabela 2-6 – Partes constituintes da especificação do padrão ISO/IEC 14443.

Parte 1	Características físicas
Parte 2	Intensidade da radiofrequência e interface do sinal
Parte 3	Inicialização e anti-colisão
Parte 4	Protocolos de transmissão

O ISO 14443 define um protocolo que suporta a transmissão de dados confiáveis e sem erros por meio de múltiplos cartões, mas não define o conteúdo dos dados. Uma vantagem desse padrão é a compatibilidade com padrões anteriores como o ISO 7816-4, preservando assim o investimento prévio realizado nos *smart cards*.

2.6 MiFare

MiFare é o padrão *open-source* criado pela Philips e regularizado pela NXP Semiconductors que lidera a indústria para transações em *smart cards contactless* [36]. Esse padrão nada mais é do que um protocolo de codificação/autenticação a ser utilizado em *smart cards contactless*, de acordo com as especificações do ISO/IEC 14443 - tipo A. A "Arsenal Research", (Instituto de Certificação MiFare independente) garante que aplicações certificadas de diferentes vendedores são compatíveis entre si. O

padrão MiFare é considerado um padrão de fato para a indústria e é atualmente utilizado como base de comparação para novos padrões. A plataforma de interface MiFare consiste em uma família de seis produtos [15]:

- MiFare classic - circuitos integrados (IC) que utilizam o protocolo de comunicação MiFare (padrão MiFare 1K e 4K);
- MiFare ultralight - desenhados para serem baratos e caberem em um bilhete de papel. Apresentam uma alternativa para os bilhetes atuais de banda-magnética;
- Controladores dupla interface - inclui o MiFare PRO e o MiFare PROX, que fornecem flexibilidade e segurança para suportarem múltiplas aplicações em um único cartão com IC;
- MiFare DESFire8 - primeiro IC *contactless* a suportar *Standard de Codificação Avançado* (AES) assim como métodos de codificação mais comuns como o DES ou o 3DES; e
- Componentes de leitura - leitores e kits de avaliação em conformidade com os *padrões contactless* tais como o ISO/IEC 14443 A/B e o ISO/IEC 15693.

2.7 **MiFare classic**

Existem dois ICs MiFare classic diferentes no mercado, o MF1 IC S50 (MiFare 1k) [37] e o MF1 IC S70 (MiFare 4K) [17]. Ambos os ICs diferem-se apenas na memória.

Um cartão MiFare Classic consiste em um cartão de plástico com as medidas especificadas pelo ISO/IEC 7810 de tipo ID-1 [68], com uma antena e com um chip encapsulados. Pode-se observar na Figura 2.5, o chip é constituído pela interface RF, pela Unidade de Controle Digital e pela memória (EEPROM) [16]. Os dados e a energia

são transferidos via antena. A antena consiste em uma bobina com 4 voltas diretamente ligada ao chip.

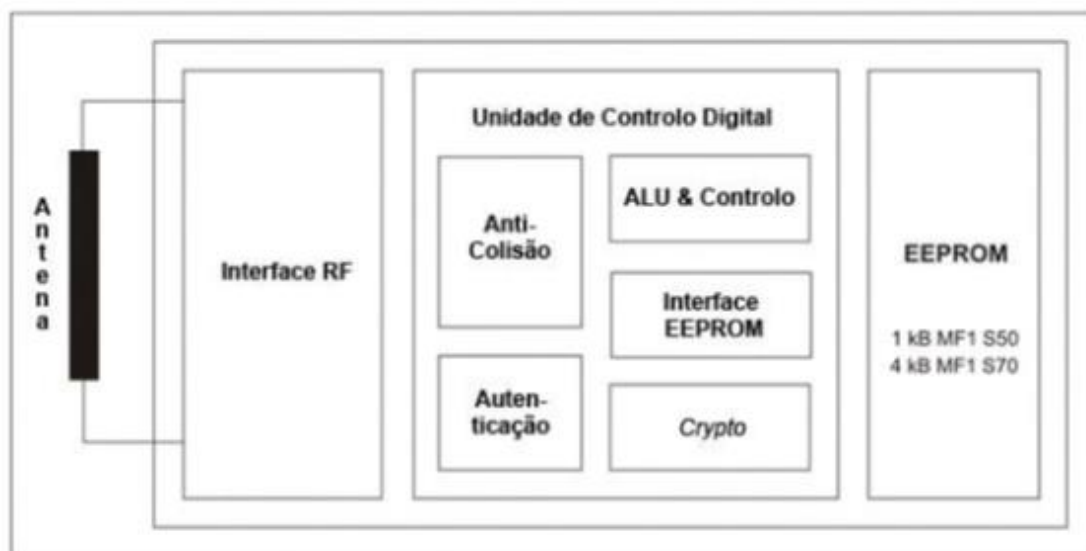


Figura 2-5 – Estrutura do IC com um cartão MiFare

A seguir descreve-se cada um dos componentes que constituem um cartão MiFare Classic.

2.7.1 Interface de radiofrequência.

A interface de radiofrequência de um chip MiFare Classic está de acordo com a ISO/IEC 14443 (Tipo A) [35] como mostrado na Tabela 2.7.

Tabela 2-7 - Principais características de acordo com a ISO 14443-tipo A.

Frequência	13,56 MHz
Alcance leitura/escrita	<=10 cm
Velocidade comunicação	106 Kbps (fase de anti-colisão) 212 Kbps ou mais (opcional)

2.7.2 Organização da memória.

Como foi citado no subitem 2.7.1 deste capítulo, os chips MiFare MF1 IC S50 e MF1 IC S70 diferem apenas na memória. O MF1 IC S50 tem uma memória de 1 k organizada da seguinte forma [16]:

- 16 setores;
- Cada setor contém 4 blocos; e
- Cada bloco tem 16 bytes.

O chip MF1 IC S70 tem uma memória de 4 k organizada da seguinte forma [38]:

- 40 setores;
- 32 setores com 4 blocos;
- 8 setores com 16 blocos; e
- Cada bloco tem 16 bytes.

Existem 3 tipos diferentes de blocos no chip MF1 IC S50 e MF1 IC S70:

- Bloco de fabricante (*manufacturer*): trata-se do primeiro bloco do primeiro setor e contém a informação a respeito do fabricante do IC. Quando é produzido esse bloco fica protegido contra gravação após a sua escrita quando é produzido. Os primeiros quatro bytes do bloco contêm o número de série;
- Setor *trailer*: o setor *trailer* consiste em 16 bits de acesso. Os bits de acesso 6,7 e 8 especificam o tipo de dados dos blocos e as condições de acesso aos blocos do setor. O bit 9 está disponível para dados de utilização. As chaves de acesso necessárias para garantir o acesso aos blocos do setor estão armazenadas nos bits

0 a 5 (chave A) e nos bits 10 a 15 (chave B). Se não é necessária a chave B, esses últimos bits podem ser utilizados para armazenar outros dados; e

- Blocos de dados: os blocos de dados podem ser blocos de escrita/leitura ou blocos *value*. Os primeiros são utilizados para aplicações do género de controle de acesso e os blocos *value* são utilizados quando é necessário efetuar operações aritméticas nos valores armazenados (por exemplo, crédito ou pontos de um cartão de fidelização). Em um bloco de dados, o valor é armazenado três vezes (4 bits a cada vez) e o endereço é armazenado quatro vezes (1 bit a cada vez). Por razões de segurança, o valor é armazenado de forma inversa.

2.7.3 Unidade de Controle Digital

A Unidade de Controle Digital do MiFare Classic é constituída de:

- Anti-colisão: método que permite que vários cartões no campo de alcance de um leitor possam ser selecionados e operados de forma sequencial. Esse método está de acordo com o ISO/IEC 14443-3 [35];
- Autenticação: cada bloco de memória está protegido com duas chaves. Esses blocos só podem ser acessados se o processo de autenticação que utiliza as suas duas chaves é efetuado com sucesso;
- Unidade lógica aritmética, do inglês *Arithmetic Logic Unit* (ALU) e Controle: os dados são armazenados de forma redundante e podem ser incrementados ou decrementados;
- Interface EEPROM: fornece acesso a EEPROM; e
- Unidade Crypto (Unidade de Criptografia): a unidade de controlo utiliza uma cifra STREAM1.

2.8 *FeliCa*

Desenvolvido pela SONY, FeliCa é, assim como o MiFare, um padrão para IC contactless. Esse padrão foi adotado em larga escala em muitos países asiáticos, principalmente em áreas como bilheteria de transportes e sistemas de pagamento eletrônico. De fato, o FeliCa pode mesmo ser visto como o equivalente asiático ao europeu MiFare. Esse padrão recorre a um protocolo de comunicação proprietário e é compatível com 212 Kbps, modo de comunicação passivo do ISO 18092 [48].

2.9 *Considerações finais deste capítulo*

Este capítulo apresentou todas as tecnologias que se comportam do mesmo modo que o NFC, e suas características. Foram analisadas as tecnologias do código de barras, as bandas magnéticas, os *smart cards*, terminando com uma análise da tecnologia escolhida para realizar este trabalho, NFC.

Embora cada tecnologia seja distinta, tanto na forma como funciona quanto na sua capacidade, a maioria delas atualmente é utilizada como meio de pagamento ou em programas de fidelização. A identificação por radiofrequência (RFID) foi estudada por ser uma tecnologia em que se baseia o NFC, e não devido a sua utilização como auxílio a projetos de meio de pagamento.

O próximo capítulo apresenta a tecnologia da comunicação por proximidade de campo (NFC). É realizada uma pequena introdução sobre os modos de operação da NFC, sua topologia de comunicação, aspectos de codificação e modulação, prevenção de colisão, fluxo geral do protocolo, aspectos de segurança e aplicabilidade.

Capítulo 3

COMUNICAÇÃO POR PROXIMIDADE DE CAMPO

3.1 Introdução

A comunicação por proximidade de campo do inglês *Near Field Communication* (NFC) é também uma tecnologia de radiofrequência, mas diferencia-se pela distância de operação, normalmente de 0 a 20 cm entre os dispositivos.

A NFC é uma tecnologia que evoluiu da combinação de outras tecnologias de comunicação e identificação sem contato que facilita a conectividade entre os dispositivos eletrônicos. A comunicação por proximidade de campo permite interações bidirecionais de forma simples e segura entre os dispositivos eletrônicos, permitindo assim aos consumidores efetuarem de forma segura transações sem contato, acessarem o conteúdo digital e conectar dispositivos com um simples toque [39].

Essa tecnologia móvel vem assim aumentar o conforto, a segurança e a rapidez em inúmeros processos tais como pagamentos sem dinheiro físico, compra de bilhetes por meio do celular a qualquer hora e em qualquer lugar, melhores esquemas de fidelização com cupons, vouchers e cartões sempre no seu celular e muitos outros.

A NFC resultou de um esforço inicial da Royal Philips Electronics e da Sony Corporation [42]. Em 2004 essas empresas formaram o NFC Forum para promover a implementação e a definição como padrão da tecnologia NFC para garantir a interoperabilidade entre os dispositivos e os serviços. O NFC Forum tem nesse

momento cerca de 130 membros e continua a ser a entidade de referência no universo em expansão da NFC.

O princípio da NFC é tornar a comunicação entre os dispositivos mais simples: basta aproximá-los para que isso ocorra, eliminando a necessidade de procedimentos eventualmente complexos. Pelo fato da distância de operação ser curta, a comunicação é inerentemente segura no que diz respeito as tentativas de interceptação. Caso ocorra necessidade de coibir esse tipo de ação, as medidas usuais de segurança devem ser implementadas no protocolo de rede e/ou da aplicação [40].

A tecnologia NFC pode ser utilizada essencialmente para dois propósitos:

- **Transmissão de pequena quantidade de dados:** como a finalidade da NFC não é prover grandes velocidades, mas sim uma comunicação segura a curta distância, a mesma não é adequada para a transmissão de grandes volumes de dados. Dessa forma, dados como informações de pagamento, cartões de visita, autenticação, são os mais indicados para as transferências exclusivamente pela NFC; e
- **Iniciador de comunicação secundária:** fazendo com que dois dispositivos se reconheçam pela simples aproximação, a NFC pode ser utilizada para disparar um canal de comunicação secundário, como o *Bluetooth* ou o *WiFi*.

A especificação NFC prevê ainda que a tecnologia seja compatível com os dispositivos de Identificação por Radiofrequência (RFID) do inglês *Radiofrequency IDentification*, que operam na mesma frequência e mesmos modos de operação (especialmente os passivos). Dessa maneira muitos dispositivos habilitados com a NFC são capazes de emular cartões com a tecnologia RFID ou mesmo etiquetas (tags) RFID.

Este capítulo apresenta os modos de operação, a topologia e a comunicação, a codificação e a modulação, a prevenção de colisão, o fluxo geral deste protocolo, os aspectos de segurança e a aplicabilidade da comunicação por proximidade de campo.

3.2 *Modos de operação*

A NFC é uma tecnologia de comunicação sem fio que opera na frequência de rádio de 13.56 MHz. Esta frequência é livre de restrições na maioria dos países. A comunicação por proximidade de campo tem uma distância de operação de 4 cm e suporta taxas de dados que variam entre 106 e 424 k bits/s.

Dois modos de operação estão disponíveis na tecnologia: ativo e passivo [40].

No modo de comunicação **ativo**, ambos os dispositivos são capazes de gerar seus sinais de radiofrequência para a comunicação. Normalmente são dispositivos dotados de fonte de energia própria, como a bateria ou a energia elétrica convencional. Os leitores NFC são exemplos de dispositivos ativos.

No modo de comunicação **passivo**, apenas um dispositivo (denominado iniciado) gera o sinal de radiofrequência para comunicação. Neste caso, um campo eletromagnético é gerado, e esse campo induz uma corrente elétrica no dispositivo passivo, que faz com que o mesmo tenha energia para funcionar pelo tempo em que estiver sob a ação do referido campo. Cartões NFC são exemplos de dispositivos passivos.

A Figura 3.1 mostra uma etiqueta RFID passiva colocada em um cartão de ônibus.

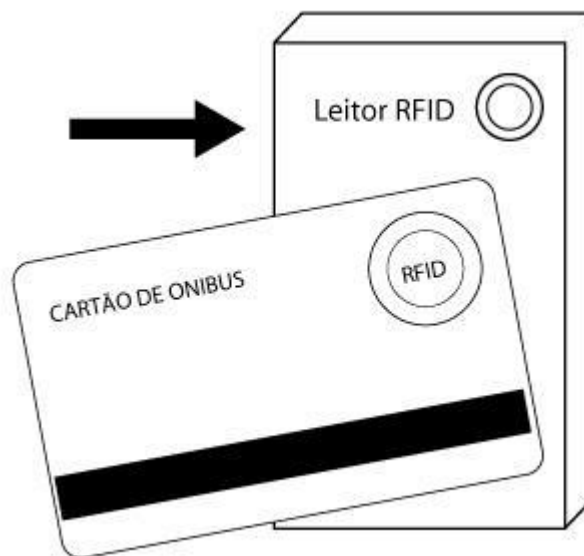


Figura 3-1 – Etiqueta RFID passiva colada em um cartão de ônibus.

3.3 *Topologia e Comunicação*

Na tecnologia NFC, o número de participantes na comunicação é limitado a dois, portanto utiliza-se um protocolo *peer-to-peer*. Pelo fato dos dispositivos compartilharem uma única banda de radiofrequência, a comunicação é *half-duplex*, ou seja, apenas um dispositivo transmite dados por vez.

A estratégia adotada na comunicação por proximidade de campo é conhecida como “ouça antes de se comunicar”, onde o dispositivo participante da comunicação deve primeiro ver se não tem ninguém transmitindo dados no momento e só então iniciar a sua comunicação.

3.4 *Codificação e Modulação*

Na NFC, a distinção entre um dispositivo ativo e um passivo especifica o modo em que os dados são transmitidos. Dispositivos passivos codificam os dados sempre com a codificação Manchester e a 10% *Amplitude-Shift Keying* (ASK) – uma forma de

modulação que representa os dados digitais com variações na amplitude de uma onda portadora) [43]. Por outro lado, para os dispositivos ativos há uma distinção entre a codificação Miller modificada com 100% de modulação se a taxa de dados é 106 kbps, e a codificação Manchester utilizando uma taxa de modulação de 10% se a taxa de dados é maior do que 106 kbps. Como será mostrado no item 3.4.1 deste capítulo a taxa de modulação, definida em [41] é de extrema importância para a segurança da transferência de dados da NFC.

A Tabela 3.1 mostra a codificação e a modulação em diferentes velocidades de transferências [41].

Tabela 3-1 - Codificação e modulação em diferentes velocidades de transferência [41]

	Dispositivo Ativo	Dispositivo Passivo
106 kBaud	Miller Modificado, 100% ASK	Manchester, 10% ASK
212 kBaud	Manchester, 10% ASK	Manchester, 10% ASK
424 kBaud	Manchester, 10% ASK	Manchester, 10% ASK

3.4.1 Código Manchester

A codificação Manchester depende de duas transições possíveis no ponto médio de um período. Uma transição de subida (*low-to-high*) expressa um bit 0, e uma transição de descida (*high-to-low*) representa o bit 1. Consequentemente, no meio de cada período de bit sempre existe uma transição. As transições no começo de um período não são consideradas.

A Figura 3.2 ilustra o código Manchester.

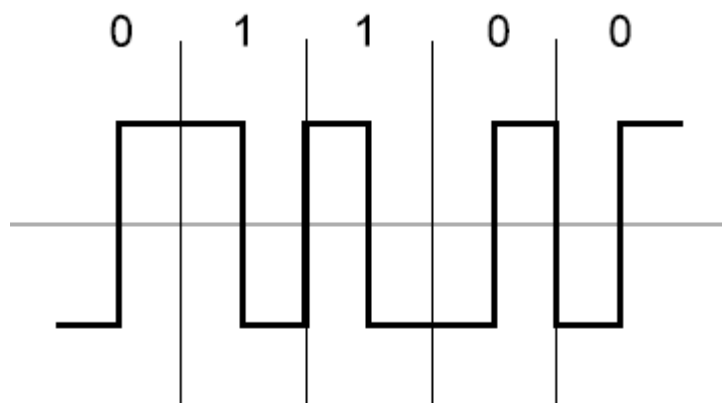


Figura 3-2 - Código Manchester.

3.4.2 Código Miller modificado

A linha de código Miller modificado é caracterizada por pausas na portadora em diferentes posições de um período. Dependendo da informação a ser transmitida, os bits são codificados como mostrado na Figura 3.3. O 1 é sempre codificado da mesma maneira e a codificação do 0 é determinada com base no bit anterior.

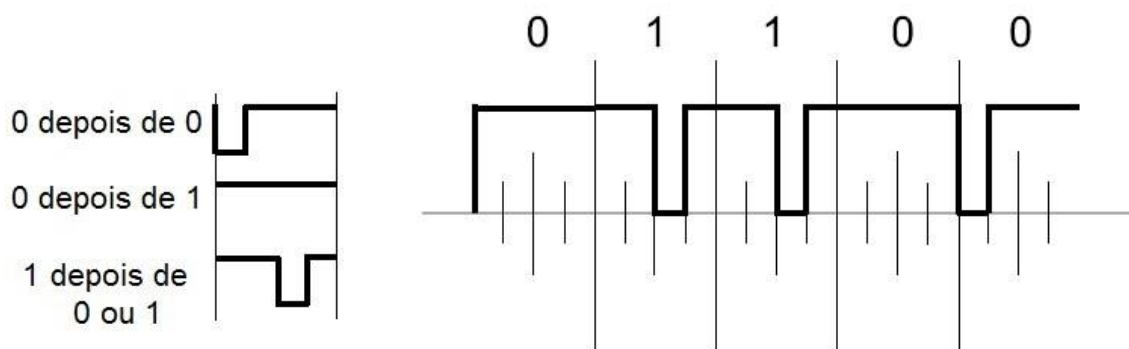


Figura 3-3 - Código Miller modificado.

3.5 Prevenção de Colisão

Geralmente funcionamentos incorretos são raros, uma vez que os dispositivos devem ser colocados em uma proximidade direta. O protocolo procede pelo princípio: escute, depois fale. Se o iniciador quer se comunicar, primeiro, ele deve ter certeza que não existe campos de RF externos com a finalidade de que não atrapalhe nenhuma outra comunicação NFC. Ele deve esperar silenciosamente enquanto outro campo RF é

detectado, antes de começar a comunicação, depois de um tempo de guarda definido precisamente [40].

Caso ocorra um caso em que dois ou mais alvos respondam ao mesmo tempo, a colisão é detectada pelo iniciador.

3.6 Fluxo Geral do protocolo

Como mostra a Figura 3.4 o fluxo geral do protocolo pode ser dividido em inicialização e protocolo de transporte. A inicialização compreende a prevenção de colisão e a seleção de alvos, onde o iniciador determina o modo de comunicação (ativo ou passivo) e escolhe a velocidade de transferência.

Como definido em [40], o protocolo de transporte é dividido em três partes:

- Ativação do protocolo, que inclui a *requisição de atributos* e a *seleção de parâmetros*;
- O *protocolo de troca de dados*, e
- A desativação do protocolo incluindo a *desmarcação e a liberação*.

Durante uma transação, o modo (ativo ou passivo) e o papel (iniciador ou alvo) não muda até que a comunicação seja finalizada. Entretanto, a velocidade de transferência de dados pode ser mudada por um procedimento de mudança de parâmetro. Mais informações podem ser obtidas em [40].

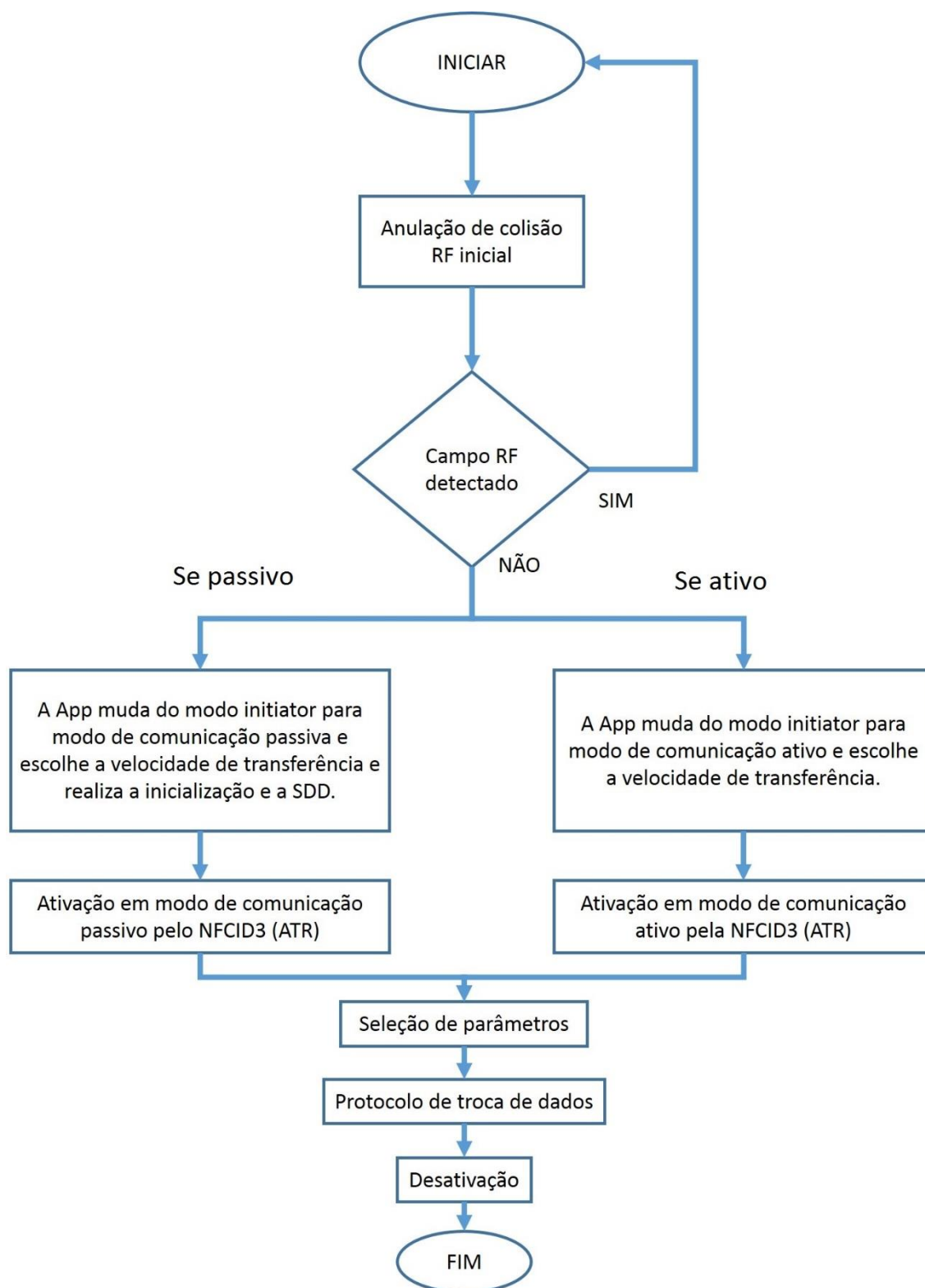


Figura 3-4 – Inicialização geral e protocolo de transporte

3.7 *Aspectos de Segurança*

Este item apresenta a segurança da NFC. Neste contexto dois artigos muito importantes foram publicados. Haselsteiner e Breitfuss [41] discutem algumas ameaças e soluções para a segurança da NFC. Em [42] esses mesmos autores apresentaram algumas informações úteis.

Primeiro deve ser mencionado que a pequena distância de comunicação de alguns centímetros, a qual requer uma interação consciente do usuário, não assegura realmente uma segurança na comunicação.

Existem diferentes possibilidades de ataque a tecnologia da comunicação por proximidade de campo. De um lado dispositivos diferentes podem ser manipulados fisicamente. Isso pode ocorrer pela remoção de uma etiqueta do item etiquetado ou envolver o dispositivo em uma folha de metal para bloquear o sinal RF. Outro aspecto é a violação de privacidade. Se a informação privada é armazenada em uma etiqueta, é importante prevenir a leitura não autorizada e o acesso a modificação. Como descrito em [42] etiquetas de leitura somente são seguras contra o acesso não autorizado. No caso das etiquetas regraváveis, tem-se que assumir que os invasores têm leitores móveis e software apropriado que possibilita a leitura não autorizada e o acesso à gravação se a distância do leitor é normal. Um dos objetivos deste trabalho é estudar os ataques com respeito a comunicação entre dois dispositivos.

Para a detecção de erros, a NFC utiliza a verificação cíclica redundante (CRC). Este método possibilita aos dispositivos verificarem se o dado recebido foi corrompido.

A seguir são considerados diferentes tipos de ataques possíveis à comunicação da NFC. Para muitos desses ataques, existem prevenções com a finalidade de que sejam evitados ou ao menos reduzidas as ameaças.

3.7.1 Escutas (*Eavesdropping*)

A NFC não oferece nenhuma proteção contra escutas entre as comunicações. As ondas RF para a transferência de dados sem fio por uma antena possibilitam invasores interceptarem os dados transmitidos pelo monitoramento do canal. Na prática, uma pessoa mal intencionada teria que manter uma longa distância com a finalidade de não ser notada, ou instalar um dispositivo nas proximidades da comunicação que efetuará a escuta.

A pequena distância entre o iniciador e o alvo para uma comunicação bem sucedida não é um problema significativo, uma vez que os invasores não estão vinculados pelos mesmos limites de transmissão. Consequentemente a distância máxima para uma sequência normal de leitura pode ser excedida. O questionamento do quão perto um invasor deve estar localizado para restabelecer um sinal RF utilizável é difícil de responder. Como listado em [65], isso vai depender do número de parâmetros, como:

- RF com características arquivadas do dispositivo de envio (isto é, a geometria da antena, o efeito do bloqueio do pacote, da placa de circuito impresso (PCB), do ambiente);
- Características da antena do invasor (isto é, a geometria da antena, a possibilidade de mudar a posição em todas as 3 dimensões);
- Qualidade do receptor do invasor;

- Qualidade do decodificador do sinal RF do invasor;
- Instalação da localização onde a invasão é realizada (por exemplo, as barreiras como paredes ou metais, o nível de ruído do piso); e
- Energia de saída do dispositivo NFC.

Além disso, a escuta é extremamente afetada pelo modo de comunicação. Isto ocorre pois, baseado no modo ativo ou passivo, a transferência de dados é codificada e modulada diferentemente. Se o dado é transferido com codificação Manchester a 10% ASK ele pode ser invadido facilmente. Assim, um dispositivo passivo, que não gera seu próprio campo RF é muito mais difícil de se interceptar, que um dispositivo ativo. Com a finalidade de deixar que o leitor suponha o risco resultante da escuta, existem algumas distâncias associadas a isso [65]: “Quando um dispositivo está enviando dados no modo ativo, a escuta pode ser efetuada em uma distância de até 10 m, enquanto que quando o dispositivo está no modo passivo, essa distância é reduzida significativamente para 1 metro.”

Entretanto, assume-se que essa invasão ocorre uma vez que o equipamento necessário está disponível para todo mundo. Equipado com uma antena, uma pessoa mal-intencionada que é capaz de monitorar passivamente o sinal RF, pode também extrair os dados em forma de um simples texto. Experimentos e a pesquisa na literatura podem ser usados para ganhar esse conhecimento necessário. Por isso, a confidencialidade da NFC não é garantida. Um canal seguro é a única solução para as aplicações que transmitem dados sensíveis. Em [43] são fornecidas informações mais detalhadas desse ataque.

3.7.2 Destruição de dados

Um invasor que deseja destruir dados, pretende corromper a comunicação. O efeito é que o serviço não fica disponível. Entretanto, o invasor não é capaz de gerar uma mensagem válida. Ao contrário da escuta (*eavesdropping*), esse não é um ataque passivo. Ele é relativamente fácil de realizar. Uma possibilidade de atrapalhar o sinal é a utilização do chamado “*RFID Jammer*”.

Não existem maneiras de prevenir a destruição de dados por um invasor, mas pode-se detectá-lo. Dispositivos NFC são capazes de receber e transmitir dados ao mesmo tempo. Isso significa que, eles podem conferir o campo de frequência de rádio e notar a colisão, podendo também tocar um alarme para avisar sobre intrusos.

3.7.3 Modificação dos dados

A modificação dos dados não autorizada, é muito mais complexa e demanda uma compreensão completa. Como será mostrado nesta seção, a modificação dos dados é possível apenas sob certas condições. Com a finalidade de modificar o dado transmitido, um invasor tem de se preocupar com os bits do sinal RF. Como mencionado anteriormente neste capítulo, os dados são enviados de diferentes maneiras. A viabilidade desse ataque, o que significa se é possível alterar um bit de valor 0 para 1 ou vice versa, está sujeita à intensidade da amplitude de modulação.

Se a codificação Miller com 100% da modulação é utilizada, é possível eliminar uma pausa do sinal RF, mas não se deve gerar pausa onde não existe pausa. Isso exige na antena receptora uma sobreposição exata impraticável do sinal dos invasores com o sinal original. Entretanto, a NFC utiliza codificação Manchester com modulação de 100% em conjunto com a codificação modificada de Miller o que leva a 4 casos possíveis, como mostrado na Figura 3.5. O único caso, onde um bit pode ser alterado

por um invasor é, onde um “1” é seguido de outro “1”. Ao preencher a pausa da mensagem com duas metades de bit vindas da mensagem do sinal RF, o decodificador fica livre para receber o sinal do terceiro caso, devido a esta pausa gerada. Conforme o bit precedente, o decodificador deve verificar um bit válido. Com isso os outros três casos não são susceptíveis a um ataque para modificação dos dados.

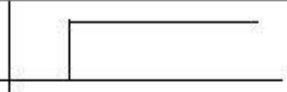
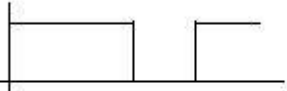
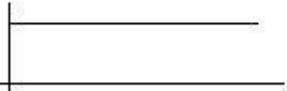
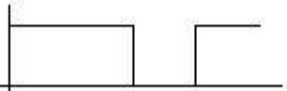
Bit x-1	Bit x		Modificação do Bit x p/	Possível ?
0	0		1	NÃO
0	1		0	NÃO
1	0		1	NÃO
1	1		0	SIM

Figura 3-5 – Modificação de bit da codificação de miller modificada

Para a comunicação por proximidade de campo, uma taxa de modulação ASK de 10% é sempre utilizada em conjunto com a codificação Manchester. Em contraste com a modulação 100%, onde realmente nenhum sinal é enviado durante uma pausa, aqui, em uma pausa o sinal RF é por exemplo 82% do nível do sinal total. Assume-se neste trabalho que sem ser notado pelo decodificador, um invasor possa aumentar o sinal RF existente em 18% durante toda a sessão. Assim, o invasor é capaz de modificar um 0 por 1 ao aumentar o sinal RF durante a primeira metade do período do sinal por outros 18%, e também pode mudar um bit de valor um para zero simplesmente parando de enviar qualquer coisa.

Resumindo, em relação à ameaça: exceto por um caso, apenas a codificação Manchester com 10% ASK é utilizada para a transferência dos dados na NFC. Isto

representa as melhores condições possíveis para as intenções de invasão e de modificação dos dados NFC como mostra a Tabela 3.1. Essa maneira de transmissão de dados oferece um ataque de modificação para todos os bits. A única exceção são os dispositivos ativos transferindo os dados a 106 Kbps. Neste caso a utilização da codificação Miller modificada com taxa de modulação de 100% garante que apenas alguns bits podem ser modificados.

Em [41] três contramedidas são descritas. Uma possibilidade é a utilização do modo de comunicação ativo com 106 Kbps. Como mencionado acima isso não previne, mas ao menos reduz o risco de um ataque. Além disso, é possível permitir que o dispositivo confira o campo RF como descrito na subseção 3.7.2 deste capítulo. Denominada como “provavelmente a melhor solução” é a utilização de um canal seguro. Isso fornece integridade dos dados.

3.7.4 Inserção de dados

Se existir tempo suficiente para enviar uma mensagem de inserção antes do dispositivo real iniciar seu envio de respostas, a inserção dos dados pode ser realizada apenas por um invasor. Se ocorre uma colisão, a troca de dados é interrompida de uma vez. Para prevenir esse ataque o dispositivo deve tentar responder sem atraso. Alternativamente, deve-se conferir novamente o campo RF e também o canal seguro pode ser utilizado como proteção contra ataques.

3.7.5 Man-in-the-middle-attack

Com a finalidade de mostrar que a NFC é segura contra ataques do tipo *Man-in-the-middle* é necessário examinar ambos os modos de comunicação, ativo e passivo. A seguir, distingue-se entre o dispositivo A e o dispositivo B que estão trocando dados.

No modo passivo o dispositivo ativo (A) gera o campo RF com a finalidade de enviar dados para o dispositivo passivo (B). O objetivo de um invasor é interceptar essa mensagem e prevenir o dispositivo B de recebê-la. O próximo passo é substituí-la por uma mensagem diferente. O primeiro passo, é possível, mas pode ser detectado se o dispositivo A verificar o campo RF enquanto envia a mensagem. Entretanto, o segundo passo é praticamente impossível. Para enviar uma mensagem para o dispositivo B o invasor, um dispositivo C, deveria gerar seu próprio campo RF. Por isso, o campo RF do dispositivo A tem que estar perfeitamente alinhado com o dispositivo B, tornando assim a prática de um dispositivo C enviar uma mensagem não ser praticamente realizável.

Em contraste com o modo passivo, no modo ativo o dispositivo A desliga o campo RF depois de enviar a mensagem. Assim o invasor depara-se com outro problema: mesmo que ele consiga gerar um campo RF, ele não é capaz de transferir uma mensagem como sendo o dispositivo B, pois este não será reconhecido pelo dispositivo A. O dispositivo A está esperando por uma resposta do dispositivo B com seu campo de RF específico. Assim, o dispositivo A é possui a tarefa de verificar se a mensagem recebida realmente veio do dispositivo B, conferindo sua identidade. Essa verificação de identidade, além do alinhamento dos campos de RF, acontece tanto em uma comunicação de A para B, quanto de B para A.

Desconsiderando os ataques de revezamento, a NFC fornece uma proteção boa contra o ataque *Man-in-the-middle*. Isto aplica-se particularmente se é utilizado o modo de comunicação ativo e o campo RF é monitorado pelo dispositivo A.

3.8 *Aplicabilidade*

O número de aplicações de média distância para a tecnologia NFC está crescendo continuamente, aparecendo em várias áreas da vida do ser humano. Especialmente as utilizações em conjunto com os celulares oferecem excelentes oportunidades. As principais aplicações são:

- Pagamento e e-ticket

A NFC habilita os usuários a realizarem compras rápidas e seguras, irem as compras com dinheiro eletrônico, e também para comprar, armazenar e utilizar tickets eletrônicos, de shows/eventos, de aviões, cartões de viagem, etc.;

- Chaves eletrônicas

Por exemplo, elas podem ser chaves do carro, chaves da casa/trabalho, etc.;

- Identificação

Além disso, a NFC torna possível a utilização de celulares ao invés de documentos de identificação. No Japão, por exemplo, a carteira de estudante pode ser armazenada no celular, isso permite aos estudantes registrarem-se eletronicamente em aulas, abrirem seus armários no campus, comprarem comida na cafeteria da universidade, pegarem livros emprestados, e até mesmo conseguirem descontos em cinemas locais, restaurantes e lojas;

- Receber e compartilhar informações

O dado armazenado em qualquer objeto etiquetado (por exemplo, uma caixa de DVD ou um pôster) pode ser acessado por celulares com a finalidade de baixar trailers de filmes, mapas de ruas, horários de ônibus, etc.; e

- Serviços de instalação

Para evitar processos de configuração complicados, a NFC pode ser utilizada para instalar outras tecnologias de longo alcance, como o *bluetooth* ou uma rede wireless.

Até o momento a conveniência da NFC é amplamente utilizada na Ásia, no Japão e na Coreia do Sul, onde pagar com um celular ou um cartão-NFC já faz parte da vida cotidiana desses povos. Em setembro de 2006, uma pesquisa previu que até o ano de 2013, em torno de 30% dos celulares no mundo (aproximadamente 450 milhões de celulares) estarão habilitados com a tecnologia da NFC [66].

3.9 *Considerações Finais deste Capítulo*

Este capítulo apresentou os modos de operação, a topologia e a comunicação, a codificação e a modulação, a prevenção de colisão, o fluxo geral do protocolo, os aspectos de segurança e a aplicabilidade da comunicação por proximidade de campo.

O próximo capítulo apresenta a arquitetura do sistema S-Wallet, com suas características, estrutura de operações e de comunicações e também informações sobre o protocolo SWEP e a app S-Wallet.

Capítulo 4

ARQUITETURA DO SISTEMA S-WALLET

4.1 *Introdução*

Atualmente, as compras efetuadas no varejo possibilitam várias formas de pagamento, como cartão de crédito, cartão de débito, cheques e dinheiro. Quando o cliente não possui em mãos essas formas de pagamento, isto dificulta a aquisição dos produtos ou até mesmo o pagamento de pequenas dívidas entre as pessoas. Além disso, a utilização de cartões e cheques leva a uma dependência dos varejistas quanto as instituições financeiras. Dependências que vão desde a disponibilidade do serviço até as taxas cobradas pela utilização dos mesmos.

O principal objetivo no desenvolvimento deste trabalho é possibilitar praticidade ao usuário final, por meio de um sistema que integre pagamentos financeiros entre os clientes e o varejo e também entre dois clientes quaisquer. Espera-se também fornecer confiabilidade, segurança e facilidade de uso, com o desenvolvimento de um protocolo para o fluxo de pagamentos financeiros.

Este capítulo mostra as principais características do sistema S-Wallet, a estrutura desenvolvida para esse sistema, com as explicações sobre a conta S-Wallet, as operações e as comunicações que ocorrem no fluxo do pagamento móvel e o protocolo SWEP. Finalmente, é apresentada a App S-Wallet.

4.2 *Principais Características do Sistema S-Wallet*

As principais características do sistema S-Wallet desenvolvido para pagamentos móveis foram criadas levando-se em consideração alguns estudos como [23,24,25]:

Usabilidade: o protocolo deve ser fácil de usar por qualquer pessoa que possua um *smartphone* compatível. Ele também deve transmitir confiabilidade que o pagamento irá ocorrer sem interrupção;

Realizar micro pagamentos: a maioria das transações de pagamento entre os clientes ou em pontos de venda de compra rápida é de pequenos valores, portanto o custo para o varejista deve ser mínimo para a utilização da tecnologia;

Segurança: tratando-se de somas financeiras, um sistema inseguro não é plenamente utilizado. A cadeia de fluxo de pagamento deve assegurar primeiro ao varejista que ele vai receber seus créditos em sua conta bancária, ao cliente que ele está realmente pagando pelo item desejado e que o devido valor foi debitado da sua conta; e

Privacidade: os clientes que utilizarem o sistema desejam que as características de suas compras permaneçam anônimas, eles querem que o banco e as operadoras de telecomunicações se mantenham apenas informadas dos valores e dos recibos. Informações relativas a localização (onde), produto (o que) e quem está comprando devem permanecer privadas.

4.3 *Estrutura do Sistema S-Wallet*

O Sistema **S-Wallet** é composto por um protocolo de pagamentos móveis denominado neste trabalho de Pagamentos Fáceis de Forma Inteligente do inglês *Smart Way for Easy Payments* (SWEP). Ele possui também uma conta na nuvem (*cloud computing*) – um servidor remoto - [26] denominada **Conta S-Wallet**, que estabelece o

contato entre as instituições financeiras ou empresas de telecomunicações para a aquisição de créditos e de uma aplicação (**App S-Wallet**) para a plataforma Android.

O sistema S-Wallet satisfaz as necessidades dos usuários tais como segurança, usabilidade e anonimato. Com o protocolo SWEP, as informações são criptografadas, a comunicação ocorre em conexões seguras e mediante a troca de certificados. Além disso, esse protocolo se baseia nas autenticações de senha, facial ou com QR-Code para a confirmação de registro e pagamento.

As entidades participantes do ciclo de pagamentos na estrutura da S-Wallet são: **Banco, Operadora de Telecomunicações, Aplicação Cliente, Varejista (Loja), Aplicação P2P, Conta S-Wallet e eNotas**. A Figura 4.1 mostra uma visão geral das entidades do sistema S-Wallet.



Figura 4-1 – Entidades participantes do ciclo de pagamentos da S- Wallet.

- i) **eNotas:** ela pode ser definida como a criação do dinheiro virtual. Sua estrutura consiste: um ID, uma chave pública de criptografia, certificados digitais de autenticação, valor da quantia monetária a ser transferida e uma assinatura da conta. Esta assinatura possui 128 bytes de tamanho e essa estrutura é armazenada em uma sequência de bytes (*byte array*), gerando essencialmente uma eNota de 170 bytes. A eNota é inserida em um pacote de dados que é codificado e trafegado durante os pagamentos P2P ou POS;

- ii) **Conta S-Wallet:** ficar armazenada nas “nuvens” (*cloud computing*), podendo ser acessada pelo usuário para a conversão do dinheiro, saldo e créditos em eNotas. A característica e a segurança dessa conta, que pode ser assim denominada integrante do fluxo de pagamento desde o dinheiro real até o produto final, seja ele pagamento P2P ou compra do produto em loja, é a mesma de qualquer servidor de armazenamento de dados online, com informações criptografadas e conexões seguras seja ela por VPN, proteção por HTTPS ou TLS;
- iii) **Banco:** central real de transações financeiras, instituição que por meio da conexão segura, fornece à conta S-Wallet, as autorizações e certificados digitais para o crédito ao cliente. O cliente transfere de sua conta física no banco, uma determinada quantia para sua conta virtual para os pagamentos móveis. Essa transferência entre o banco e a conta S-Wallet pode ser realizada pelo *internet banking*, por um APP do banco no smartphone ou por um caixa ATM. As futuras aplicações poderão se submeter ao crédito imediato das eNotas em caixas ATM com leitores NFC e a conexão direta ao banco. Este trabalho considera apenas as transações efetuadas entre as aplicações e os leitores NFC. A definição da comunicação entre a instituição financeira e a S-Wallet é proposta de trabalhos futuros.

A transferência bancária ocorre de modo simples online para a conta S-Wallet. A partir desta conta o cliente sabe: **o saldo, o extrato e o histórico.**

A criação da conta evita o acesso direto a conta física do indivíduo, evitando assim que pessoas com outras intenções venham a efetuar invasões que comprometam o crédito do usuário e até mesmo o sistema do banco;

iv) Operadora de Telecomunicações: instituição que suporta o sistema S-Wallet no momento em que o cliente encontra as melhores tarifas e as velocidades de conexão se comparado com a solução de comunicação com as instituições financeiras. Ela pode exercer o mesmo papel do banco na transferência para a conta S-Wallet das autorizações e dos certificados digitais para o crédito do cliente. A mecânica de cobrança dos valores creditados ao cliente é deixada em aberto para a escolha da operadora, que pode vincular seus serviços de pagamento móvel com serviços prestados usualmente ao cliente. Como no caso das instituições financeiras (banco) neste trabalho define-se o protocolo SWEP e sua interação com a APP S-Wallet para pagamentos P2P e POS. A definição da comunicação entre as instituições de crédito são propostas de trabalho futuro.

A liberação do saldo também pode ocorrer da conta bancária para a conta S-Wallet. A liberação dos créditos e o envio para o usuário ocorrem via: SMS, Internet. A operadora garante o serviço contínuo de fornecimento de conexão com a conta do cliente/aplicação móvel, uma vez que o usuário pode confiar na sua utilização caso ocorra falha no serviço bancário;

v) Aplicação Cliente: é a App instalada no dispositivo do cliente que efetua as operações de comunicação com a rede, inicia o protocolo e efetua o pagamento. Além disso, a App armazena os dados e as informações inerentes a transação;

- vi) Aplicação P2P:** É a App instalada no *smartphone* do usuário que efetua os pagamentos P2P. Esta App tem a mesma finalidade da Aplicação Cliente. A App se comporta de dois modos: **receptora e emissora**. A primeira quando recebe pagamentos e a segunda quando realiza pagamentos; e
- vii) Varejista (Loja):** Representa o leitor NFC que recebe o pagamento e efetua a comunicação com a **Aplicação do Cliente** para iniciar a transação, informa os valores e os produtos do estoque, efetua a transação de valores por meio do protocolo SWEP, envia o recibo para o cliente e para a instituição financeira que gerou a autorização para a eNOTA.

4.3.1 Sistema Cliente

O **Sistema Cliente** consiste na **Aplicação Cliente/Aplicação P2P** ou App S-Wallet instalada junto ao usuário do *smartphone* que permite a utilização do pagamento móvel na sua forma P2P ou POS. Em um pagamento P2P ambos os usuários são considerados clientes, recebendo e enviando pagamento. Esse sistema possui as seguintes funcionalidades:

- Permite a instalação segura da aplicação no dispositivo móvel do usuário;
- Permite ao utilizador do dispositivo móvel acesso às funções de verificação de saldo, histórico das operações, aquisição do crédito e pagamento;
- Permite ao usuário gerir os dados de sua conta S-Wallet; e
- Permite a troca de dados utilizando a tecnologia da NFC.

O sistema cliente (App S-Wallet) divide-se em duas partes: a componente J2ME (MIDlet) e uma componente Java Applet (applet).

a) Componente J2ME

A componente J2ME consiste na MIDlet J2ME que serve de interface para que o usuário do *smartphone* acesse e gerencie seus dados vinculados a conta virtual e possa também se comunicar com as entidades participantes do ciclo de pagamentos.

A MIDlet implementa os algoritmos que gerenciam a troca de informações entre a camada de aplicação e a camada do protocolo SWEF. Essa pode obter a informação que se apresenta ao usuário no seu banco de dados de registro da conta S-Wallet, comunicando assim com a componente Java Applet, com o sistema S-Wallet ou com outro dispositivo móvel. Esta informação pode ser trabalhada pela aplicação e apresentada de uma forma amigável na tela do *smartphone*.

A estrutura da MIDlet é definida nas seguintes camadas:

- **Comunicação:** efetua a troca de mensagens entre o protocolo SWEF, a conta S-Wallet e as diferentes funcionalidades do sistema Android do *smartphone*;
- **Base de Dados:** com informações vinculadas a conta S-Wallet e ao ID do usuário;
- **Apresentação:** fornece uma interface simples e de fácil utilização para o usuário; e
- **Protocolo:** implementação do protocolo SWEF que realiza a maior parte do fluxo de pagamento móvel.

A camada de comunicação fornece os pontos de acesso fundamentais para que a informação chegue desde a MIDlet até o usuário ou possa transitar entre as aplicações e entre as entidades do sistema S-Wallet. Essa camada permite ainda que a informação seja compartilhada pelo *General Packet Radio Service* (GPRS), GSM/3G, pelo ISO/IEC 18092 NFC-IP1 e ISO/IEC 14443-A [48].

A camada de base dos dados estabelece uma conexão segura por TLS ou HTTPS com o servidor da conta S-Wallet para manter o sistema Android do *smartphone* sempre atualizado com as informações relativas a conta do usuário. Essa conta está sempre vinculada ao seu ID de registro. Uma segunda função da base de dados é assegurar a informação de crédito e os valores monetários que foram transferidos de instituições para a conta S-Wallet e creditados junto a App S-Wallet.

Finalmente, a camada de apresentação possibilita a interação do usuário com a MIDlet. A verificação do saldo e do histórico, assim como a realização de uma simples compra é efetuada por meio da aplicação. A aplicação fornece ao usuário uma experiência fácil, rápida e segura, para que as dificuldades na utilização das formas de pagamento “reais” sejam solucionadas por meio dessa nova forma “virtual” baseada no pagamento móvel.

O interior da camada do protocolo é a implementação da principal estrutura de todo o sistema S-Wallet.

b) Componente Java Applet

A componente *Java Applet* possui parte da estrutura do protocolo SWEP que promove a integração entre o mesmo e a App S-Wallet. Esta *applet* gerencia as senhas,

os dados confidenciais como certificados digitais e as assinaturas, assim como as chaves de criptografia utilizadas nas conexões entre a App S-Wallet e a conta S-Wallet.

A *Java Applet* possui um alto nível de segurança com redundância criptográfica e somente pode ser acessada por desenvolvedores que possuem a chave privada de acesso. A estrutura da *applet* fornece segurança e protege o usuário de ataques ao seu dispositivo móvel.

Hoje acredita-se que o *smartphone* já é visado por hackers e crackers com o objetivo de acessar o alto nível de informações que tais dispositivos armazenam. Uma vez que esta dissertação trata de quantias monetárias, essa estrutura fornece a devida segurança para a aplicação. Neste trabalho são realizados alguns testes de segurança para mostrar a eficiência da *applet*.

4.3.2 Sistema varejista (loja)

O **sistema varejista** consiste de um sistema com um leitor NFC e o software de comunicação entre a loja, o cliente e a conta S-Wallet. O equipamento de leitura NFC pode ser um computador modificado para leitura de *smartcard* ou um outro *smartphone* funcionando como servidor (receptor). No pagamento entre o cliente e a loja, o atendente seleciona o produto desejado, informando seu valor. Ao realizar o emparelhamento do dispositivo com o dispositivo *smartphone* do cliente, ocorre a troca de valores. O sistema varejista possui as seguintes funcionalidades:

- Permite a instalação segura da aplicação no dispositivo fixo da loja;
- Permite ao varejista acesso às funções de verificação dos valores, histórico das operações, comunicação com as instituições financeiras;

- Permite ao usuário gerir os dados de sua conta S-Wallet; e
- Permite a troca de dados utilizando a tecnologia da NFC.

4.3.3 Conta S-Wallet

A criação da conta se inicia pelo cadastro do cliente junto ao banco de sua utilização ou à operadora de telefonia, autorizando a realização de créditos junto a conta S-Wallet. A conta S-Wallet está vinculada ao APP cliente instalado no *smartphone* do cliente, com dados de IMEI, cartão SIM, chip NFC para efetuar o débito/crédito da troca de informações evitando assim ataques e utilizações por terceiros.

A comunicação entre a conta e o cliente é on-line. Os créditos são transmitidos ao applet/midlet, estes créditos são vinculados ao *smartphone*. Sendo os mesmos pessoais e intransferíveis, apenas por meio de pagamento NFC P2P, sendo debitados/creditados de ambas as contas.

Com um determinado saldo na aplicação, ela cria as eNotas estruturadas como mencionado acima de (ID, chave de codificação, certificado digital, valor monetário e assinatura digital).

4.3.4 Operações da S-Wallet:

As operações definidas neste trabalho visam se adequar às características e aos benefícios citados no começo deste capítulo. O principal beneficiário de todas essas operações é o usuário do pagamento móvel. Com isso, quanto mais facilidade e segurança o usuário encontra dentro do sistema, mais vantagens ele encontra ao trocar o dinheiro físico de papel pelo dinheiro digital utilizado no sistema S-Wallet.

Dessas características analisadas das pesquisas e dos estudos de outros sistemas de pagamento móvel, foram encontradas algumas operações básicas para o sistema desenvolvido: **crédito, pagamento, extrato, e verificação de histórico**. A operação de pagamento divide-se ainda em pagamento local P2P, pagamento local POS e recepção de pagamento.

Operações básicas do sistema S-Wallet:

a) Crédito

A operação de crédito corresponde à transferência de valores monetários entre a instituição financeira escolhida (seja ela banco ou operadora de telecomunicações) e a conta S-Wallet. Essa operação visa primordialmente a segurança da transação dentro do fluxo de pagamentos móveis, pois ela mantém as contas físicas do usuário e a conta s-wallet sem contato direto constante. Evitando assim que as contas físicas sofram algum tipo de ataque.

O primeiro passo para que o cliente utilize a transferência bancária de créditos para a conta S-Wallet é o seu cadastro no banco para acesso remoto da conta por um portal na internet (*internet banking*). Assim, ele poderá realizar a transferência para a conta que tem contato direto com o sistema S-Wallet. O banco fornece um ID exclusivo e intransferível para essa conta S-Wallet.

Esse ID fornece segurança e privacidade ao usuário. Segurança pois ele realiza as verificações pontuais para as conexões de aquisição de crédito sempre que o cliente acessa sua conta por meio do *internet banking*. Privacidade, pois o contato entre o banco, a conta S-Wallet, e os estabelecimentos varejistas e outros usuários ocorre por meio de um ID e não de dados do usuário.

Para as transferências de crédito entre a operadora de telecomunicações e a conta S-Wallet, o usuário pode cadastrar seu SIM Card vinculado à operadora na conta. Ele deve também habilitar a opção pagamentos móveis junto a operadora de telecomunicações para efetuar os débitos automáticos dos créditos transferidos diretamente em sua fatura mensal. O usuário recebe um ID vinculado ao seu SIM Card com os dados do IMEI do seu *smartphone*.

Nesse caso, a transferência é independente do acesso do usuário ao portal da operadora de telecomunicações e ocorre diretamente do dispositivo móvel do usuário por meio do SMS ou da própria APP S-Wallet. O desenvolvimento dessa funcionalidade requer necessariamente um esforço conjunto com a operadora de telecomunicações que fornece as funções específicas para a ativação da aplicação em conjunto com suas operações padrão.

Uma vez cadastrado em uma instituição, o usuário realiza a transferência ou o crédito das quantias que acha necessário para sua conta S-Wallet. Estipula-se que como nesta dissertação trabalha-se com micro pagamentos, os valores não excedam a \$50.00 (cinquenta dólares) ou a R\$100.00 (cem reais). Outra regra que se aplica neste trabalho é o período que o usuário pode efetuar as “recargas” de valores. Como nos limites em um saque em um caixa eletrônico (ATM), o limite diário para crédito do usuário é \$250.00 (duzentos e cinquenta dólares) aproximadamente R\$500.00 (quinhentos reais). Esta regra fornece segurança ao portador do dispositivo móvel, evitando assaltos/sequestros dos mesmos, uma vez que o *smartphone* por si só já corresponde a uma grande quantia.

Realizada a transferência, a conta S-Wallet adiciona essa quantia permitindo que o usuário utilize os créditos por meio da App S-Wallet. Antes de realizar qualquer

pagamento, o usuário deve sincronizar a App S-Wallet instalada no dispositivo móvel com a conta S-Wallet. Assim, para efetuar a transferência de dados, com o ID e os créditos, na App S-Wallet o protocolo SWEP efetua a inicialização das eNOTAS. Por meio desta inicialização, o usuário está habilitado a realizar os pagamentos a terceiros e/ou lojas.

A seguir descreve-se o fluxo definido para a operação de crédito representada na Figura 4.2.

Primeiro, o usuário realiza seu registro junto a uma instituição financeira por meio da conta S-Wallet. Realizado o registro, o usuário escolhe a quantia e transfere os valores em forma de crédito para a conta S-Wallet. A App S-Wallet sincronizada com a conta S-Wallet informa-se do ID enviado pela instituição, assim como dos créditos transferidos. A App S-Wallet realiza as operações internas necessárias para que a OPERAÇÃO DE CRÉDITO seja concluída neste ponto entre a conta S-Wallet e a App S-Wallet.

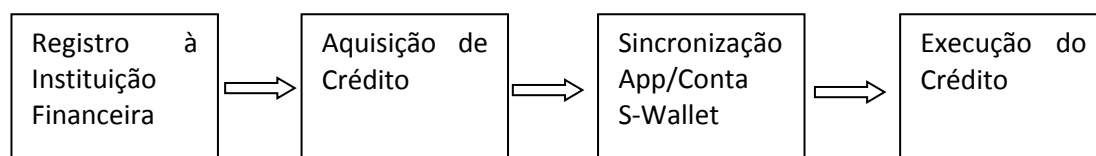


Figura 4-2 – Fluxo da operação de crédito

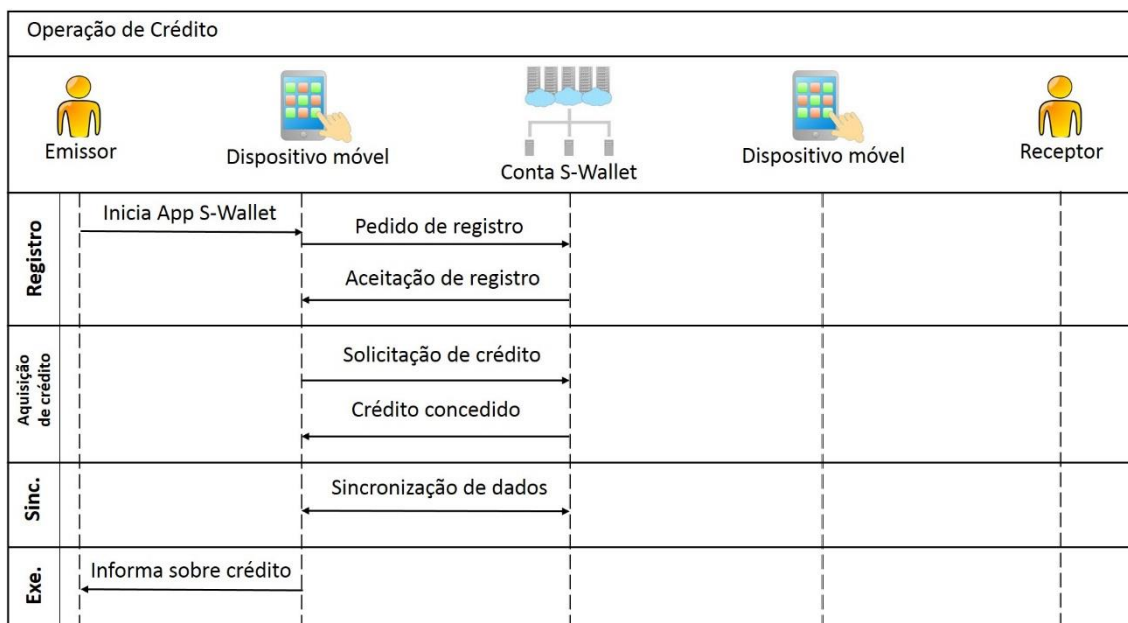


Figura 4-3 – Ações que ocorrem durante o fluxo da operação de crédito.

A Figura 4.3 ilustra as ações que ocorrem durante o fluxo da operação de crédito.

b) Pagamento

A principal função de um sistema de pagamentos móveis é a operação de pagamento, que é a transferência de valores entre duas entidades. Esses créditos são denominados neste trabalho de eNotas. As eNotas são inicializadas pelo protocolo SWEP. As entidades que fazem parte do fluxo de pagamento podem variar de acordo com o tipo de pagamento a ser efetuado.

Grande parte das ações realizadas durante a operação de pagamento utilizam o protocolo SWEP. Em especial, a ação de transferência quase que em sua totalidade se baseia nos passos do protocolo para a sua execução. As outras ações da operação acontecem com o auxílio de todo o sistema S-Wallet.

A entidade receptora pode ser um varejista ou um outro usuário. Ela pode estar próxima da entidade emissora, onde é utilizado a NFC para realizar a conexão entre os dispositivos do emissor e do receptor.

Em um pagamento usuário para usuário (P2P), ambas as entidades podem ser consideradas pagantes, no momento em que o ato de enviar e receber é um pagamento de ambas as partes. Neste ponto, a designação do usuário e do varejista se torna ambígua, assim determina-se que a entidade que efetua o pagamento é denominada emissora e a que recebe o pagamento é denominada receptora. Em seguida descreve-se o fluxo do sistema S-Wallet para a operação de pagamento que é ilustrada na Figura 4.4.

A operação de pagamento é iniciada pelo emissor da transação. O emissor inicia a App S-Wallet no seu *smartphone* e com isso também inicializa o protocolo SWEP. O usuário precisa se identificar junto à App no seu dispositivo e selecionar a opção de pagamento pretendida (seleção de pagamento): P2P ou POS. Posteriormente, o dispositivo móvel do receptor recebe o pedido de conexão para iniciar o fluxo do pagamento móvel (pedido de conexão).

Com os dados fornecidos no passo anterior (pedido de conexão), os dispositivos iniciam o protocolo SWEP para processar o pagamento (inicialização do SWEP). Então, o protocolo é utilizado para **verificação de identidade**, onde o sistema realiza a verificação dos IDs, certificados, chaves de criptografia e assinaturas digitais. O objetivo desta ação é assegurar a segurança na transação dos pagamentos móveis. Com essas informações as App S-Wallet verificam a identidade dos usuários e se ambos tem condições e acesso a todos os parâmetros necessários para realizar o pagamento.

Após a **verificação de identidade**, o emissor determina o produto a ser adquirido ou o valor a ser transferido. Neste ponto ocorre a inicialização da **eNota**.

Inicializada a eNota, neste momento o protocolo SWEP atua em conjunto com os dois dispositivos para a **transferência** de dados entre o emissor e o receptor utilizando a tecnologia da NFC. Então, os dados são codificados para essa transferência.

A ação de **confirmação** da transferência é realizada durante a recepção dos dados pelo usuário receptor. Nela, a App S-Wallet decodifica o pacote de dados, verificando os valores e os IDs inclusos na eNota. Para a conclusão dessa ação é solicitado ao usuário emissor o débito dos créditos inclusos na mesma.

Assim que é concluída a transferência dos créditos, a última fase da operação de pagamento é o **encerramento**, onde o usuário receptor é informado dos créditos em sua conta. A App S-Wallet receptora envia para a emissora um recibo com os dados pertinentes como ID de ambas as entidades, o valor transacionado para débito e para crédito e a inclusão no histórico das transações.

A Figura 4.4 mostra o fluxo da operação de pagamento.

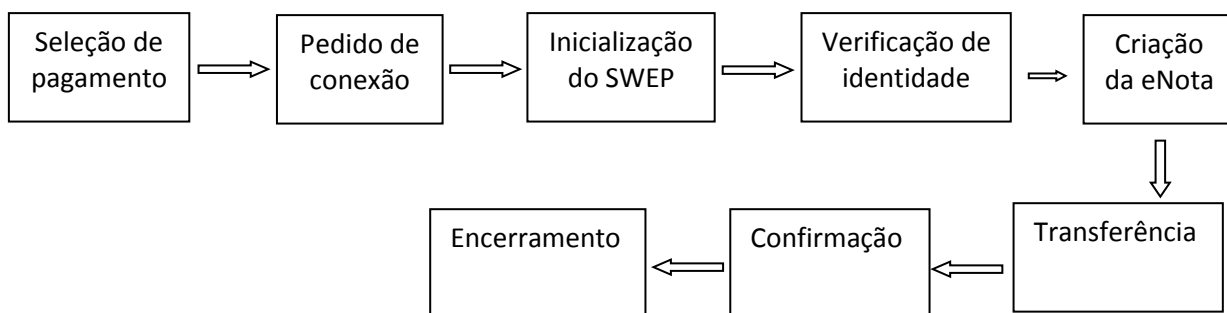


Figura 4-4 – Fluxo da operação de pagamento.

Os passos definidos pelo sistema S-Wallet para cada uma das ações mostradas na Figura 4.4 são descritos a seguir.

Seleção de pagamento: a operação de pagamento inicia pela seleção da aplicação no dispositivo móvel do usuário. Seleccionada, a App S-Wallet inicializa o sistema do protocolo SWEP. Primeiro, o usuário precisa se identificar junto à App por uma senha (PIN) ou de reconhecimento de face, dependendo da disponibilidade dessa funcionalidade no dispositivo móvel do usuário. Identificado o usuário, ele deve escolher dentro da App S-Wallet, por meio da interface gráfica da aplicação, a forma de pagamento que será utilizada pela entidade emissora, como mostrado na Figura 4.5.

Independentemente do tipo de pagamento escolhido pelo usuário, o protocolo que realiza a transação entre as aplicações é o protocolo SWEP, que faz parte do conjunto de todo o sistema S-Wallet. A forma de pagamento pode ser determinada manualmente ou de forma automática, a partir das fontes como etiquetas NFC ou códigos de barra em estabelecimentos da rede de Varejo que possuem esse tipo de tecnologia para realizar um pagamento POS.

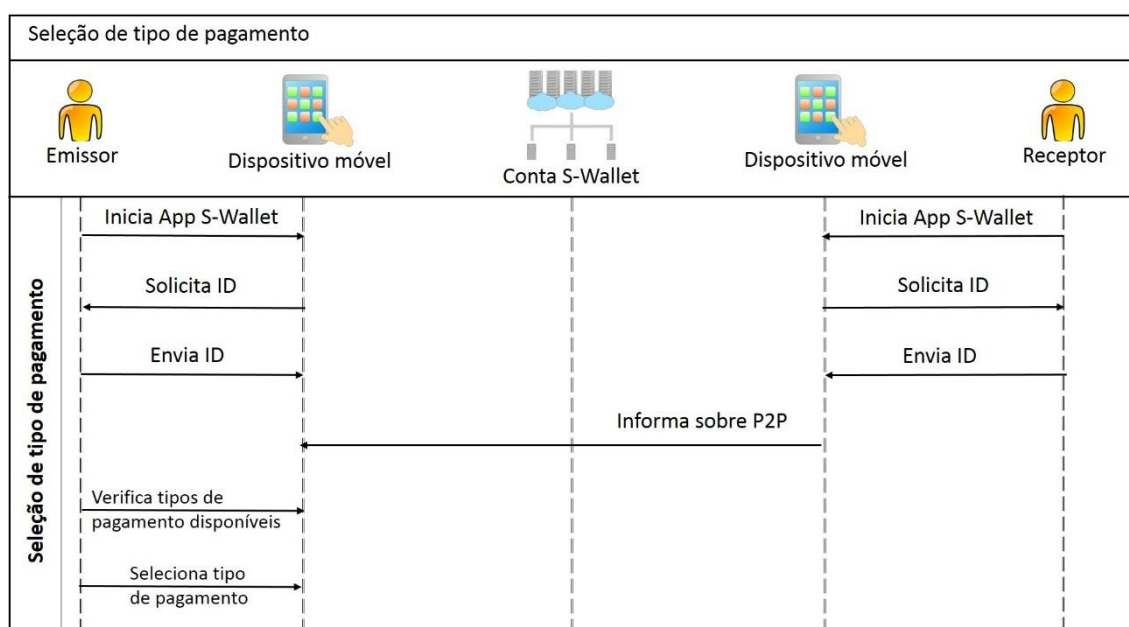


Figura 4-5 – Ações executadas durante a operação de seleção de pagamento.

Pedido de conexão: uma vez selecionado o tipo de pagamento, a entidade emissora envia para a entidade receptora um pedido de conexão, para que ambas estabeleçam a conexão por meio da NFC. Se a transação é um pagamento P2P, essa conexão pode ser estabelecida pela aproximação dos dispositivos. Com esta aproximação aparece na tela de ambos os dispositivos um pedido de conexão. Se eles concordam com esse pedido, ambos selecionam a opção “Sim”. E é estabelecida a conexão.

A partir deste momento, ambas as aplicações S-Wallet trocam as informações relativas aos IDs dos usuários receptor e emissor e os certificados de autenticação para a conexão e para os dados que são trafegados.

O principal objetivo desse passo é estabelecer a conexão entre os dispositivos móveis e realizar uma primeira troca de dados entre as entidades, isso inclui por exemplo o produto ou o serviço a ser adquirido e o valor do pagamento.

Se o pagamento é POS, o leitor NFC pode fornecer automaticamente o valor do pagamento para a entidade emissora. Em pagamentos P2P, o emissor introduz manualmente a informação relativa à transação, como o valor do pagamento e ele tem a possibilidade de informar também o ID da entidade receptora.

A Figura 4.6 ilustra as ações durante a função de pedido de conexão.

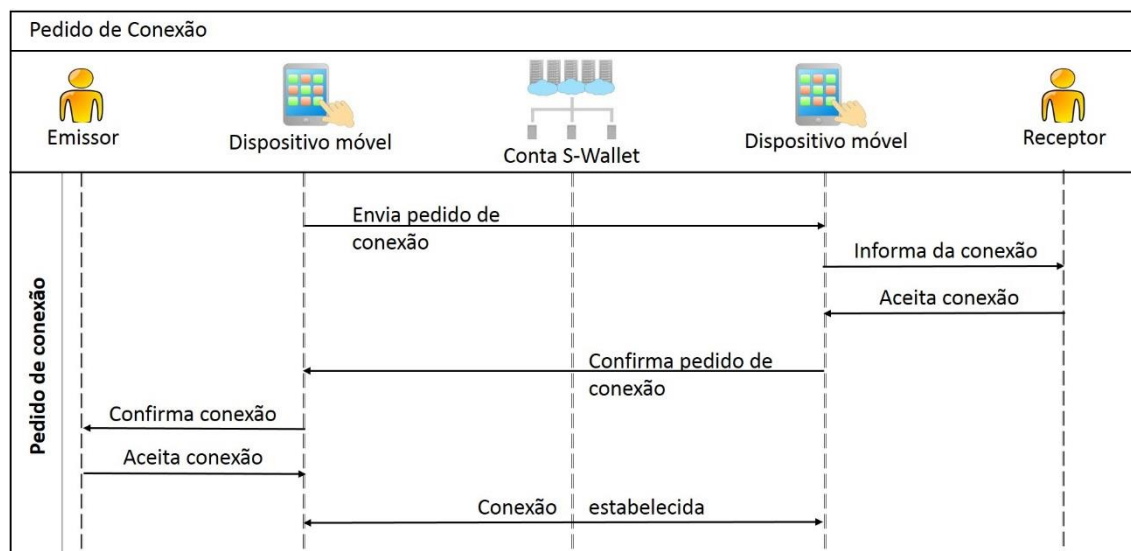


Figura 4-6 – Ações durante a função de pedido de conexão

Inicialização do SWEP: como mostrado na Figura 4.7, a App S-Wallet ao estabelecer a conexão entre as entidades, inicializa integralmente esse protocolo com os dados iniciais obtidos durante o pedido de conexão.

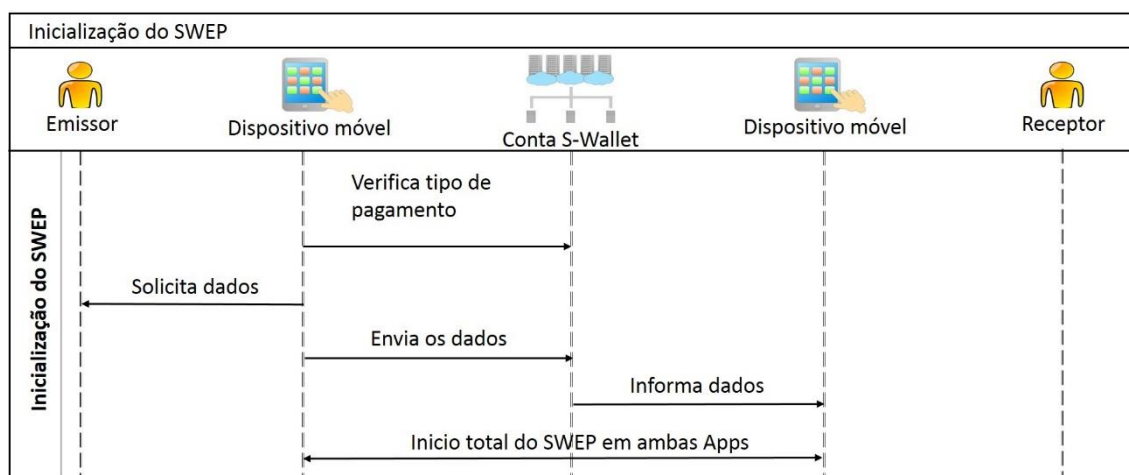


Figura 4-7 – Ações executadas durante a inicialização do SWEP.

Em um primeiro momento o protocolo SWEP verifica o tipo de pagamento escolhido pela entidade emissora e inicia junto a App S-Wallet a interface para a

realização dos pagamentos. As características da conexão, identificação, troca de chaves criptográficas e a transferência de certificados são definidas na seção 4.3 deste capítulo.

Verificação da identidade: também fazem parte da ação do sistema S-Wallet a verificação das IDs das entidades participantes da transação assim como dos certificados digitais de autenticação. Esse sistema verifica a veracidade das IDs e os certificados de autenticação utilizados em conjunto com o protocolo SWEF.

Inicialização da eNota: Uma vez verificadas e confirmadas as identidades das entidades, a conexão se torna segura e é confirmada a possibilidade de realização do pagamento. Neste passo, a entidade emissora pode por meio da interface da aplicação determinar o valor monetário (R\$) que é inserido na eNota para a transferência entre as App S-Wallet. O usuário emissor determina o valor a ser transferido para o usuário receptor ou escolhe um produto com um preço especificado no ponto de venda para realizar sua compra. Cria-se aqui um pacote de dados com os créditos presentes na App S-Wallet em conjunto com os dados como ID, chave de criptografia e certificados.

A Figura 4.8 mostra as ações executadas durante a verificação do ID e a inicialização da eNota.

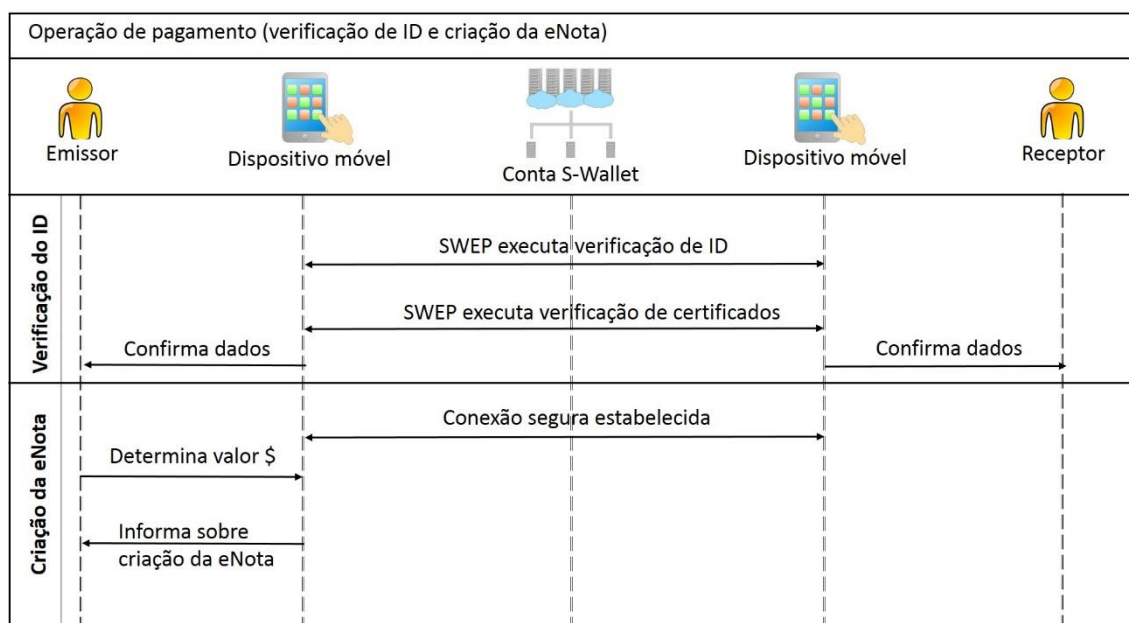


Figura 4-8 – Ações executadas durante a verificação do ID e inicialização da eNota.

Transferência: Com a inicialização da eNota, o protocolo SWEP entra no ponto máximo do seu funcionamento. Ele realiza um processo de codificação da eNota, assim como dos dados que são trafegados. Esse protocolo realiza um processo de certificação das informações, por meio dos protocolos de criptografia simétrica, certificados digitais e identidades dos usuários. Os dados codificados são enviados do emissor para o receptor e no pacote de dados são enviados também os créditos para realizar o pagamento.

A Figura 4.9 ilustra as ações executadas durante a transferência de dados.

Na seção 4.3 deste capítulo são mostrados os passos do protocolo SWEP. A inicialização da eNota e a transferência de dados correspondem a mais de 50% dos passos realizados por esse protocolo para realizar um pagamento móvel. Em específico, a transferência de dados corresponde aos passos de 3 a 6. Estes passos representam o

processo de criptografia e certificação do sistema S-Wallet utilizando o protocolo SWEP com técnicas de criptografia simétrica e IDs para ambos os usuários.

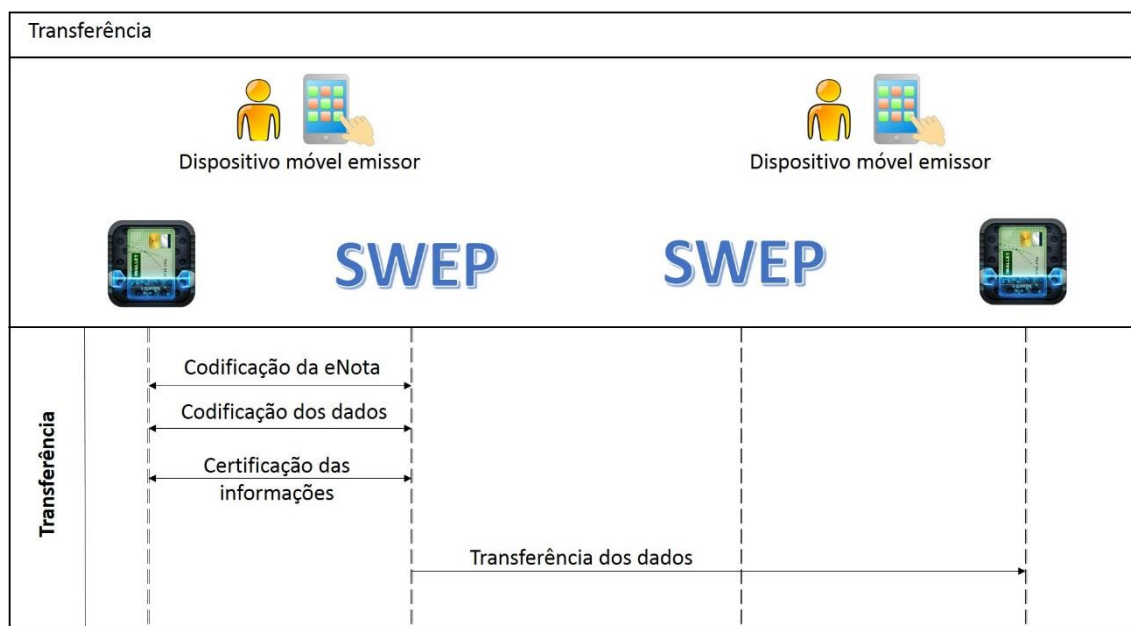


Figura 4-9 – Ações executadas durante a transferência de dados.

Confirmação: os dados chegam na App S-Wallet receptora codificados. Em conjunto com o protocolo SWEP, a aplicação utiliza as chaves de decodificação para descompactar o pacote de dados, verificando os valores e os IDs inclusos na eNota. A App S-Wallet receptora notifica a App do usuário emissor da recepção dos dados, assim como da necessidade de débito em sua aplicação dos créditos que foram transferidos. É enviado um recibo da transferência de dados contabilizando todos os dados que fazem parte da operação.

A Figura 4.10 mostra as ações executadas durante a confirmação do pagamento.

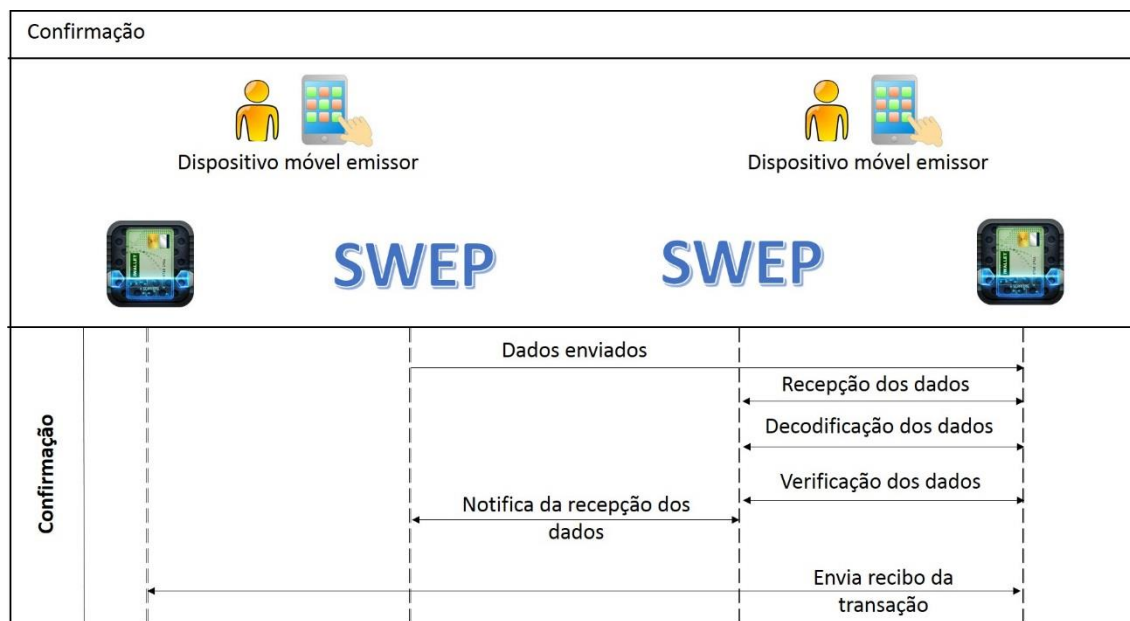


Figura 4-10 – Ações executadas durante a confirmação do pagamento.

Encerramento: concluída a transferência dos créditos e dos dados, a App emissora é informada pela App S-Wallet do débito dos créditos em sua conta. Posteriormente, ela debita do saldo de créditos existente em seu interior e insere o recibo no seu histórico de transações. Finalmente, a App emissora encerra a conexão.

A Figura 4.11 ilustra as ações executadas pelas Apps durante o encerramento da conexão.

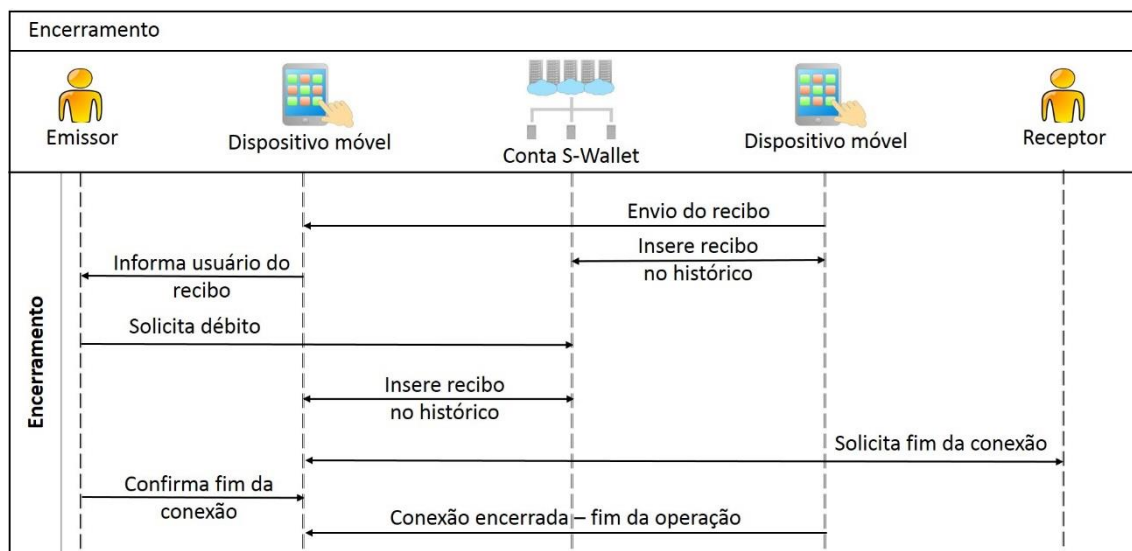


Figura 4-11 – Ações executadas pelas Apps durante o encerramento da conexão

c) Depósito e débito

A operação de depósito e débito fornece aos usuários do sistema S-Wallet a possibilidade de transformar em valor monetário real os créditos contidos em cada eNota transferida. Assim, os clientes e os vendedores podem transferir os créditos de sua App S-Wallet para a conta S-Wallet e posteriormente para as suas instituições financeiras. Nessa operação, um dispositivo que atuou como receptor pode informar a uma instituição bancária os pagamentos que recebeu. O dispositivo emissor pode também solicitar o débito em sua conta dos créditos que foram transferidos. A atualização da transação é imediata caso ambas a Conta S-Wallet, e a App S-Wallet estejam em sincronia. Esse sincronismo é efetuado sempre que o usuário se conecta a Conta S-Wallet.

O fluxo definido para o sistema S-Wallet efetuar a operação de depósito e débito é formado pelas ações: definição do tipo de usuário, onde o sistema determina se é um

usuário emissor ou um receptor, e dependendo da escolha a execução de débito ou depósito.

A Figura 4.12 mostra o fluxo da operação de depósito e débito.

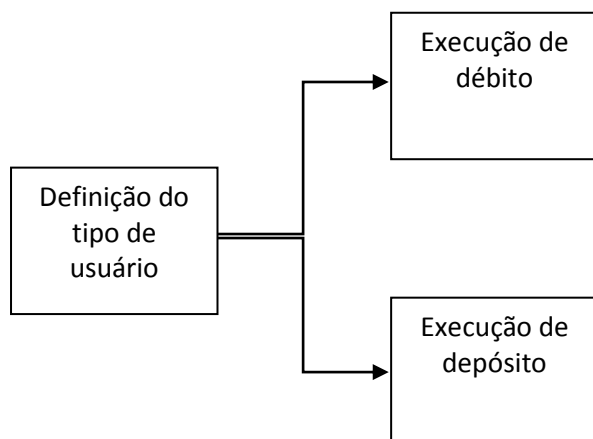


Figura 4-12 – Fluxo da operação de depósito e débito.

As operações executadas pelo sistema S-Wallet para cada uma das ações são descritas em seguida.

Definição do tipo de usuário: Neste ponto o sistema S-Wallet verifica o estado do usuário dentro da App S-Wallet durante a última transação. Se o usuário é um emissor, ele define a próxima ação como sendo de débito. Se o usuário é um receptor, ele define a próxima ação como sendo de crédito.

Execução de débito ou depósito: o dispositivo realiza uma troca de mensagens com a conta S-Wallet para informar a quantia em créditos que cada usuário tem a receber ou a debitar de sua conta. A conta S-Wallet posteriormente realiza a atualização de seu estado de crédito e informa a cada usuário do seu saldo atual, que pode ser verificado na operação de **verificação de histórico/saldo**.

A Figura 4.13 ilustra o fluxo de ações da operação de débito ou depósito.

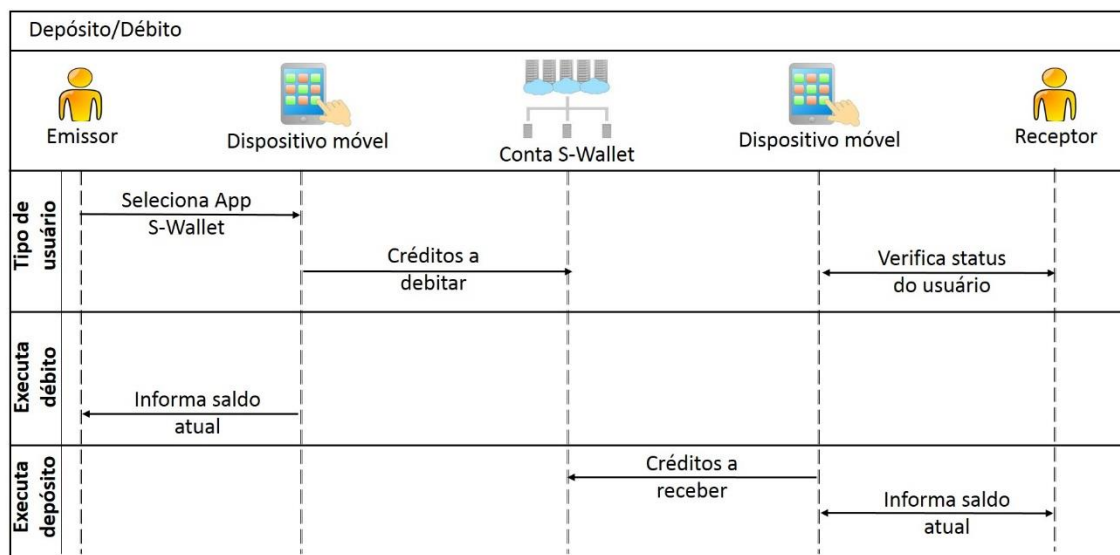


Figura 4-13 – Fluxo de ações da operação de débito ou depósito.

d) Verificação de Histórico/Saldo

A operação de verificação do histórico e do extrato é essencial para o sistema S-Wallet. Ela possibilita ao usuário facilidade e confiabilidade na conexão entre a App S-Wallet e a conta S-Wallet, uma vez que ele tem total acesso e controle dos seus créditos e do histórico das suas compras.

A função da verificação do histórico/saldo é mostrar ao usuário seu saldo pela **verificação de saldo** e um histórico detalhado das compras realizadas pelo usuário pela **verificação de histórico**. Esta operação compreende duas ações dentro do sistema S-Wallet, a primeira delas é a escolha da opção **conta S-Wallet** dentro da App S-Wallet e a segunda é a escolha entre a opção **histórico ou saldo**. Novamente os dados dependem da sincronia entre a Conta S-Wallet e a App S-Wallet para manter os registros de transações atualizados.

A Figura 4.14 mostra o fluxo da operação de verificação do histórico/saldo.

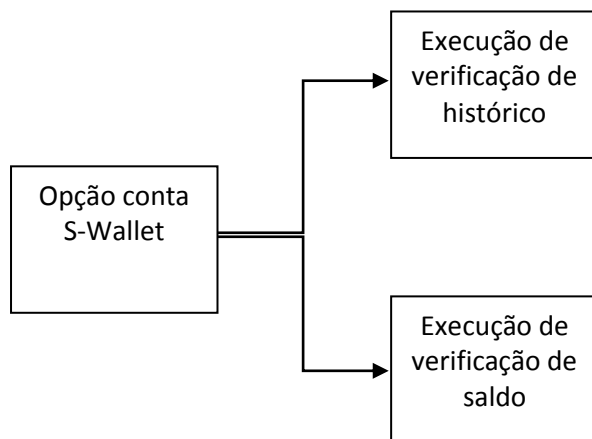


Figura 4-14 – Fluxo da operação de verificação de histórico/saldo.

As ações realizadas pelo sistema S-Wallet durante a operação de verificação do histórico/saldo são:

Opção conta S-Wallet: dentro da aplicação o usuário deve selecionar a opção conta S-Wallet para realizar a conexão com a conta que está armazenada nas nuvens. Neste momento, é necessário uma conexão com a internet para o acesso entre o dispositivo móvel e a conta S-Wallet.

Execução da verificação de histórico/saldo: escolhida a opção **conta S-Wallet** dentro da App S-Wallet, o usuário pode agora selecionar a opção histórico ou saldo. Selecionando a opção saldo, o dispositivo móvel do cliente solicita o saldo atual dos créditos do usuário junto a conta. O usuário pode verificar dois tipos de saldo: crédito ou débito. O saldo de crédito representa o valor disponível para efetuar os pagamentos. O saldo de débito representa o valor acumulado dos pagamentos recebidos pela App S-Wallet. Ao selecionar a opção histórico, é mostrado ao usuário todas as compras efetuadas até aquele momento, assim como os débitos dos valores recebidos. Nesse histórico, constam dados como ID dos usuários que fizeram a conexão com aquela aplicação, data do pagamento e o valor.

Ao selecionar a opção histórico é mostrado ao usuário todas as compras efetuadas até aquele momento, assim como os débitos dos valores recebidos. Nesse histórico, constam dados como ID dos usuários que fizeram a conexão com aquela aplicação, data do pagamento e o valor.

A Figura 4.15 ilustra as ações realizadas pela operação de verificação do histórico/saldo.

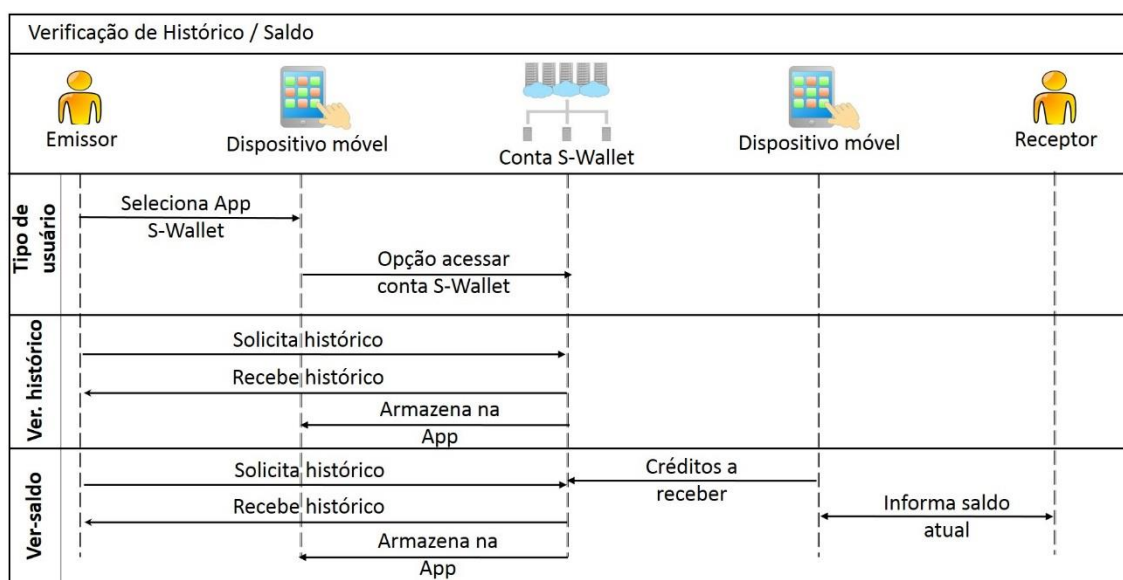


Figura 4-15 – Ações realizadas pela operação de verificação de histórico/saldo.

4.3.5 Comunicações do sistema S-Wallet

As comunicações do sistema S-Wallet entre suas entidades ocorrem em passos bem determinados dentro do sistema e do protocolo SWEP. Cada passo da execução destas comunicações são descritos abaixo:

a) Comunicação conta S-Wallet – cliente

- I) O cliente acessa o sistema online e transfere da sua conta bancária ou da operadora, os créditos para a sua conta S-Wallet. Essa primeira transferência traz alguns benefícios:
- Evita ficar sem acesso à créditos em possíveis quedas no sistema bancário e/ou de telecomunicações;
 - Mantêm as contas bancária e a conta S-Wallet isoladas, evitando fraudes e roubos; e
 - Maior controle sobre os dados transmitidos.
- II) O cliente acessa o sistema S-Wallet e pode verificar o saldo, ID, IMEI (aparelho *smartphone*), os dados do seu SIM Card e o histórico de transações;
- III) O cliente transfere esse saldo para o dispositivo móvel armazenando-o na App S-Wallet; e
- IV) A conexão *online* entre a conta S-Wallet e o dispositivo móvel possui a mesma segurança de uma conexão do internet banking. Aqui ela é utilizada em conexões por TLS e HTTPS.

b) Comunicação cliente-cliente

- I) O cliente 1 solicita a conexão pelo NFC com o cliente 2. Neste primeiro processo de tentativa de conexão (*handshake*) ambos os clientes trocam informações quanto a identidade das partes;
- II) O cliente 2 confirma a conexão e envia ao cliente 1 sua ID-2 para manter durante a conexão;
- III) É estabelecida a conexão segura entre as partes;

- IV) O cliente 1 determina o valor a ser transferido para o cliente 2;
- V) O cliente 2 confere os dados da eNota e envia uma confirmação para o cliente 1;
- VI) O cliente 1 codifica a eNota e envia para o cliente 2; e
- VII) O cliente 2 confirma o recebimento, e envia o recibo do valor pago com sua ID.

c) Comunicação cliente-loja

- I) O cliente solicita a conexão com o leitor NFC da loja;
- II) A loja autoriza a conexão com o cliente pela troca de IDs;
- III) O cliente obtém a lista de produtos e preços;
- IV) O cliente escolhe o produto desejado e o valor a ser transferido. E verifica o crédito na conta;
- V) O cliente solicita a conexão por um canal seguro;
- VI) A loja conecta-se ao cliente por uma conexão segura;
- VII) O cliente envia o valor por meio da eNota, que contém o ID, a chave de criptografia e a assinatura digital;
- VIII) A loja recebe os dados, verifica as chaves e a assinatura, o ID do cliente e o valor da eNota;
- IX) Com a verificação correta do item VIII a loja informa ao cliente a validação da compra;
- X) A loja confirma o pagamento e libera o produto ou o serviço;
- XI) A loja envia ao cliente um recibo com o ID, o produto e o valor; e
- XII) É encerrado o fluxo de pagamento.

4.4 *Protocolo SWEF*

A. Estrutura do protocolo SWEF

Uma das preocupações quanto ao desenvolvimento do protocolo SWEF neste trabalho era relacionada à segurança das transações financeiras entre as entidades do sistema S-Wallet. Essa preocupação é inerente, pois, após a aquisição dos créditos por parte do usuário, as trocas comerciais P2P poderiam ser executadas de modo *off-line*. Com isso não era possível controlar e verificar todas as transações.

Nesta dissertação também foi verificado alguns riscos tais como: o risco do dinheiro digitalizado ser perdido na transação e a atuação de pessoas de má fé tentando realizar a cópia do dinheiro digital creditado na conta que permanece nas nuvens. Este trabalho denominou essa tentativa de crime de falsificação virtual (*e-counterfeiting*). Considera-se que a melhor forma de prevenção é a criação de uma chave de criptografia interbancos e a regulamentação das transações dos pagamentos móveis.

No momento da inicialização da conta S-Wallet, o usuário efetua o *download* para o seu computador pessoal de uma aplicação da conta. Nesta conta o usuário pode gerir seus dados de crédito, saldo, histórico, além de efetuar as novas transferências de crédito. Neste registro, o usuário cria um ID vinculado a todas as suas transferências.

O próximo passo é o usuário realizar o *download* da App S-Wallet no *smartphone*. Esta App é definida como um *MIDlet*, desenvolvido em Java ME para o Android. Neste *MIDlet* foi implementado neste trabalho o protocolo SWEF com toda a parte de comunicação entre as entidades e as funcionalidades.

Em um primeiro momento, durante o registro, a conexão entre a conta S-Wallet e a aplicação cliente possibilita a troca dos certificados digitais e da chave pública da conta. A conta S-Wallet possui uma chave privada para realizar a autenticação junto aos usuários. O par de chaves RSA do cliente utilizado para a autenticação com outros usuários e terminais de pagamento é gerado pela App. Durante a inicialização, o ID da conta do usuário e a chave pública (RSA) são registrados junto a conta S-Wallet. Esta conta envia para o cliente um certificado de autenticação vinculado ao seu ID. Com a recepção da chave pública do usuário, o sistema S-Wallet (conta) gera também um certificado X.509 para essa chave pública e o envia para a App cliente.

Em um segundo estágio, o saldo dos créditos existentes dentro da conta pode ser utilizado pela App na criação das eNotas. Estas eNotas são codificadas e inseridas em um pacote de dados (emissor) e são enviadas para outro App cliente (receptor). Durante a recepção da eNota, o *smartphone* do receptor inicia o *MIDlet*, que a decodifica, extrai os dados dela e verifica o certificado de autenticação do cliente. Os usuários podem gerenciar suas eNotas por meio da App S-Wallet, permitindo também gerenciar o saldo e o histórico das transações realizadas.

B. Estrutura das chaves criptográficas

As chaves que fazem parte do protocolo SWEF são respectivamente:

- A conta S-Wallet possui dois pares de chaves RSA: um de assinatura e outro de codificação. A chave de assinatura é utilizada para autenticar a troca dos créditos entre a conta e a App cliente. Utiliza-se essa chave também na geração de certificados para os terminais POS. O par de chaves de codificações proporciona a comunicação de dados segura entre as entidades que fazem parte do processo; e

- A App cliente no celular do usuário possui um único par de chaves RSA, que recebe um certificado, assinado pela conta S-Wallet. Utilizando esse certificado e a chave privada correspondente, a App pode se comunicar de maneira segura e autenticada com outras Apps e terminais de pagamento. Por razões práticas, esse par de chaves é utilizado para assinar e para codificar.

C. Estágios do protocolo do SWEP

Neste trabalho, durante o desenvolvimento do protocolo SWEP muitas interações foram pensadas entre as entidades integrantes do fluxo de pagamentos. Esta dissertação mostra a interação entre dois clientes durante a realização de um pagamento P2P.

Como mencionado anteriormente, a App do cliente receptor se comporta de uma forma passiva (*smart card*). Por outro lado, a App do cliente emissor atua como um dispositivo *ativo*. Esse emissor simula um terminal de *smart card*, que inicia a segurança da comunicação na conta S-Wallet. Esse modo ativo é propiciado pela App (*MIDlet*). A *MIDlet* é o centro de comunicação e codificação de todo o fluxo de pagamento.

A seguir são definidas as etapas do fluxo de mensagens e os estágios do protocolo SWEP durante um pagamento P2P entre os clientes utilizando a App S-wallet:

- 1) O emissor (App cliente 1 – App-1) seleciona a App (*MIDlet*) para transferir os valores monetários para o receptor (App cliente 2 – App-2). Após a identificação (**reconhecimento facial ou PIN**) junto a App, o usuário acessa seu painel de créditos, com a possibilidade de inicializar uma eNota com um determinado valor a ser transferido. Inicia-se um pedido de comunicação entre os usuários. Nesse

primeiro processo de conexão (*handshake*) entre a App emissora e a App receptora, existe uma troca de informações referentes à **IDs e certificados** de autenticação para garantir a segurança da conexão e das informações que serão trafegadas;

- 2) Uma vez determinado o valor a ser transferido, inicializa-se a **eNota** com valor de X R\$ (Reais). Realiza-se o processo de transferência da eNota da App-1 para App-2 utilizando a NFC. Os MIDlets desses dois clientes interagem por meio de um canal seguro para garantir a conexão efetiva entre os dispositivos;
- 3) Após a inicialização da eNota, a App do receptor (App cliente – 2 ou App-2) gera um código aleatório X e envia para a App do emissor (App cliente – 1 ou App-1), juntamente com o certificado PKI da chave relacionado com a MIDlet (e também com o receptor). Esse certificado contém o ID da App-2 e sua chave pública;
- 4) Após receber o código aleatório X e o certificado, a App-1 realiza os seguintes passos:
 - Confere a informação do certificado, extrai o ID da App-2 e sua chave pública;
 - É construída uma chave de sessão aleatória e simétrica (3DES) C1;
 - O RSA codifica a chave C1 com a chave pública da App-2. Resultando na resposta R1;
 - Gera um ID dessa sessão;
 - A codificação RSA assina digitalmente (X, ID de sessão, ID do Receptor, C1) com a chave RSA privada da App-1. A resposta R2 consiste do ID da sessão e das informações do certificado da App-1; e
 - Envia as respostas R1 e R2 para a App-2.

- 5) Após receber (as respostas R1, R2), a App-2 realiza os seguintes passos:
- A codificação RSA decodifica a resposta R1 com a chave privada da App-2. Resultando na chave C1;
 - Armazena o ID de sessão;
 - Verifica o certificado da App-1;
 - Verifica a assinatura da App-1 no X, no ID de sessão, no ID do receptor e na chave C1;
 - É calculada a chave *Message Authentication Code* (MAC) $C2 = \text{SHA-1}(C1)$;
 - É calculada uma 3DES MAC no ID da sessão e no X, com a chave C2, gerando a resposta R3; e
 - Envia a resposta R3 para a App-1.
- 6) A App-1 recebe a resposta R3, verifica a MAC, realiza uma codificação 3DES da eNota sob a chave C1, resultando na mensagem M1 e a envia para a App-2;
- 7) A App-2 decodifica a mensagem M1, armazena e verifica a eNota, calcula uma 3DES MAC denominada mensagem M2 sob a eNota recebida com a chave C2 e a envia para a App-1;
- 8) A App-1 ao receber a mensagem M2, verifica a MAC e com a confirmação de recebimento, debita do sistema aquela eNota e a lança no histórico das transações; e

- 9) Após realizar os passos de 1 a 8, a App -2 pode notificar o usuário da chegada de uma nova eNota.

Existe no protocolo SWEF a garantia de que a chave simétrica C1 é gerada pela App S-Wallet. Essa chave é assinada com um par de chaves certificadas. Além disso, após a resposta R3, ambas as aplicações dos clientes 1 e 2 têm confiabilidade na legitimidade da comunicação. Como a App-2 (receptora) recupera corretamente a chave C1, isto prova que ela possui a chave privada conectada com seu certificado. Com isso, a App-1 (emissora) mostra a posse da chave privada assinando corretamente X, o ID da sessão e a chave C1. Assim, é estabelecido que o X foi recebido corretamente, o ID da sessão e a chave C1 são originais e a mensagem tem como destino a App do cliente 2.

4.5 *App S-Wallet*

A aplicação do sistema S-Wallet instalada no dispositivo móvel do usuário se comporta como um *middleware*. Para melhor integração de todas as estruturas desse sistema, ele foi desenvolvido neste trabalho utilizando a plataforma Android SDK baseado em Java.

A App S-Wallet possibilita a apresentação de uma aplicação com layout amigável para que o usuário se sinta seguro em inserir dados pessoais e efetuar compras com seu dispositivo móvel. A App também é de fácil utilização para que o usuário não tenha dificuldades na realização das operações do sistema S-Wallet.

A Figura 4.16 mostra a estrutura do sistema S-Wallet.



Figura 4-16 – Estrutura do sistema S-Wallet.

Na camada de aplicação existe a interação com o usuário por meio da App S-Wallet. Todas as operações de segurança e integração são realizadas pelo protocolo SWEP. A principal tecnologia de comunicação do sistema S-Wallet é a NFC. Esta tecnologia possibilita a troca de informações a curta distância.

A conta S-Wallet faz parte do sistema como um todo, mas considerando os blocos que serão instalados e inicializados junto ao dispositivo móvel do usuário, ela permanece em um nível superior. Mesmo interagindo com todo o sistema, essa conta permanece armazenada nas nuvens e não faz parte de nenhuma camada do sistema S-Wallet.

4.6 *Considerações Finais deste Capítulo*

Este capítulo mostrou as principais características do sistema S-Wallet, a estrutura desenvolvida para esse sistema, com as explicações sobre a conta S-Wallet, as operações e as comunicações que ocorrem no fluxo do pagamento móvel e o protocolo SWEP. Finalmente, foi apresentado a App S-Wallet.

O próximo capítulo apresenta o desenvolvimento do sistema S-Wallet, com definições do hardware utilizado, das interfaces de comunicação, do protocolo SWEP desenvolvido como uma *java applet*, da conta s-wallet e da App S-Wallet.

Capítulo 5

MÉTODO PROPOSTO

5.1 Introdução

Este capítulo descreve o desenvolvimento do sistema S-Wallet e do protocolo SWEP e algumas considerações sobre as funcionalidades desse sistema. O sistema S-Wallet deve satisfazer os requisitos apresentados de usabilidade, segurança e privacidade.

Com a finalidade de obter a usabilidade, a segurança e a privacidade e pela complexidade e relevância do sistema S-Wallet enfatiza-se o sistema cliente e a App S-Wallet. No entanto, são mostrados neste capítulo o desenvolvimento do sistema varejista, a conta S-Wallet e demais operações do sistema.

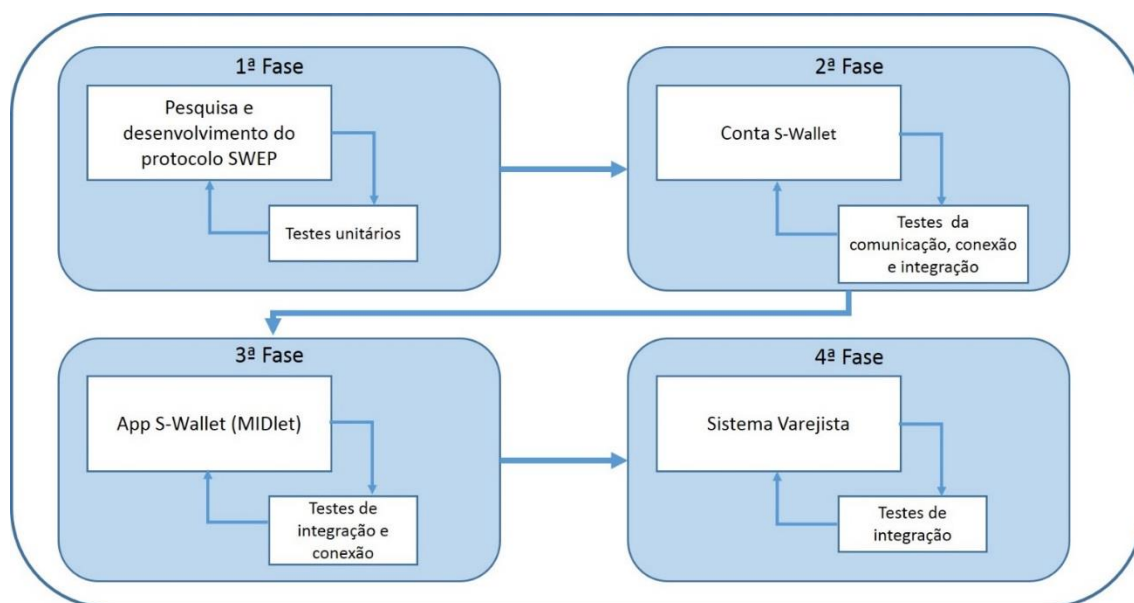


Figura 5-1 – Fases do desenvolvimento.

A estrutura utilizada para o desenvolvimento é descrita a seguir em termos da lógica de negócio e da estrutura do sistema S-Wallet. A Figura 5.1 ilustra como foi

desenvolvido esse sistema e a conexão entre cada um dos componentes. Estas etapas se tornam necessárias principalmente para alguns componentes que são utilizados durante os testes.

A primeira etapa deste trabalho é a pesquisa e o desenvolvimento do **protocolo SWEP** utilizando o *applet Java*, que efetua a inicialização da comunicação entre as duas entidades, a troca de dados, a codificação e a decodificação e a autenticação da transferência dos pagamentos móveis. Ao final dessas ações foram realizados testes.

A segunda etapa é o desenvolvimento da **conta S-Wallet**. Esta conta permite a pessoa que utiliza o sistema consultar e gerenciar seus dados bancários e seus créditos. A conta S-Wallet está armazenada em um servidor que se encontra nas nuvens (*cloud computing*). Os testes unitários de comunicação e a conexão foram realizados nessa etapa, primeiro isoladamente e posteriormente em conjunto com o protocolo SWEP.

A terceira etapa é o desenvolvimento da **App S-Wallet** utilizando o *MIDlet Java*, onde o protocolo SWEP está integrado no seu interior. Foi desenvolvido também uma aplicação gráfica que possibilita a interação com o usuário na camada de aplicação e uma interação com esse protocolo para realizar o fluxo de pagamentos móveis. Os testes de integração e a conexão foram realizados nesse momento.

A quarta etapa é o desenvolvimento da componente do **sistema varejista**, responsável pelas transações *Point of Sale* – Ponto de Venda (POS), que permanece no interior dos aparelhos NFC das lojas de varejo. Além dos testes unitários, foram realizados testes de integração com a conta S-Wallet e o protocolo SWEP.

Todos os testes de integração, conexão e segurança são apresentados no Capítulo 6 deste trabalho.

5.2 *Hardware utilizado*

Para a simulação de um serviço nas nuvens (*cloud computing*) representando a conta S-Wallet foram utilizados dois notebooks Samsung Chronos NP700, com Core I5, 6GB de RAM, usando um servidor Apache Tomcat [49]. A conta foi desenvolvida em Java utilizando o kit de desenvolvimento Java Card para facilitar a integração com a aplicação Android.

Como a NFC é uma tecnologia em desenvolvimento e sua integração junto aos dispositivos móveis ainda é pequena, a escolha final do dispositivo a ser utilizado foi o aparelho Galaxy S III, com processador Cortex-A9 de 1.4 GHz Quad-core, 1 GB de RAM e Android OS, v4.0.4 (*Ice Cream Sandwich*).

A aplicação para Android foi desenvolvida em Java utilizando a IDE para Eclipse [50] e a plataforma Android SDK. Neste trabalho a aplicação S-Wallet foi desenvolvida de forma básica com o objetivo de testar a comunicação do protocolo e a conclusão de uma troca de dados entre dois dispositivos com a aplicação instalada.

A principal preocupação para escolher o leitor que auxiliaria nos testes do sistema S-Wallet era a necessidade dele ser compatível com as especificações da tecnologia NFC, denominada de ISO/IEC 14443 Tipo A & B e com NFCIP-1 (ISO/IEC 18092) [48]. Devido ao custo e a indisponibilidade do produto no mercado brasileiro foi escolhido o leitor Pegoda CL RD 701 da NXP/Philips [52]. Este leitor é compatível apenas com o ISO/IEC 14443 Tipo A & B.

Neste trabalho foi desenvolvida a comunicação NFCIP-1 (*Peer-to-Peer*) para a troca de dados entre dois *smartphones*. Esse desenvolvimento permitiu provar o conceito desse tipo de comunicação.

5.3 Interfaces de Comunicação

As interfaces de comunicação definidas nesta dissertação são os meios que podem ser utilizados para a conexão entre os clientes durante um pagamento P2P e a conexão entre o cliente e o servidor para os pagamentos POS. Na arquitetura do sistema S-Wallet, as interfaces de comunicação são:

Comunicações locais: leitores compatíveis com os protocolos ISO/IEC 14443 A & B e ISO/IEC 18092 NFC-IP1 [48];

Comunicações remotas: *General Packet Radio Service* (GPRS) e *Global System for Mobile Communications* (GSM).

A Figura 5.2 ilustra a arquitetura do sistema S-Wallet. Dois *notebooks* foram utilizados para simular a conta S-Wallet e o sistema varejista. A App S-Wallet pode usar uma rede 3G ou uma conexão WiFi disponível para acessar a conta S-Wallet. Em ambos os casos é utilizado um túnel TLS para estabelecer um canal seguro. O leitor NFC Pegoda CL RD 701 foi conectado no *notebook* para simular o varejista.

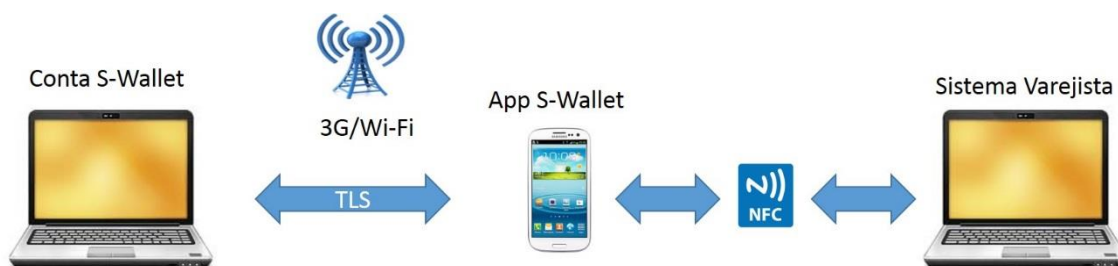


Figura 5-2 – Arquitetura do protótipo de testes do sistema desenvolvido neste trabalho.

5.4 *Applets Java – Proctolo SWEP*

Uma *Applet* pode ser definida como um software aplicativo que é executado no contexto de outro programa, como por exemplo, um web browser. Uma *applet* geralmente executa funções bem específicas.

Diferente de um programa, uma *applet* não pode ser executada independentemente. Ela geralmente exibe uma parte gráfica e por vezes interage com o usuário. Entretanto, essas aplicações geralmente não possuem um estado definido (*stateless*) e possuem privilégios de segurança restritos. A *applet* deve ser executada em um pacote de dados (*container*), que é fornecido por um programa hospedeiro. Esse programa pode ser fornecido por meio de um *plugin* ou uma variedade de outros aplicativos, incluindo aparelhos móveis que suportam o modelo de programação da *applet*.

No sistema S-Wallet, o protocolo SWEP se comporta como uma *Applet Java*, onde o núcleo de toda a solução contém toda a lógica desse sistema. Para o desenvolvimento do sistema S-Wallet foi utilizado o *eclipse*, que é um *Integrated Development Environment (IDE) Open Source*. Para o desenvolvimento desse protocolo foi utilizado o *plugin* de ferramentas *Java Card Open Platform (JCOP)* [53] e a versão 3.0.2 do JCRE. O sistema operacional em que a *applet* é executada é o Android OS, v4.0.4.

Essa *applet* contém os metadados que representam as funções de codificação, decodificação, conexão e troca de dados do sistema S-Wallet.

A *applet* deve permitir executar as seguintes operações:

- Conexão segura *peer-to-peer* entre dois smartphones;

- Troca de certificados e autenticação por chaves de criptografia;
- Envio de dados codificados e seguros;
- Conexão com o ambiente externo de nuvem (*cloud computing*);
- Codificação e decodificação de dados; e
- Inicialização do recibo das operações efetuadas e manutenção de um histórico.

Além de desenvolver operações básicas de um protocolo de pagamentos móveis, foi preciso também definir o comportamento de erros quando uma operação não era finalizada. Para essas operações, os erros existentes são:

- Dados inválidos (*DATA_INVALID*) – os dados fornecidos à *applet* são inválidos;
- ID duplicado (*DUPLICATE_ID_REGISTER*) – tentativa de registro de um mesmo ID;
- Entidade não encontrada (*ENTITY_NOT_FOUND*) – uma tentativa de conexão fornece um erro ao não encontrar a entidade denominada para a conexão;
- Memória excedida (*OUT_OF_MEMORY*) – a alocação de memória para determinado registro de transações não executado com êxito; e
- Transação mal sucedida (*TRANSACTION_FAILED*) – A troca de dados entre as duas entidades de forma não adequada.

A *applet* também trata erros a nível da camada de transporte, por exemplo, quando o tamanho dos dados não é o esperado ou a aplicação executa um comando não suportado.

O sistema S-Wallet também possui outras *applets* que compõem a estrutura que permite à App S-Wallet realizar todas as suas operações. Trata-se aqui de um módulo intermediário (*middleware*) que é formado pelas classes que são descritas a seguir.

A classe *ProtocolSWEP* tem a capacidade de iniciar a *applet* do protocolo SWEP e realizar uma integração com toda a estrutura da aplicação. Essa classe possibilita o início do fluxo de pagamentos móveis.

As classes *SystemPolicy* e *ConnectionPolicy* apresentam todas as principais políticas de estrutura e funcionamento do sistema S-Wallet e as principais políticas de conexão desse sistema, respectivamente.

A classe *AbstractApplet* disponibiliza as funções genéricas comuns as várias *applets* da App S-Wallet, como tratamento básico das mensagens.

A *applet* *MobilePaymentInfo* fornece as funcionalidades do início da conexão e do pedido de serviço. Ela ainda armazena essas informações inicializadas pelo receptor do pagamento até que o emissor contate essa *applet* para obter tais informações.

A classe *HistoricMPayment* representa a informação sobre o pagamento fornecido pelos dispositivos emissor e receptor durante as transações. No conjunto de informações do receptor encontram-se os dados que não são interpretados pela *middleware*, com exceção das políticas de conexão.

Os algoritmos de criptografia utilizados para o protocolo foram: Rivest, Shamir e Adleman (RSA) [54] de acordo com a versão 1.5 do padrão *Public-Key Cryptography Standards* (PKCS #1) e também Triplo DES (3DES), sigla para *Triple Data Encryption Standard* [55]. Nas assinaturas digitais foi utilizado o algoritmo de *Hashing Secure Hash Algorithm* (SHA-1) [56].

Neste trabalho, inicialmente desenvolveu-se um protótipo da arquitetura criptográfica do protocolo para saber se o *smartphone* utilizado para os testes teria a capacidade computacional para realizar os cálculos do sistema S-Wallet. Após os testes decidiu-se utilizar para as funções criptográficas a versão 1.46 da biblioteca Bouncy Castle [57].

5.5 *Conta S-Wallet – Base de Dados/Cloud Computing*

No sistema S-Wallet, a conta S-Wallet é uma aplicação servidor que está armazenada nas nuvens (*cloud computing*) podendo ser acessada de qualquer dispositivo e de qualquer lugar do planeta. Não foi realizada a implementação completa dessa conta, apenas uma simulação de sua atuação nesse sistema.

A simulação da conta S-Wallet é realizada em um *notebook* e consiste em um servidor que fornece um ponto de conexão TCP. Foi realizada uma simulação de um servidor escrita em Java utilizando *Apache Tomcat*.

A simulação deve ser conectada a um banco de dados de armazenamento como o MySQL [58] para armazenar o histórico das transações e dos créditos dos usuários. Um processo de limpeza pode ser realizado em separado para eliminar os dados antigos do banco do histórico das transações.

Foi utilizada na conta S-Wallet uma solução simples da conexão TCP, utilizando a filtragem por TLS. A biblioteca *Bouncy Castle* foi usada para os cálculos criptográficos. Parte da solução da conexão do protocolo SWEP foi implementada na conta que possibilita as operações de identificação (login), requisição de crédito e armazenamento das transações.

Neste trabalho foi desenvolvido uma estrutura que permite o registro dos usuários para associar IDs para cada um deles e assegurar um dos atributos do sistema S-Wallet que é a privacidade. Este processo assegura também que a mesma pessoa não pode se registrar várias vezes, impossibilitando assim uma tentativa de ataque de força bruta (*brute-force attack*) com a finalidade de obter os créditos sem a autorização da conta.

5.6 *Componente Java Micro Edition (App S-Wallet)*

A componente *Java Micro Edition* (ME) é basicamente uma *MIDlet J2ME* que fornece a interface para que o usuário do *smartphone* acesse e gerencie seus dados da conta e possa estabelecer uma conexão com outros usuários e entidades. Essa componente funciona como intermediária entre o usuário, o protocolo SWEP e a conta S-Wallet. Assim como as *applets*, essa *MIDlet* foi desenvolvida no *IDE Eclipse*, recorrendo ao J2ME, um subconjunto da plataforma Java 2 [59].

A *MIDlet* implementa os algoritmos que gerenciam a troca de informações entre o protocolo SWEP e a interface do usuário. Essa *MIDlet* pode obter as informações que são solicitadas ao usuário durante as etapas de identificação, registro, conexão e transação. Depois de obter tais informações, elas são armazenadas em um banco de dados da *MIDlet* e apresentadas ao usuário recorrendo ao visor do *smatphone*.

A *MIDlet* está estrutura da seguinte forma:

- Camada de apresentação;
- Camada de execução; e
- Camada de comunicação.

5.6.1 Camada de apresentação

A camada de apresentação é responsável por apresentar o *layout* com as informações dos dados do usuário e do sistema S-Wallet, recorrendo a uma interface gráfica do utilizador ou *Graphic User Interface* (GUI).

O objetivo principal da camada de apresentação é interagir com o usuário, encaminhando os seus pedidos para a camada de execução. Essa interação possibilita a escolha do tipo de pagamento, identificação do usuário, registro da conta, aquisição do crédito e da consulta dos saldos, dos débitos e do histórico das transações. Tais operações são as principais funcionalidades da *MIDlet*.

O protocolo SWEF depende em grande parte da camada de apresentação, pois é nela que ocorre a entrada dos dados e as informações que são tratadas no seu interior. O principal objetivo deste trabalho é desenvolver uma interface simples e de fácil utilização. Para isso, o código dessa camada deve ser o mais genérico possível.

A identificação é um passo muito importante no desenvolvimento da *MIDlet*, pois sua adição permite a manipulação e o acesso aos dados apenas de quem possui conhecimento da senha PIN ou o reconhecimento da face se a mesma estiver disponível no *smartphone*. Essa função aumentou muito a segurança da App S-Wallet e com isso do sistema S-Wallet.

A Figura 5.3 mostra o *layout* da operação de identificação. Nesta operação, durante a inicialização o sistema S-Wallet solicita ao usuário o seu PIN e realiza a verificação dele com a conta S-Wallet.

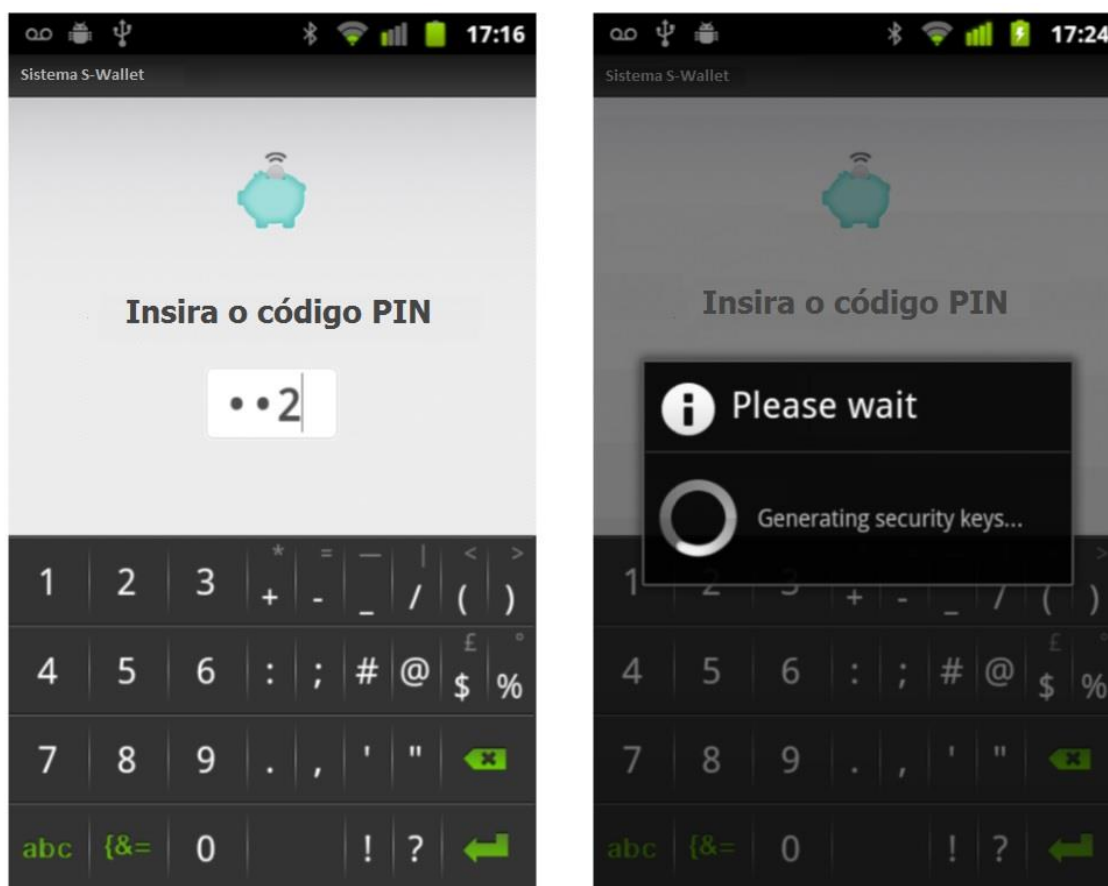


Figura 5-3 – *Layout* da operação de identificação do sistema S-Wallet

5.6.2 Camada de execução

A camada de execução é aonde a *MIDlet* interage com a *applet* do protocolo SWEP realizando o tratamento da informação que foi recebida na camada anterior. Nessa camada, os dados são gerenciados e utilizados em conjunto com o protocolo SWEP para iniciar uma conexão entre as duas entidades, realizar a troca dos dados, realizar o pagamento móvel e armazenar as informações das transações no sistema e na conta S-Wallet.

A Figura 5.4 ilustra o *layout* de uma execução de pagamento.

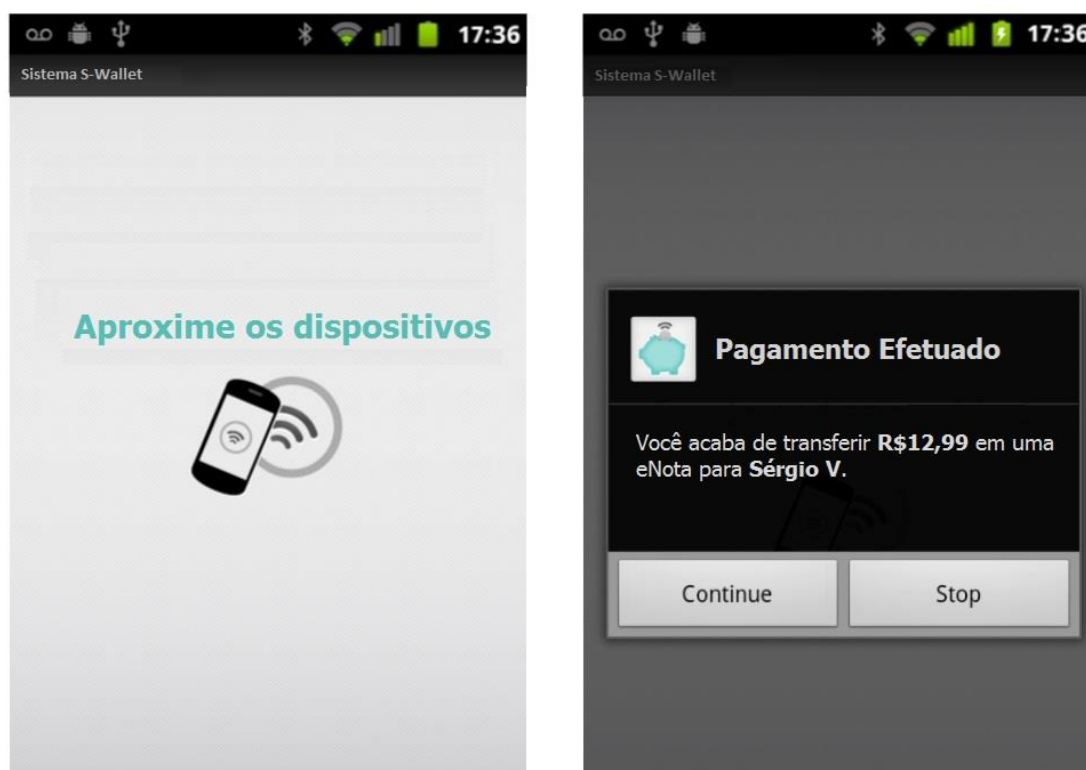


Figura 5-4 – *Layout* de uma execução de pagamento.

5.6.3 Camada de comunicação

A camada de comunicação fornece os pontos de acesso necessários para que a informação possa chegar até a *MIDlet* ou possa ser fornecida pela mesma. Essa camada permite ainda que a informação seja trocada por meio do GPRS, GSM, ISO/IEC 18092 NFC-IP1 e ISO/IEC 14443-A.

A camada de comunicação possui uma classe denominada *NFCIPMgr*, responsável por estabelecer a conexão com os outros dispositivos NFC (que também devem ter a App S-Wallet instalada) e enviar ou receber os dados.

A camada de comunicação também possui uma classe denominada *JavaMgr*, responsável por inicializar e enviar os comandos APDU que permitem comunicar com

as *applets*. A informação recebida nessa camada retorna posteriormente até a camada de apresentação.

A Figura 5.5 mostra o *layout* de solicitação de conexão para o pagamento P2P.

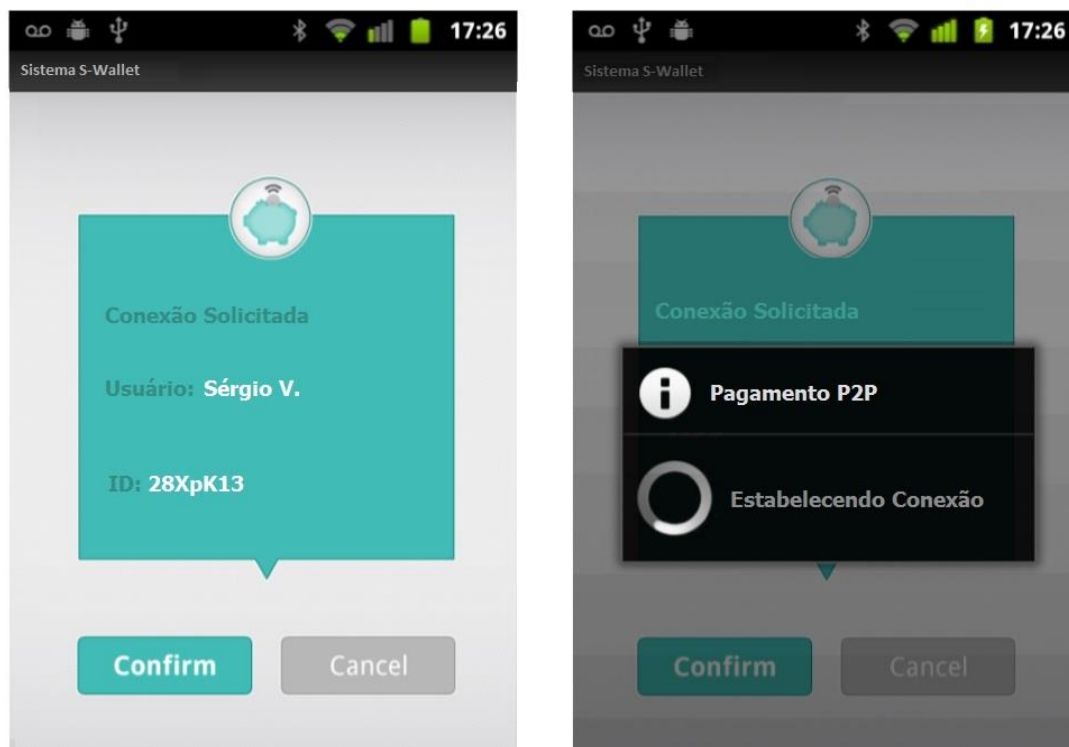


Figura 5-5 – *Layout* de solicitação de conexão para o pagamento P2P.

5.7 Sistema Varejista

O sistema varejista é executado em um *notebook*. Neste trabalho, ele foi desenvolvido em Java devido a existência de uma biblioteca NFC [60], que possui um desenvolvimento inovador do protocolo LLCP. Essa biblioteca também suporta os leitores NFC para *desktops* como o chip PN533 [61] e o leitor Pegoda CL RD 701 utilizado nesta dissertação.

Para desenvolver as operações de criptografia – 3DES, SHA-1, RSA, também foram utilizadas as bibliotecas da Bouncy Castle. Desenvolveu-se também uma interface gráfica mínima para os testes, uma vez que o pagamento POS não é o objetivo principal deste trabalho.

No sistema varejista não foi desenvolvido o armazenamento dos dados. Em um cenário real um equipamento de lojista deve ter capacidade de hardware e software para manter um banco de dados que possibilite a troca de informações entre a conta e a App S-Wallet.

As máquinas varejistas são construídas para não serem alteradas. Mesmo que um invasor tente acessar o banco de dados do equipamento, ele não é capaz de decodificar os dados presentes nessas máquinas. Esse invasor pode simplesmente ver os dados do histórico das transações, que possuem os valores e as datas. Mesmo assim, devido as características da criptografia utilizada no sistema S-Wallet os dados pessoais do ID e das senhas dos usuários permanecem inalterados.

5.8 *Considerações Finais deste Capítulo*

Este capítulo descreveu o desenvolvimento do sistema S-Wallet e do protocolo SWEP e algumas considerações sobre as funcionalidades desse sistema.

O próximo capítulo apresenta os resultados obtidos nos teste realizados utilizando o sistema S-Wallet para verificar o desempenho, a integração e a qualidade desse sistema. Também são apresentados os custos com hardware para o desenvolvimento do sistema S-Wallet.

Capítulo 6

RESULTADOS OBTIDOS

6.1 *Introdução*

Os testes do sistema S-Wallet começam pela análise do desempenho do protocolo SWEF em um *smartphone*, levando em consideração a limitação computacional desse dispositivo. Seguida pela análise dos custos de hardware para o desenvolvimento desse sistema e a realização de testes reais. Posteriormente, são mostrados os testes de integração do sistema S-Wallet em diferentes etapas de seu funcionamento. E finalmente, são analisados os testes qualitativos desse sistema.

6.2 *Desempenho do Protocolo SWEF*

O primeiro teste realizado analisa o desempenho do protocolo SWEF. O objetivo do sistema S-Wallet é propiciar rapidez no pagamento e segurança na troca de dados. A solução implementada apresentou *overhead* de 5 seg. nos cálculos computacionais relacionados à codificação e à decodificação criptográfica.

Devido à utilização de um hardware robusto como o do Galaxy S III (processador Cortex-A9), a utilização de codificações e assinaturas de segurança como RSA, 3DES e SHA-1 trouxeram o desempenho esperado ao sistema S-Wallet. Este sistema apresentou segurança e confiabilidade na troca de dados dos pagamentos com dinheiro virtual.

A Tabela 6.1 mostra os resultados obtidos no teste de desempenho do sistema S-Wallet.

Tabela 6-1 – Desempenho do sistema S-Wallet.

Atividade do Sistema	Tempo (ms)
Inicialização da MIDlet S-Wallet	1.350
Autenticação (Facial ou PIN)	1.850
Selecionar tipo de pagamento	210
Conexão P2P	770
Escolha do valor da eNota	500
Envio de eNota	3.570
Concluir transação/recibo de transação concluída	3.680
TOTAL	11.930

Pode-se verificar na Tabela 6.1, que a atividade do sistema S-Wallet que demanda mais tempo para ser realizada é justamente o envio da eNota e a troca de dados para a conclusão da transação. Essas duas atividades resultam em 7.250 ms, sendo respectivamente 3.570 e 3.680 ms. Isso ocorre devido à troca de certificados e as chaves criptográficas. O tempo total de duração das atividades realizadas por esse sistema foi de 11.930 ms.

A Tabela 6.2 ilustra os resultados do desempenho do sistema de segurança criptográfico da S-Wallet, levando em consideração os passos realizados pelo protocolo SWEP.

Tabela 6-2 – Desempenho do sistema de segurança criptográfico da S-Wallet.

Criptografia da S-Wallet	Tempo (ms)
Autenticação Conta S-Wallet/App	5.000
Troca de certificados App-1 / App-2	1.520
Codificação RSA (Passo 4)	377
Codificação RSA/3DES/SHA-1 (Passo 5)	585
Codificação 3DES (Passo 6)	150
Codificação 3DES (Passo 7)	148
Autenticação Final / Recibo de Transação	487
TOTAL	8.267

Pode-se observar na Tabela 6.2, que o tempo total do sistema criptográfico da conta S-Wallet foi de 8.267 ms. Ao aumentar o volume de dados trafegados, o resultado do cálculo do tempo de transação de 10 eNotas de um *smartphone* para outro foi de 14,8 segundos. Assim, quando os dois clientes já se encontram autenticados, a média de tempo do fluxo de dados entre a App-1 e a App-2 é de 1,48 segundos por eNota.

Independentemente do número de eNotas utilizadas, ocorreu um *overhead* de 4,8 segundos. Este valor pode ser considerado relativamente grande, levando em consideração à expectativa de desempenho esperado durante o desenvolvimento do protocolo SWEP. Esse *overhead* elevado foi devido aos protocolos de criptografia utilizados e o modo com que os *smartphones* se comunicam entre si.

A maior parte do tempo da codificação criptográfica é devido às operações da chave assimétrica (RSA). Pode-se verificar na Tabela 6-2 que o tempo total utilizado na codificação RSA (codificação RSA (Passo 4) + codificação RSA/3DES/SHA-1 (Passo

5)) foi de 962 ms. O *overhead* de utilizar o RSA é outra razão significativa para o tempo elevado da transação do sistema S-Wallet.

Esses resultados mostraram que o processador Cortex-A9 do Galaxy S III é capaz de realizar as operações computacionais necessárias para o protocolo SWEP. Mesmo assim, melhores tempos de envio e troca de dados podem ser obtidos melhorando continuamente o código do sistema S-Wallet.

6.3 *Custo do Hardware*

Inicialmente não foi considerado o custo total da inclusão do sistema S-Wallet em uma rede de varejo. O objetivo deste trabalho era propor o desenvolvimento da transação de pagamentos móveis entre dois usuários (P2P). Como o protocolo SWEP fornece suporte à um sistema varejista, é apresentado nesta dissertação o custo de hardware a ser introduzido em lojas para a utilização do pagamento móvel por meio da NFC.

Para cada loja do varejo fornecer o serviço de pagamentos móveis (POS) é necessário uma leitora com suporte a NFC. De acordo com estudos realizados pela Digi-Key Corporation [62], um chip PN544 NFC tem em média um custo de R\$17,00 por unidade e cada leitora deve possuir um. Verificando o preço de leitoras no mercado brasileiro, elas variam entre R\$1.700,00 e R\$4.000,00. Existe a opção do varejista realizar um contrato com uma administradora de cartão de crédito como por exemplo a Cielo e a Redecard. Ao realizar esse contrato ele recebe gratuitamente a leitora de cartões. Desse ponto de vista, o preço da inclusão de um chip NFC na máquina não aumenta significativamente o preço da leitora.

Do ponto de vista do pagamento entre usuários (P2P), o gasto necessário para a utilização dos pagamentos móveis é a aquisição de um dispositivo móvel que possua a tecnologia NFC. Atualmente, tais dispositivos se encontram entre a faixa de R\$1.599,00 e R\$2.199,00. O valor pago pela utilização da tecnologia mais recente no Brasil ainda é alto se comparado com outros países. Isso poderá vir a ser um empecilho para a expansão e a utilização dos pagamentos móveis.

6.4 *Testes de Integração*

A finalidade dos testes de integração é verificar as funcionalidades do sistema S-Wallet em relação ao seu desempenho, velocidade e integração entre o protocolo SWEP e esse sistema. Com esses testes é determinado se o desenvolvimento do sistema Wallet foi eficaz e suficiente para satisfazer as necessidades iniciais de usabilidade, segurança e privacidade.

6.4.1 Primeiro teste: inicialização da conta S-Wallet.

Neste primeiro teste o objetivo é iniciar uma conta básica dentro do sistema S-Wallet, para a utilização da conta S-Wallet. O primeiro passo é a instalação do App junto ao dispositivo móvel. Instalada a App, o usuário deve fornecer alguns dados para inicializar a sua conta e realizar a conexão com esse sistema.

Durante os testes foi concluído que o sistema S-Wallet se comportou de forma satisfatória e executou com rapidez e eficiência a inicialização da conta. Mesmo por meio de uma conexão 3G, o sistema conseguiu trocar dados com o servidor nas nuvens e realizar o registro de um novo usuário.

A Figura 6.1 mostra a tela de cadastro do sistema S-Wallet no *smartphone*.

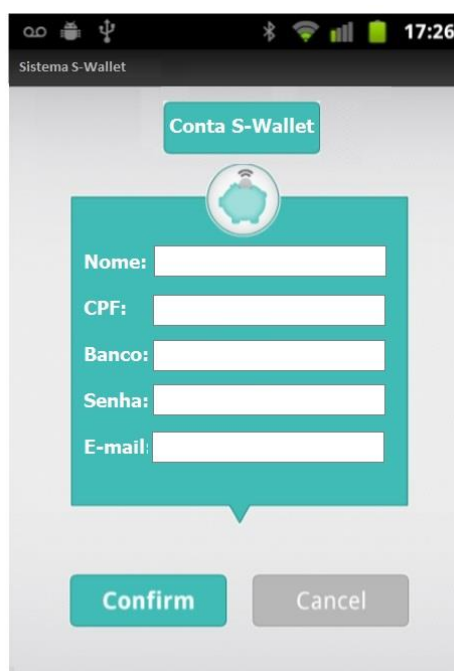


Figura 6-1 – Tela de cadastro do sistema S-Wallet no *smartphone*.

Como mostrado na Figura 6.1 os dados principais para a inicialização da conta S-Wallet são nome, CPF, nome do banco, senha e e-mail. Estes dados fornecem privacidade e anonimato nas operações de pagamento móvel ao usuário do sistema S-Wallet pela inicialização de um ID. Este ID é a identidade do usuário dentro de cada operação da App S-Wallet.

6.4.2 Segundo teste: conexão inicial entre dois usuários.

O objetivo deste teste é a realização de uma conexão entre dois usuários utilizando a App S-Wallet, para posteriormente fornecer ao sistema S-Wallet uma conexão estável. Possibilitando assim a troca de dados e a execução de pagamento pelo envio da eNota.

Após a visualização na App da disponibilidade do usuário nas proximidades do dispositivo móvel, solicita-se então uma conexão para iniciar o fluxo de pagamentos móveis. Nesta conexão testou-se a facilidade da conexão da App, a velocidade da conexão da App-1 com a App-2 de um segundo usuário de dispositivo móvel e finalmente a confiabilidade na troca dos dados entre as duas Apps.

Como mostrado na Figura 6.2, foram realizadas 20 tentativas de conexão entre dois dispositivos móveis, ocorrendo 3 conexões sem resposta e 1 queda na conexão devido a interferências no sinal. Destas 16 conexões realizadas corretamente, a velocidade de troca de dados entre os dois dispositivos móveis se mostrou estável a um nível de 212 kbp/s, como ilustrado na Figura 6.3.

Como das 20 tentativas de conexão, apenas 4 não foram realizadas corretamente, a confiabilidade na conexão/troca de dados foi de 80%. Este resultado ocorreu devido a algumas características de interferência da tecnologia NFC com outros sinais externos.

A Figura 6.2 mostra a taxa de conexão inicial entre dois usuários.

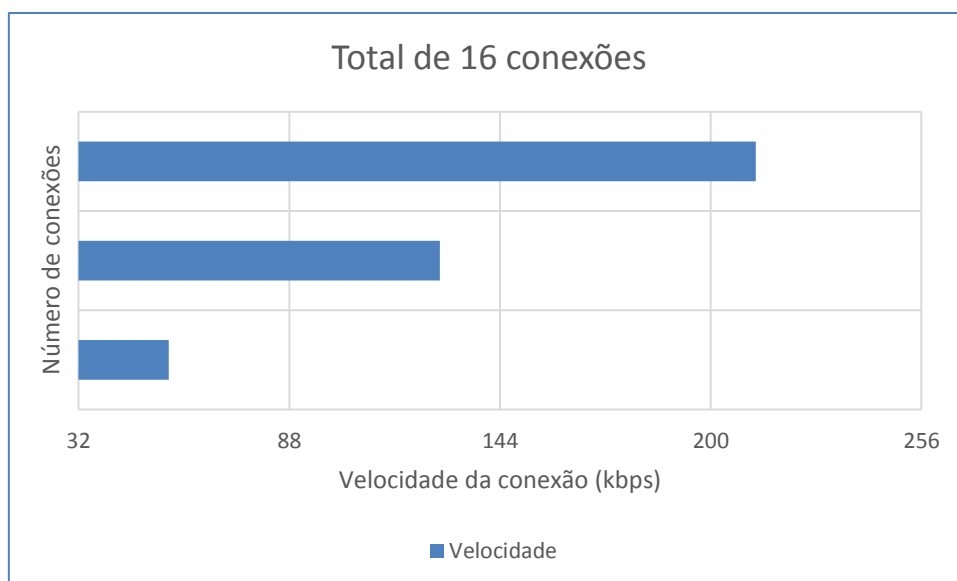


Figura 6-2 – Taxa de conexão inicial entre dois usuários.

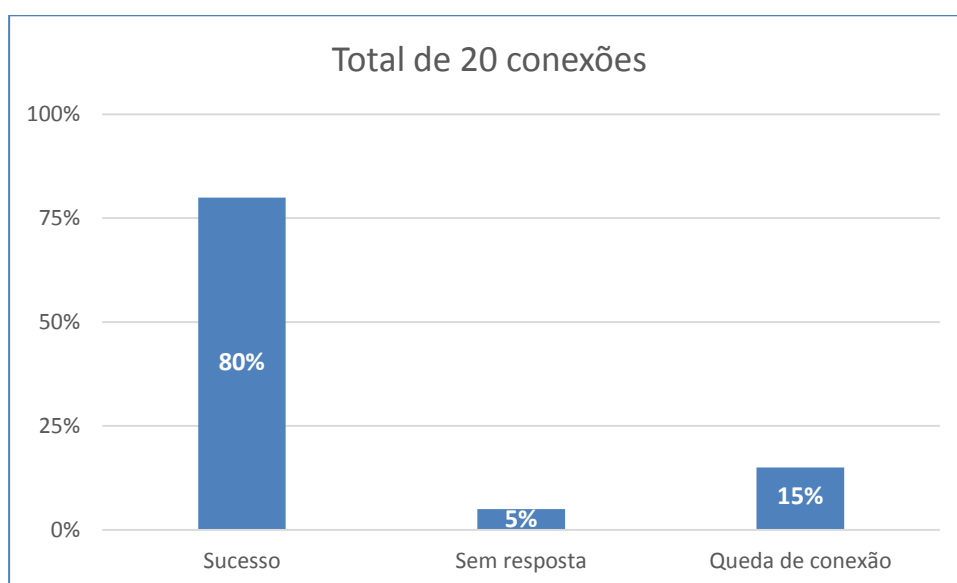


Figura 6-3 – Taxa de velocidade nas conexões realizadas com eficácia.

6.4.3 Terceiro teste: realização e execução de pagamento

A finalidade deste teste é verificar o funcionamento correto do fluxo de pagamento dentro do sistema S-Wallet. Em específico verifica-se aqui o funcionamento da funcionalidade da inicialização da eNota e do envio de dados entre dois dispositivos móveis.

Foram realizadas 50 tentativas de conexão em que o usuário primeiro deve verificar seu crédito junto a conta S-Wallet e depois transferir os créditos para a App S-Wallet. Com os créditos liberados na App, o usuário deve realizar a conexão com outro dispositivo (usuário) e efetuar o envio da eNota pela execução de um pagamento móvel.

Do total de 50 tentativas de conexão, 5 não foram realizadas corretamente. A falta dessas 5 conexões podem ser explicadas por interferências externas e pela distância indevida entre os dois dispositivos. Das 45 tentativas de conexão realizadas corretamente, a inicialização da eNota foi de 100%. Tratando-se de uma etapa puramente de codificação de dados, isso explica a porcentagem de acerto dessa etapa. A Figura 6.4 ilustra essa taxa de conexão inicial desses testes.

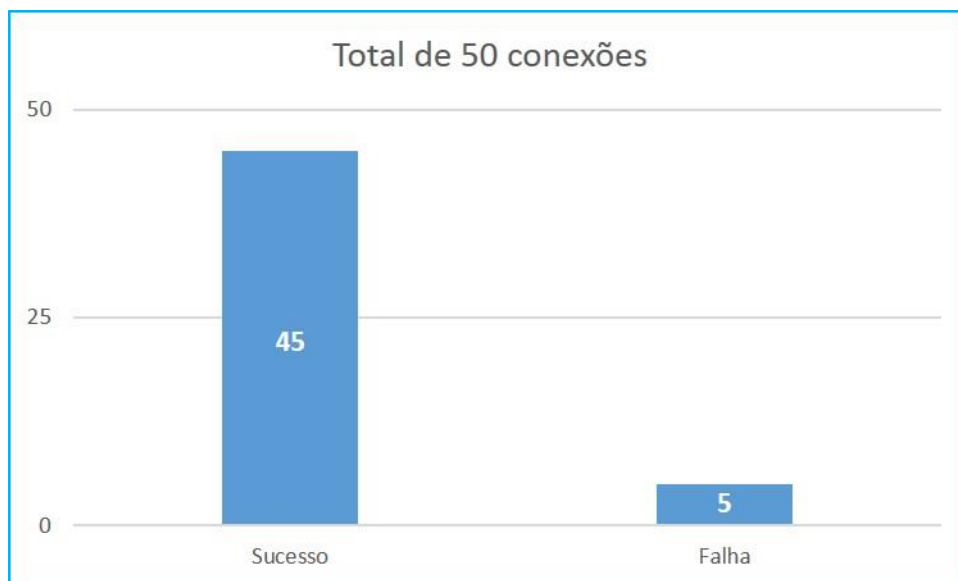


Figura 6-4 – Número de conexões realizadas no teste.

Para o envio dos dados entre os dois dispositivos, das 45 tentativas, 30 foram realizadas corretamente, 10 conexões falharam devido à queda da conexão entre os dois dispositivos e 5 testes apresentaram falha de recepção no dispositivo do usuário receptor. Como mostrado na Figura 6.5, a porcentagem de acerto dessa etapa do teste foi de 66% no envio de dados.

As 10 quedas de conexão ocorreram pela falha do sistema em realizar a codificação e a decodificação dos dados e também devido à falha do sistema de autenticação da conexão. As 5 falhas na recepção são explicadas por problemas de programação e linha de código do sistema S-Wallet.

A Figura 6.5 mostra a porcentagem de acerto nas tentativas de conexão e envio de dados.

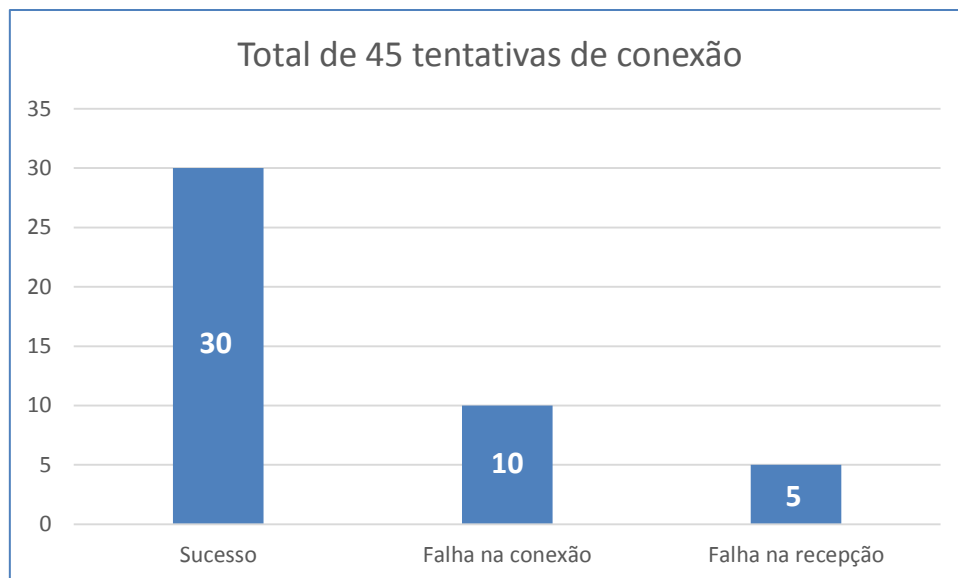


Figura 6-5 – Número de acerto nas tentativas de conexão e envio de dados.

6.4.4 Quarto teste: usabilidade da App

O objetivo do quarto teste é comprovar a usabilidade da App do sistema S-Wallet que é um dos pré-requisitos estabelecidos como base para o desenvolvimento deste trabalho. Neste teste são obtidas as seguintes informações:

- Determinação da facilidade de uso da App do sistema S-Wallet;
- Verificação do funcionamento da App do sistema S-Wallet em um cenário real;
- e
- Determinação da aceitação dos usuários ao pagamento móvel.

O teste de usabilidade da App do sistema S-Wallet foi realizado convidando 40 pessoas aleatórias para testarem o aplicativo embarcado em dois dispositivos móveis. Esse convite foi feito para estudantes de primeiro e segundo grau, universitários e

também pessoas comuns com capacidade de utilizar tal tecnologia. Todos eles realizaram os mesmos testes na App e responderam um questionário.

Durante o teste de usabilidade da App, foram realizadas cinco perguntas simples de resposta “**Sim**” ou “**Não**” para esses 40 convidados:

- 1) Existiu dificuldade para inicializar a aplicação no *smartphone*?
- 2) A velocidade de conexão com o outro dispositivo foi satisfatória?
- 3) A interface da aplicação facilitou sua utilização?
- 4) Você se sentiu seguro ao transferir dinheiro digitalmente utilizando o sistema S-Wallet?
- 5) Você trocaria o dinheiro de papel e passaria a utilizar a S-Wallet?

A Figura 6.6 mostra as respostas dos participantes do teste de usabilidade.

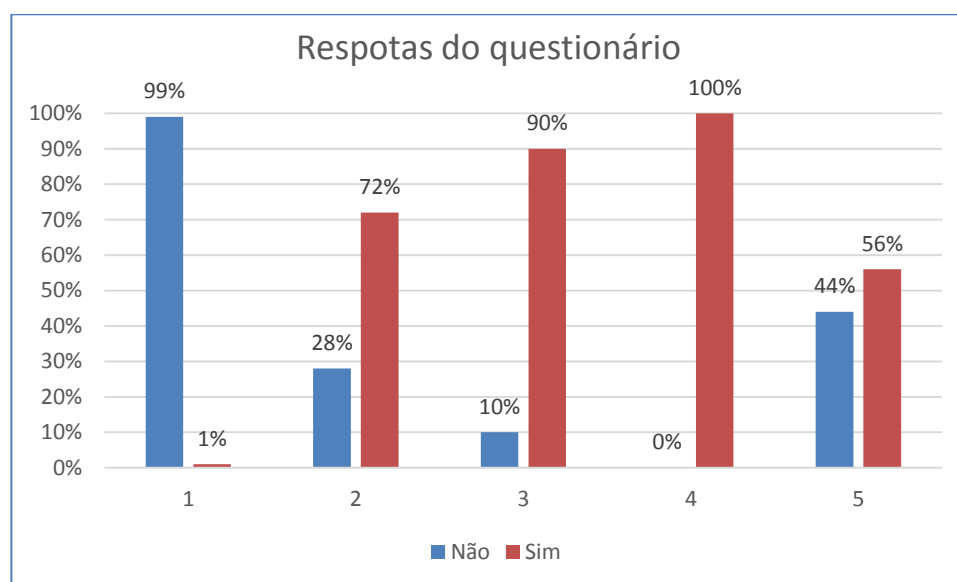


Figura 6-6 - Respostas dos participantes do teste de usabilidade.

Pode-se verificar na Figura 6.6 que a maioria dos usuários:

- i) Não sentiram dificuldades em trabalhar com a aplicação, muito menos manusear um *smartphone*. Isso é explicado pela massificação dos dispositivos móveis entre a população brasileira;
- ii) Como o ambiente utilizado para o experimento era externo, a velocidade de transmissão de dados foi satisfatória. Não ocorreu atrasos significativos para a conclusão de determinados testes;
- iii) A maioria dos usuários ficaram satisfeitos com a interface de uso e principalmente a facilidade dos botões e das configurações da aplicação. Possibilitando com isso um uso rápido e prático para os testes;
- iv) Como não foi utilizado o dinheiro de nenhum dos participantes do teste, o principal objetivo foi trabalhar a perda ou não de uma quantia devido a erros e falhas no sistema. A segurança do sistema S-Wallet foi de 100%, proporcionando assim uma aceitação e uma confiança por parte de todos eles; e
- v) A pergunta “Você trocaria o dinheiro de papel e passaria a utilizar a S-Wallet?”, mostrou que os usuários estão cada vez mais aptos e abertos a utilizar novas tecnologias. Mesmo assim, pelo resultado do questionário pode-se observar que quando se trata de dinheiro (quantia monetária), existe ainda um certo receio em digitalizar a carteira e utilizar uma e-wallet. A razão principal disso são as fraudes e os golpes que ocorrem na internet e que deixam os usuários com receio de perdas financeiras. A aceitação de mais de 50% dos usuários é suficiente para o desenvolvimento da tecnologia, mas não é o desejável para a expansão da mesma.

6.4.5 Sexto Teste: segurança do sistema S-Wallet

A segurança é um dos requisitos básicos para o desenvolvimento do sistema S-Wallet. Este sistema por trafegar dados que representam quantias monetárias foi cuidadosamente desenvolvido para proporcionar o máximo de segurança aos seus usuários.

Iniciando pela conexão de dados entre dois usuários ou entre um usuário e uma leitora NFC. Os objetivos do protocolo TLS são a utilização de criptografia para segurança, a interoperabilidade, a extensibilidade e a eficiência. Com os testes realizados de conexão foi observado que o protocolo cumpre com esses objetivos, garantindo assim 100% de conexão segura. Essa conexão segura inicial entre os “peers” da comunicação de pagamentos móveis, impossibilita tentativas de ataques como *Main in the Middle* e *DoS-Takeover*.

A troca de dados entre a conta S-Wallet e a App S-Wallet baseou-se em conexão TLS, autenticação por meio de certificados digitais e criptografia RSA. Nos testes realizados observou-se que a segurança foi significativa, uma vez que os dados não puderam ser capturados por mecanismos de análise de pacotes (*Sniffer*) em simulações de tentativa de invasão. Porém, o desempenho do sistema foi afetado pela necessidade de codificação e de decodificação dos dados a cada tentativa de conexão (*handshake*).

Finalizando pelo envio do recibo de execução e a conclusão de pagamento móvel para ambas as conta S-Wallet. Como se tratava de uma conexão simples de dados, a segurança baseou-se apenas na criação de um túnel TLS. Este túnel foi capaz de transmitir as chaves de criptografia dos dados até o servidor Apache TOMCAT que simulava a conta S-Wallet. Desta forma, os dados ao chegarem ao servidor foram

decodificados prontamente. Não ocorrendo alterações e ou interceptações no seu caminho desde a App S-Wallet até a conta S-Wallet.

O desempenho do sistema S-Wallet foi eficiente e muito seguro. Ao realizar os testes em todas as suas codificações esse sistema foi bastante eficiente. O sistema S-Wallet garante a confiabilidade na entrega dos dados e a segurança na execução de pagamentos móveis.

A Figura 6.7 mostra o gráfico dos testes de acompanhamento da rede pelo teste de análise de pacotes (*sniffer*).

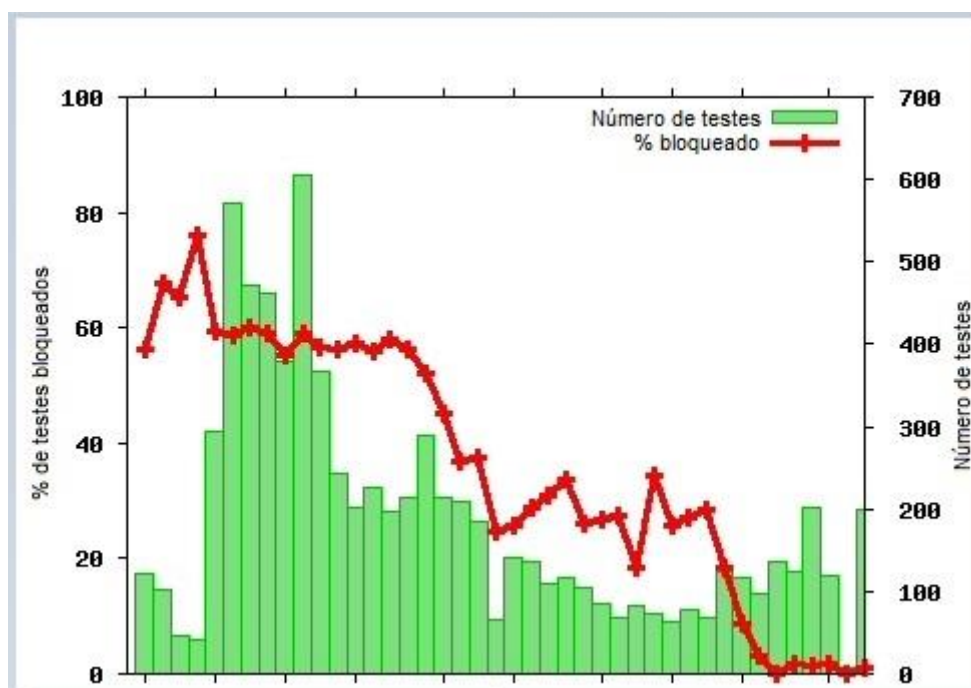


Figura 6-7 – Gráfico dos testes de acompanhamento da rede pelo teste de análise de pacotes (*sniffer*).

6.5 Testes Qualitativos

A seguir analisa-se o desempenho do sistema S-Wallet em relação a usabilidade, realização de micro pagamentos, segurança e privacidade.

Usabilidade: os resultados dos testes realizados com os usuários mostraram que essa característica foi obtida pela diminuição do número de passos necessários para que o usuário execute uma operação de pagamento.

Realizar micro pagamentos: os micro pagamentos dependem de taxas baixas por transação. O protocolo SWEP não exige que os varejistas permaneçam *online*. É o cliente que está conectado e realiza a conexão com a conta S-Wallet, assim os varejistas não dependem de custos extras para essa operação. É a conta S-Wallet que gerencia os créditos dos usuários. Para os bancos, o sistema S-Wallet é um serviço que fornece um diferencial para seu portfólio de produtos para captar clientes que necessitam armazenar dinheiro no banco para posteriormente obterem créditos e efetuarem pagamentos móveis.

Segurança: os protocolos de criptografia, assinaturas digitais e protocolos de conexão segura do SWEP possibilitam o estabelecimento de uma conexão segura entre os clientes e entre o cliente e a leitora NFC do varejista.

Privacidade: o sistema S-Wallet começa seu cadastro iniciando um ID e durante toda a operação do pagamento, os dados que são transferidos de um dispositivo para outro não contém informações sobre o usuário. Com essa utilização de um ID para a conexão e a troca de dados é garantida a privacidade do usuário.

6.6 Soluções existentes na literatura

Nos últimos anos vários autores desenvolveram protocolos de pagamentos móveis com características diferentes. Esta seção revisa algumas das propostas mais interessantes. Como as propostas incluem informações técnicas substanciais, é possível realizar uma comparação entre elas e o Sistema S-Wallet com relação as características mais importantes de um sistema para pagamentos móveis.

O protocolo de Horn e Preneel [71] fornece micro pagamentos baseado em créditos, onde cada valor deve ser múltiplo de 1 (um) crédito. Esses créditos são pré imagens de um valor inicial dentro de uma função de *hash* de apenas uma direção inserida no início do protocolo. O usuário se compromete assinando esse valor inicial e revela o número de créditos necessários para realizar o pagamento de um certo valor. Este protocolo não oferece suporte ao anonimato, requer uma *Trusted Third Party* – Terceira parte confiável (TTP) e uma chave privada armazenada com segurança no smartphone. Diferente do Sistema S-Wallet que não precisa de uma TTP, sendo a Conta S-Wallet que realiza essa conexão confiável com as entidades financeiras.

Kungpisdan, Srinivasan e Le [72] apresentam um protocolo de pagamentos móveis em paralelo com bancos. O protocolo assume que um gateway de pagamento é utilizado, a TTP, que as chaves compartilhadas existem entre o gateway de pagamento e o varejista, e entre o banco emissor e os clientes. Os clientes tem que executar um protocolo de registro de clientes na primeira vez que eles interagem com o varejista para estabelecer uma chave compartilhada. Funções de *hash* de uma direção são utilizadas para derivar chaves subsequentes em todos os casos. Utilizando estas chaves compartilhadas, o cliente gera mensagens que o varejista pode decodificar, e que incluem outras mensagens a serem decodificadas pelo banco emissor. Os varejistas se conectam ao gateway de pagamento, que em seguida conecta-se aos bancos emissor e receptor. O gateway de pagamento responde ao varejista com o resultado do pedido de pagamento. Este protocolo se baseia apenas em criptografia simétrica, pois possui uma demanda computacional menor que operações de criptografia com chave pública. O protocolo oferece anonimato ao usuário, depende de TTP e armazenamento inviolável para armazenar chaves de longo prazo no smartphone. Comparado ao Sistema S-Wallet, essa proposta depende da execução em paralelo com um banco ou um gateway de

pagamento ou autenticação de chaves de segurança, sistema esse incorporado diretamente no protocolo SWEP do Sistema S-Wallet.

mFerio [73] é um protocolo de pagamentos P2P que se baseia no NFC. Ele é estritamente P2P, não sendo necessária nenhuma infraestrutura e ambas as partes permanecendo off-line. O mFerio depende do elemento seguro para conseguir armazenamento de dados seguro para seu dinheiro digital. Mesmo que esse chip de elemento seguro esteja em alguns smartphones, eles ainda não estão acessíveis para aplicações comuns. Hoje a API do Android não fornece acesso ao elemento seguro, impossibilitando o desenvolvimento de protocolos que se baseiam nesse hardware. O mFerio foi desenvolvido para transações entre dois smartphones, assumindo que os usuários estão se vendo e em contato. Com isso eles percebem se existe uma terceira parte tentando interceptar a sua transação. Mas existem algumas vulnerabilidades relativas ao pagamento para varejistas e também P2P. O Sistema S-Wallet foi desenvolvido para ser independente do elemento seguro. Com isso, pode se beneficiar da tecnologia do NFC sem depender do acesso por parte do fabricante ao elemento seguro de cada chip NFC do smartphone.

Kadambi, Li e Karp [74] também descrevem um protocolo de pagamentos móveis baseado em NFC que se baseia em protocolos bancários tradicionais, como o EMV [75] e cartões de crédito. Utilizando o elemento seguro em dispositivos móveis para emitir tokens de autorizações de pagamento eles gerenciaram a transferência segura de informações pessoais através de redes públicas. Este protocolo baseado em bancos requer que o varejista esteja online durante toda a transação. Os pagamentos são rastreáveis pelo banco, e requer armazenamento seguro como os smartcards ou o elemento seguro no smartphone. Uma PKI também precisa ser implementada onde cada cliente possui ao menos um par de chaves pública armazenado no elemento seguro do

smartphone. No Sistema S-Wallet, especialmente no bloco de aplicação que exerce o papel do varejista, permite que o pagamento seja executado quer o varejista esteja online ou off-line, possibilitando assim a execução da operação de débito e crédito do usuário e posterior crédito em conta do varejo em questão.

Kumar e Rabara [75] propõem uma arquitetura para pagamentos móveis baseado no NFC, focando em macro pagamentos. Uma arquitetura orientada aos serviços é apresentada e que tenta integrar com infraestruturas de pagamentos móveis existentes. Seu objetivo principal é melhorar a proteção dos dados do usuário, mais controle do usuário sobre as transações, e suporte para transações por proximidade e remotas pela internet. Sua arquitetura descreve um protocolo para macro pagamentos interligados com o banco que requer que os varejistas estejam online e se baseia em criptografia simétrica além de compartilhamento de chaves com o servidor *Mobile Payment Application Service Provider* (MPASP). O foco do Sistema S-Wallet é realizar micro pagamentos, diferente do proposto por Kumar e Rabara.

A Tabela 6-3 mostra de forma gráfica a comparação realizada acima referente as propriedades de cada uma das soluções de protocolos de pagamentos móveis existentes na literatura com o Sistema S-Wallet.

Tabela 6-3 – Comparação do Sistema S-Wallet com protocolos de pagamentos da literatura.

<i>Propriedades</i>	<i>[71]</i>	<i>[72]</i>	<i>[73]</i>	<i>[74]</i>	<i>[75]</i>	<i>S-Wallet</i>
Privacidade				X		X
P2P			X	X		X
Varejista Offline			X	X		X
Micropagamentos	X		X	X		X
Sistema Offline			X			X
Criptografia de Dados	X	X	X	X	X	X
NFC			X	X	X	X
Não Depende de Hardware para Segurança					X	X

6.6.1 Soluções propostas na Coreia do Sul [76]

O desenvolvimento tecnológico na Coreia do Sul em comparação com o resto do mundo. Os Coreanos amam seus smartphones. Uma pequena volta no metro em Seoul com suas dezenas de passageiros de várias idades e podemos verificar que o smartphone hoje é adotado muito mais que apenas um dispositivo de comunicação. Atualmente os coreanos não utilizam seu smartphone apenas para jogar, mas também para realizar compras.

O país possui hoje um grupo de empresas altamente voltadas para o que chamamos de Grupo do Comércio Móvel, no qual as organizações como companhias de serviço financeiro, telecomunicações, e governo trabalham em conjunto para desenvolver soluções de pagamentos móveis. Em seguida estão listados os principais desenvolvedores destas soluções:

i) Danal

Um dos fornecedores originais de pagamentos móveis. O serviço da Danal possibilita ao usuário efetuar pequenos pagamentos por meio de sua conta telefônica utilizando uma autorização fornecida por SMS. A empresa também desenvolveu um aplicativo chamado Bartong, o qual possibilita que usuários paguem por créditos de até \$300 (trezentos dólares) em localidades POS através de código de barras ou códigos QR visualizados através da tela do smartphone. A aplicação tem um bônus adicional de cupons de fidelidade para um variado número de cafés, restaurantes e lojas de conveniência.

ii) KG Mobilians

O M-Cash compete diretamente com o serviço de pagamento por conta da empresa Danal. Eles também desenvolveram uma aplicação para *smartphone*, denominada M-Tic, a qual fornece o mesmo propósito de pagamentos por código de barras e código QR que o sistema da Danal. Atualmente o sistema M-Tic não está automatizado para aceitar os números de registro de estrangeiros, impossibilitando que não coreanos utilizem a ferramenta. Juntamente com a Danal, a KG Mobilians possui 90% do mercado de pagamentos móveis da Coreia.

iii) Won Corp.

A Won mesmo sendo menor que as últimas empresas citadas, está atraindo atenção para sua aplicação SmartPay. Lançada em 2013, a aplicação possui apenas 0.1% do mercado de pagamentos móveis, entretanto é esperado que isso aumente 10% em 2015, resultando em alianças atuais com serviços financeiros como o Banco Hana e outras companhias de pagamentos móveis como a Danal.

6.7 Conclusões

Os testes do sistema S-Wallet começam pela análise do desempenho do protocolo SWEP em um *smartphone*, levando em consideração a limitação computacional desse dispositivo. Seguida pela análise dos custos de hardware para o desenvolvimento desse sistema e a realização de testes reais. Posteriormente, foram mostrados os testes de integração do sistema S-Wallet em diferentes etapas de seu funcionamento. E finalmente, foram analisados os testes qualitativos desse sistema.

O sistema S-Wallet apresentou um desempenho eficiente se comparado a outros sistemas na literatura como o Venmo [69] e o Bump [70]. Os testes apresentaram um

overhead em alguns momentos da troca de mensagens e da conexão, mas esse atraso foi pequeno se comparado a eficiência total desse sistema. Além disso o protocolo se mostrou adaptável a um *smartphone* que possui as mesmas especificações da maioria dos aparelhos do mercado. O sistema S-Wallet mostra com isso adaptabilidade a vários aparelhos.

Em relação ao custo do hardware, o valor pago pela utilização da tecnologia NFC e do leitor Pegoda mais recente no Brasil ainda é alto se comparado com outros países. Isso poderá vir a ser uma dificuldade para a expansão e a utilização dos pagamentos móveis e do sistema S-Wallet.

Nos testes de integração do sistema S-Wallet foram observados a usabilidade, a segurança e a privacidade desse sistema. No primeiro teste, na inicialização da conta S-Wallet esse sistema se comportou perfeitamente e executou com rapidez e eficiência a inicialização dessa conta. Mesmo por meio de uma conexão 3G, o sistema conseguiu trocar dados com o servidor nas nuvens e realizar o registro de um novo usuário.

No segundo teste, na conexão inicial entre dois usuários obteve-se uma confiabilidade na conexão/troca de dados de 80%. Assim, o sistema S-Wallet proporciona confiabilidade para uma conexão utilizada para dados financeiros.

No terceiro teste, na realização e na execução de pagamento obteve-se no envio de dados uma porcentagem de acerto de 66%. Com a análise desses dados é observado que o sistema S-Wallet proporciona confiabilidade dos dados e assegura a entrega entre as duas Apps do usuário emissor e do usuário receptor.

No quarto teste realizado, observou-se a usabilidade da App. Os usuários não sentiram dificuldades em trabalhar com a App e a velocidade de transmissão de dados foi satisfatória. A segurança do sistema S-Wallet foi de 100%, proporcionando assim

uma aceitação e uma confiança por parte de todos os usuários. Foi observado que ainda existe um certo receio em digitalizar a carteira e utilizar uma e-wallet. A aceitação de mais de 50% dos usuários em relação a digitalização do dinheiro é suficiente para o desenvolvimento da tecnologia, mas não é o desejável para a expansão da mesma.

Finalmente com os testes qualitativos do sistema S-Wallet observou-se que foram obtidas as características de usabilidade, realização de micro pagamentos, segurança e privacidade desse sistema.

Capítulo 7

CONCLUSÕES E CONTRIBUIÇÕES DESTE TRABALHO E TRABALHOS FUTUROS

7.1 *Introdução*

Neste capítulo são apresentadas as conclusões e as contribuições deste trabalho e os trabalhos futuros que poderão ser realizados a partir desta dissertação.

7.2 *Conclusões*

Neste trabalho foi desenvolvido um sistema de pagamentos móveis que foi denominado sistema S-Wallet. Nesta dissertação foi realizado uma pesquisa bibliográfica de tecnologias e propostas de sistemas já desenvolvidos. Com a pesquisa, chegou-se à conclusão de que a melhor tecnologia atual para utilizar nos pagamentos móveis é a comunicação por proximidade de campo (NFC).

Com a tecnologia NFC escolhida, a pesquisa teve como objetivo a análise e o desenvolvimento dos blocos de interação do sistema S-Wallet. Esses blocos podem ser descritos como o protocolo que realiza o fluxo do pagamento móvel, a aplicação que interage com os usuários e finalmente uma conta para armazenar remotamente o crédito das operações financeiras.

Para o protocolo de pagamento móvel foi desenvolvido o protocolo SWEF. Este protocolo tinha o objetivo claro de proporcionar principalmente segurança na comunicação e nas transações financeiras entre dois usuários. A segurança foi obtida por meio do desenvolvimento desse protocolo com técnicas de criptografia simétrica,

chaves de autenticação e técnicas de troca de mensagem para o início da conexão. O protocolo SWEF mesmo com um *overhead* de dados (atraso) se mostrou eficiente e seguro.

A aplicação, denominada neste trabalho de App S-Wallet foi desenvolvida de forma simples. Ela possui uma interface gráfica e funcionalidades para a interação com os usuários. O objetivo principal dessa aplicação para os testes do sistema S-Wallet era analisar a integração entre o protocolo SWEF e esse sistema. Também foi analisado na App S-Wallet características como usabilidade, segurança e privacidade. Essa aplicação durante os testes do sistema S-Wallet e os testes com os usuários apresentou facilidade de utilização, realização de micro pagamentos, além de segurança e privacidade na troca de dados pessoais.

A conta para acesso remoto denominada de conta S-Wallet foi desenvolvida no papel como uma proposta. Ela não foi desenvolvida completamente para os testes, apenas uma simulação de sua atuação junto ao sistema S-Wallet. Com isso, mostrou-se a interação entre a conta, o protocolo e a App S-Wallet do sistema S-Wallet.

Nos testes realizados foram obtidos resultados satisfatórios, devido a facilidade de integração entre a conta, o protocolo e a App S-Wallet propostas neste trabalho. Os resultados da troca de dados e do fluxo do pagamento móvel foram apropriados, pois mesmo com um atraso nesse fluxo é possível realizar um pagamento móvel entre dois usuários com segurança e eficiência.

7.3 Contribuições deste Trabalho

De acordo com os resultados obtidos nesta dissertação pode-se concluir que ela proporcionou novas contribuições para a área de telecomunicações em geral, especialmente na utilização de tecnologias de radiofrequência, comunicação por

proximidade de campo e computação móvel. Com essas contribuições é possível a realização de muitas pesquisas no desenvolvimento específico desse tema.

As contribuições deste trabalho são:

- A estrutura desenvolvida para o protocolo SWEP, por meio da utilização de técnicas de criptografia simétrica em conjunto com chaves de autenticação e inicialização da comunicação com confirmação de ambos os usuários. Essa estrutura desse protocolo é adaptável para qualquer plataforma de dispositivos móveis;
- A App S-Wallet pela sua simplicidade e facilidade em visualizar e executar os comandos, possibilita a aceitação de vários usuários realizarem pagamentos móveis;
- A conta S-Wallet, devido a sua capacidade de inclusão de dados bancários e de dados de operações telefônicas em uma conta armazenada em um servidor remoto nas nuvens. O trabalho contribuiu também para a comunicação dessa conta com uma aplicação móvel por WiFi ou 3G. Essa conta possibilita o desenvolvimento de uma infinidade de outras aplicações para a integração com o universo móvel; e
- E finalmente, a integração de todos esses micros sistemas ao sistema S-Wallet contribuiu para o desenvolvimento de um sistema que permite com segurança e eficiência realizar pagamentos móveis. Esse sistema pode ser integrado ao comércio e as transações P2P, minimizando o custo das operações financeiras atuais.

7.4 Trabalhos Futuros

Como trabalho futuro pode-se desenvolver um protocolo com chaves de criptografia, tais como as chaves AES e ECDSA. Estas chaves podem fornecer maior velocidade e maior desempenho para o sistema S-Wallet.

A rapidez do sistema de criptografia do sistema S-Wallet pode ser melhorada com a análise e o desenvolvimento de um código que se baseia em algoritmos híbridos utilizando chaves simétricas e assimétricas.

Além disso, como trabalho futuro, pode ser melhorada a interface com o usuário desenvolvendo um *layout* mais interativo. Pode-se com esse *layout* testar o sistema S-Wallet em cenários reais, trazendo resultados que poderão ser estudados. Esses estudos possibilitarão comparar esse sistema com outras tecnologias existentes tais como RFID, tarja magnética e *QR code*, ajudando a melhorar continuamente o sistema S-Wallet em futuras versões.

Com a expansão do sistema S-Wallet e após a sua consolidação, pode-se projetar a inclusão da App S-Wallet em lojas de aplicativos como a Play Store do Google e a iTunes da Apple para testes com um maior número de pessoas e a análise de comentários dos usuários durante os testes em cenários reais.

Espera-se também o desenvolvimento e a inclusão da NFC em outros dispositivos no mercado, como computadores de bordo de carros trazendo assim a possibilidade de expansão do sistema S-Wallet para outras áreas de pesquisa.

7.5 Considerações Finais deste Capítulo

Neste capítulo foram apresentadas as conclusões e as contribuições deste trabalho e os trabalhos futuros que poderão ser realizados a partir desta dissertação.

REFERÊNCIAS

- [1] **Berners-Lee, T. J., Cailliau, R., Groff, J-F., Pollermann, B.,** CERN, *World-Wide Web: An Information Infrastructure for High-Energy Physics*, Proceedings published by World Scientific, Singapore, ed. D Perret-Gallix, 1992.
- [2] **Rescorla, E.,** *Http over tls*, RFC 2818, 2000.
- [3] **Starr, T., Cioffi, J. M., Silverman, P. J.,** *Understanding digital subscriber line technology*, Prentice Hall, 1999.
- [4] **Perkins, A. B., e Perkins, M. C.,** *The Internet bubble: the inside story on why it burst--and what you can do to profit now!* , 2001 – Harper business.
- [5] **Gallaughier, J. M., e Downing, C. E.,** *Portal Combat: An Empirical Study of Competition in the Web Portal Industry*, Journal of Information Technology Management. Vol. 11, No. 1-2, 2000, pp. 13-24.
- [6] **Turban, E., Lee, J. K., King, D., Liang, T. P., e Turban, D.** *Electronic Commerce 2010 (6th ed.)*. Prentice Hall Press, Upper Saddle River, NJ, USA, 2009.
- [7] **Mouly, M., Pautet, M. B.** *The GSM System for Mobile Communications*. Telecom Publishing, 1992.
- [8] **Viterbi, A. J.** *CDMA: Principles of Spread Spectrum Communication*. Addison Wesley Longman Publishing Co., Inc., Redwood City, CA, USA, 1995.
- [9] **Holma, H. e Toskala, A.** *HSDPA/HSUPA for UMTS: High Speed Radio Access for Mobile Communications*. John Wiley & Sons, 2006.

- [10] **Sesia, S., Toufik, I., e Baker M.** *Lte, the UMTS Long Term Evolution: From Theory to Practice*. Wiley Publishing. 2009
- [11] **PC Magazine.** (2011b). *Smartphone Definition from PC Magazine Encyclopedia*. PC Magazine. Acessada em Agosto 20, 2012:
http://www.pcmag.com/encyclopedia_term/0,2542,t=Smartphone&i=51537,00.asp
- [12] **Butler, M.** Android: Changing the Mobile Landscape. *IEEE Pervasive Computing* 10, 1 (January 2011), 4-7. 2011.
- [13] **Hall, S. P. e Anderson, E.** *Operating systems for mobile computing*. J. Comput. Small Coll. 25, 2 (December 2009), 64-71, 2009.
- [14] **TELECO – Inteligência em Telecomunicações – 3G: 3ª Geração de Celular no Brasil.** Disponível em: http://www.teleco.com.br/3g_brasil.asp. Data de acesso: 20/08/2012
- [15] **PLUS Consultoria em e-commerce – E-commerce no Brasil.** Disponível em: <http://www.plusecommerce.com.br/p/e-commerce-no-brasil.html>. Data de acesso: 20/08/2012
- [16] **Gusev, M.** *E-Commerce A big step towards E-Bussiness*. Institute of Informatics Faculty of National Sciences and Mathematics, University St .Cyril And Methodius”, 2011.
- [17] **Dahlberg, T., et al.** *Past, present and future of mobile payments research: A literature review*. *Electronic Commerce Research and Applications* 7.2 (2008): 165-181.

- [18] **ABRAS – Associação Brasileira de Supermercados** – *Tecnologia poderá impulsionar reinvenção do dinheiro.* Disponível em: <http://www.abrasnet.com.br/clipping.php?area=5&clipping=31250>. Data de acesso: 21/08/2012.
- [19] **Urbino, N. P., et al.** *Mobile Payment: Uma visão geral.* FaSCi-Tech1.3 (2012).
- [20] **Shy, Oz.** *Person-to-person electronic funds transfers: recent developments and policy issues.* FRB of Boston Public Policy Discussion Paper 10-1 (2010).
- [21] **Armbrust, M., et al.** *A view of cloud computing.* Communications of the ACM 53.4 (2010): 50-58.
- [22] **Palmer, R. C.** *The Bar Code book: Reading, Printing, and Specification of Bar Code Symbols (3ª Ed.).* s.l. : Helmers Publishing, 1995.
- [23] **Worth Data.** Bar Code Structure. *A Bar Code Primer.* s.l. : Worth Data Inc., 2004.
- [24] **Worth Data Bar Code Primer** — Introduction. *A Bar Code Primer.* s.l.: Worth Data Inc., 2004.
- [25] **Gao, J. Z., Prakash, L. e Jagatesan, R.** *Understanding 2D-BarCode Technology and Applications in M-Commerce - Design and Implementation of A 2D Barcode Processing Solution.* San Jose State University: IEEE Computer Society, 2007. 0730-3157/0-7695-2870-8.
- [26] **Aim Global.** Magnetic Stripe. *Card Technology: Magnetic Stripe.* [Online] <http://www.didyouknow.cd/creditcards.htm>.
- [27] **IDAT Consulting & Education.** Overview of Magnetic Stripe Technology. *Web Site de IDAT Consulting & Education.* [Online] <http://www.idat.com/t-magstripe.html>.

[28] **RFID Journal**. The History of RFID Technology. *RFID Journal - The World's RFID Authority*. [Online] RFID Journal LLC.

URL: <http://www.rfidjournal.com/article/view/1338/1/129>.

[29] **RFID Journal LLC**. Q&A Section about RFID Uses & RFID Technology. *RFID Journal - The World's RFID Authority*. [Online] RFID Journal LLC.

[30] **Savi Technology**. *Active and Passive RFID: Two Distinct, but Complementary, Technologies for Real-Time Supply Chain Visibility*. s.l. : Savi Technology, 2002.

[31] **Cross, R.** Smart cards for the intelligent shopper. *Allbusiness.com*. [Online] Direct Marketing, 1 de Abril de 1996. <http://www.allbusiness.com/marketing/direct-marketing/554240-1.html>.

[32] **Farrell, J. J.** *Smartcards Become an International Technology*. s.l.: IEEE Computer Society, 1996. 0-8186-7658-2/96.

[33] **Ttfn.net**. ISO/IEC 7816-4 (first edition 1995--09-01). *ttfn.net*. [Online] http://www.ttfn.net/techno/smartcards/iso7816_4.html.

[34] **Nunes, R.** *APSE - Aplicações para Sistemas Embebidos*.

[35] **Smart Card Alliance**. *Contactless Technology for Secure Physical Access: Technology and Standards Choices*. s.l.: Smart Card Alliance, 2002.

[36] **NXP Semiconductors**. MIFARE from NXP Semiconductors. *NXP Semiconductors*. [Online]

[http://www.nxp.com/#/pip/pip=\[pfp=53422\]|pp=\[v=d,t=pfp,i=53422,fi=,ps=0\]||0||0](http://www.nxp.com/#/pip/pip=[pfp=53422]|pp=[v=d,t=pfp,i=53422,fi=,ps=0]||0||0).

[37] **NXP B.V.** *MIFARE Standard Card IC MF1 IC S50 Functional Specification revision 5.3*. 2008. 001053.

- [38] **NXP B.V.** *MIFARE Standard Card IC MF1 IC S70 Functional Specification revision 4.0*. 2007. 043540.
- [39] **Cassidy, R.** *Call For Entries Touching the Future: NFC Forum Global Competition*. NFC Forum. [Online] 2007.
http://www.nfc-forum.org/news/pr/view?item_key=ffc0422bbc6504e49.
- [40] **Ecma International**. *Near field communication white paper*. Disponível em <http://www.ecma-international.org/activities/Communications/2004tg19-001.pdf>, 2004.
- [41] **Ernst H. e Klemens B.** *Security in near field communication (NFC)*, Philips Semiconductors, Printed handout of Workshop on RFID Security RFID Sec 06, July 2006, URL:
<http://events.iaik.tugraz.at/RFIDSec06/Program/papers/002%20%20Security%20in%20NFC.pdf>.
- [42] **Oertel W., Hilty K., Kelter U., Wittmann J.** *Security Aspects and Prospective Applications of RFID Systems*, Bundesamt für Sicherheit in der Informationstechnik, Bonn, 11. January 2005, URL: http://www.bsi.de/fachthem/rfid/RIKCHA_englisch.pdf.
- [43] **Gerhard P. H.** *A practical relay attack on ISO 14443 proximity cards*. 2005, URL: <http://www.cl.cam.ac.uk/~gh275/relay.pdf>.
- [44] **Kim C., Mirusmonov M., e Lee I.** *An empirical examination of factors influencing the intention to use mobile payment*. Computers in Human Behavior, 26(3):310–322, 2010.
- [45] **Pousttchi, K.** *Conditions for acceptance and usage of mobile payment procedures*. In The Second International Conference on Mobile Business, pages 201–210. Citeseer, 2003.

- [46] **Schierz, P., Schilke, O., e Wirtz, B.** *Understanding consumer acceptance of mobile payment services: An empirical analysis.* Electronic Commerce Research and Applications, 9(3):209–216, 2010.
- [47] **Armbrust, M., et al.** *A view of cloud computing.* Communications of the ACM 53.4 (2010): 50-58.
- [48] **ISO 18092 (ECMA-340).** *Information technology telecommunications and information exchange between systems - Near Field Communication - Interface and Protocol (NFCIP-1).*
- [49] **Wiggers, C., Galbraith, B., Chopra, V. e Fowler, C.** *Professional Apache Tomcat.* Wrox, 2004.
- [50] **Eclipse Foundation.** *Eclipse - an open development platform.* Eclipse.org Home. [Online] <http://www.eclipse.org/>.
- [51] **Shin, D. H.** *Towards an understanding of the consumer acceptance of mobile wallet.* Computers in Human Behavior 25, no. 6 (2009): 1343-1354.
- [52] **Pegoda CL RD 701,** *PEGODA Contactless Smart Card Reader based on CL RC632, NXP/Philips,* [Online] <http://www.nxp.com/demoboard/MFEV700.html>.
- [53] **Janson, P.** *JCOP embedded security software.* IBM Zurich Research Laboratory. [Online] IBM. <http://www.zurich.ibm.com/jcop/>.
- [54] **RSA Laboratories.** *PKCS #1 v2.1: RSA Cryptography Standard,* Apr. 2002.
- [55] **IBM,** *The Cryptography Guide: Triple DES.* Cryptography World. [Online] <http://publib.boulder.ibm.com/infocenter/zos/v1r12/index.jsp?topic=/com.ibm.zos.r9.csfb400/tdes1.htm>

- [56] **Eastlake, D., e Jones, P.** *US secure hash algorithm 1 (SHA1)*. (2001).
- [57] **The Legion of the Bouncy Castle.** *Bouncy castle*, June 2011. URL: <http://www.bouncycastle.org/>.
- [58] **MySQL, A. B.** *MySQL reference manual*. (2001).
- [59] **Gong, L., e Ellison, G.** *Inside Java (TM) 2 Platform Security: Architecture, API Design, and Implementation*. Pearson Education, 2003.
- [60] **Lotito, A., e Mazzocchi, D.** OPEN-NPP: an open source library to enable P2P over NFC. In *Near Field Communication (NFC), 4th International Workshop on* (pp. 57-62). IEEE, March, 2012.
- [60] **NXP. Pn533** user manual rev 03, May 2011. URL: http://www.nxp.com/documents/user_manual/157830_PN533_um080103.pdf.
- [62] **Digi-Key Corporation.** *RFID ICs | Digi-Key*, June 2011. URL: <http://search.digikey.com/scripts/DkSearch/dksus.dll?keywords=pn544>.
- [63] **Philips Electronics WebPage.** URL: http://www.newscenter.philips.com/br_pt/standard/about/news/press/article-3017.wpd
- [64] **Wikipedia:** *Amplitude-shift-keying*, URL: [http://en.wikipedia.org/wiki/Amplitude shift keying](http://en.wikipedia.org/wiki/Amplitude_shift_keying).
- [65] **Ernst, H. and Klemens, B.** *Security in near field communication (NFC)*, Philips Semiconductors, Printed handout of Workshop on RFID Security RFIDSec 06, July 2006, URL: <http://events.iaik.tugraz.at/RFIDSec06/Program/papers/002%20-%20Security%20in%20NFC.pdf>.

- [66] **Burkard, S.** *Near Field Communication in Smartphones*. Berlin Institute of Technology, Germany, 2012.
- [67] **High Tech Aid.** *Introduction to Magnetic Stripe & Other Card Technologies*. High Tech Aid - Consulting on RFID, Barcode, AIDC. [Online] High Tech Aid. http://www.hightechaid.com/tech/card/intro_ms.htm.
- [68] **Pentz, J.** *Data card*. U.S. Patent No. D460.455. 16 Jul. 2002.
- [69] **Venmo.** *Venmo trends in social payments*, 2010, Maio 2012. URL: <http://blog.venmo.com/post/3291380355/venmo-trends-in-social-payments-2010>.
- [70] **Bump Technologies.** *The bump app for iPhone and Android*, Maio 2012. URL: <http://bu.mp/faq>.
- [71] G. Horn and B. Preneel. Authentication and payment in future mobile systems. In J.-J. Quisquater, Y. Deswarte, C. Meadows, and D. Gollmann, editors, *Computer Security — ESORICS 98*, volume 1485 of *Lecture Notes in Computer Science*, pages 277–293. Springer Berlin / Heidelberg, 1998.
- [72] S. Kungpisdan, B. Srinivasan, and P. Le. A secure account-based mobile payment protocol. In *Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC'04) Volume 2 - Volume 2*, volume 1 of *ITCC '04*, pages 35–39, Washington, DC, USA, 2004. IEEE Computer Society.
- [73] R. Balan, N. Ramasubbu, K. Prakobphol, N. Christin, and J. Hong. mferio: the design and evaluation of a peer-to-peer mobile payment system. In *Proceedings of the 7th international conference on Mobile systems, applications, and services*, pages 291–304. ACM, 2009.

- [74] K. Kadambi, J. Li, and A. Karp. Near-field communication-based secure mobile payment service. In Proceedings of the 11th international Conference on Electronic Commerce, pages 142–151. ACM, 2009.
- [75] S. Kumar and S. Rabara. An architectural design for secure mobile remote macro-payments. *Journal of Next Generation Information Technology*, 1(2), 2010.
- [76] Mobile Payment in Korea: Ready and Waiting - Posted on June 26, 2012 at 1:59 pm - <http://seoulspace.co.kr/blog/2012/06/26/mobile-payment-in-korea-ready-and-waiting/>