UNIVERSIDADE DO VALE DO RIO DOS SINOS - UNISINOS
UNIDADE ACADÊMICA DE PESQUISA E PÓS-GRADUAÇÃO
PROGRAMA INTERDISCIPLINAR DE PÓS-GRADUAÇÃO
EM COMPUTAÇÃO APLICADA
NÍVEL MESTRADO

TIAGO ANDRÉ JOST

UniPag

Um modelo de pagamento móvel voltado ao comércio ubíquo

São Leopoldo
2013

TIAGO ANDRÉ JOST

UniPag:

Um modelo de pagamento móvel voltado ao comércio ubíquo

Dissertação apresentada como requisito parcial para a obtenção do título de Mestre, pelo Programa Interdisciplinar de Pós-Graduação em Computação Aplicada da Universidade do Vale do Rio dos Sinos – UNISINOS

Orientador: Prof. Dr. Cristiano André da Costa

Co-orientador: Prof. Dr. Rodrigo da Rosa Righi

São Leopoldo

2013

J84u Jost, Tiago André

UniPag: um modelo de pagamento móvel voltado ao comércio ubíquo / por Tiago André Jost. -- São Leopoldo, 2013.

136 f. : il. color. ; 30 cm.

Dissertação (mestrado) – Universidade do Vale do Rio dos Sinos, Programa Interdisciplinar de Pós-Graduação em Computação Aplicada, São Leopoldo, RS, 2013.

Orientação: Prof. Dr. Cristiano André da Costa; Coorientação: Prof. Dr. Rodrigo da Rosa Righi, Escola Politécnica.

1.Arquitetura de rede de computador. 2.Computação móvel. 3.Transferência eletrônica de fundos. 4.Comércio eletrônico. 5.Carteira digital. 6.Computação ubíqua. I.Costa, Cristiano André da. II.Righi, Rodrigo da Rosa. III.Título.

CDU 004.72
004.75.057.5
004.77:336.71
658.84:004.738.5

Catalogação na publicação:
Bibliotecária Carla Maria Goulart de Moraes – CRB 10/1252

UNISINOS

UNIVERSIDADE DO VALE DO RIO DOS SINOS
Ciências Exatas e Tecnológicas
Programa Interdisciplinar de Pós-Graduação em Computação Aplicada – PIPCA

ATA DE BANCA EXAMINADORA DE DISSERTAÇÃO DE MESTRADO Nº 20/2013

Aluno: **Tiago André Jost**

Título da Dissertação: **"UniPag**
Um modelo de pagamento móvel voltado ao comércio oblíquo".

Banca:
Prof. Dr. Cristiano André da Costa
Presidente da Banca e Orientador - UNISINOS
Prof. Dr. Rodrigo da Rosa Righi
Membro da Banca e Coorientador – UNISINOS
Prof. Dr. Jorge Luis Victória Barbosa
Membro da Banca – UNISINOS
Prof. Dr. Claudio Fernando Resin Geyer
Membro da Banca - UFRGS

Aos dezenove dias do mês de agosto do ano de 2013, às 14h reuniu-se na sala 6B423, a Comissão Examinadora de Defesa de Dissertação composta pelos professores: Cristiano André da Costa, Orientador e Presidente, UNISINOS; Rodrigo da Rosa Righi, Coorientador, UNISINOS; Jorge Luis Victória Barbosa, UNISINOS; Philippe Olivier Alexandre Navaux, UFRGS para analisar e avaliar a Dissertação apresentada pelo aluno Tiago André Jost.
APÓS A DEFESA A BANCA SE REUNIU E CONSIDEROU O TRABALHO APROVADO.
A BANCA DESTACA A CONTRIBUIÇÃO DO TRABALHO E O DOMÍNIO DE DIVERSAS TECNOLOGIAS.

A Banca Examinadora, em cumprimento ao requisito exigido para a obtenção do Título de Mestre em Computação Aplicada, julga esta dissertação:

(X) APROVADA
( ) REPROVADA

São Leopoldo, 19 de agosto de 2013.

Prof. Dr. Cristiano André da Costa

Prof. Dr. Rodrigo da Rosa Righi

Prof. Dr. Jorge Luis Victória Barbosa

Prof. Dr. Claudio Fernando Resin Geyer

A Deus, minha família, orientador, colegas e amigos que me ajudaram com o apoio, amizade e ideias durante a realização deste trabalho.

AGRADECIMENTOS

Agradeço principalmente à minha família. À minha mãe Márcia e meu pai Danilo por sempre acreditarem que o presente mais importante que eles podem me dar é a educação, e à minha irmã, Carolina, por todo o apoio durante estes dois anos.

Ao professor Cristiano André da Costa, pela orientação e incentivo desde o início do curso.

Ao professor Rodrigo Righi, pela coorientação e pronta disponibilidade.

À Unisinos, pela qualidade dos professores, aulas e laboratórios, que facilitaram meus estudos durante estes dois anos.

À Getnet, por acreditar no meu potencial desde minha saída da Universidade e permitir que eu retomasse os estudos com seu total apoio.

A todos os demais professores e funcionários do PIPCA

RESUMO

O uso de dispositivos móveis como meio de pagamento vem crescendo ao longo dos últimos anos. Embora algumas implantações de carteiras digitais tenham sido bem sucedidas, ainda não existe um padrão a ser utilizado pelo mercado. Este trabalho tem como objetivo apresentar uma solução para pagamento móvel através da utilização de uma carteira digital. Esta solução deve ser heterogênea, sendo disponibilizada para o maior número possível de dispositivos móveis, como telefones celulares e tablets, e deve permitir o pagamento entre dois usuários sem a necessidade de conexão à internet. O trabalho também leva em consideração as informações de contexto do usuário, e busca oferecer uma solução diferenciada ao usuário final, através da interface da aplicação com um servidor de pedidos, a ser instalado no estabelecimento comercial. A segurança também é um item importante, e o modelo deve prever a utilização de um elemento seguro, garantindo a segurança das informações gravadas no dispositivo. Foi desenvolvido um protótipo da arquitetura proposta, denominado Unipag. O protótipo foi desenvolvido através da avaliação de quatro diferentes soluções de carteira digital, sendo duas soluções acadêmicas e duas soluções comerciais. O protótipo foi desenvolvido inicialmente para o sistema Android, e foram realizadas duas avaliações. A avaliação por cenários demonstrou a utilização com sucesso da aplicação em cenários de pagamento cotidianos. A avaliação de usabilidade demonstrou que o aplicativo é de fácil utilização, e 96% dos usuários utilizariam a aplicação se disponível. Os resultados encorajam o estudo e demonstram a viabilidade da solução.

Palavras-Chave: Carteira Digital. Pagamento Móvel. Pagamento Ubíquo. NFC. Comércio Móvel. Comércio Ubíquo.

ABSTRACT

The use of mobile devices as a payment device has been growing over the last few years. Although some deployments of digital wallets have been successful, there is still no standard to be used by market. This work aims to present a solution for mobile payment through the use of a digital wallet. This solution must be heterogeneous, being made available to the largest possible number of mobile devices such as mobile phones and tablets, and should allow payment between two users without internet connection. The solution also considers the context information of the user, and seeks to offer a different solution to the end user through the application interface with a server application to be installed on the premises. Safety is also an important item, and the model should provide for the use of a secure element, ensuring the security of information stored on the device. We developed a prototype of the proposed architecture, called Unipag. The prototype was developed by evaluating four different solutions digital wallet, two academic solutions and two commercial solutions. The prototype was initially developed for the Android system, and were assessed twice. The evaluation scenarios demonstrated the successful use of the application for daily payment scenarios. The usability evaluation demonstrated that the application is easy to use, and 96% of users would use the application if available. The results encourage the study and demonstrate the feasibility of the solution.

Keywords: Digital Wallet. Mobile Payment. Ubiquitous Payment. NFC. Electronic Payment. Ubiquitous commerce.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

3G	3rd Generation
ADT	Android Development Tools
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
APDU	Application Protocol Data Unit
API	Application Programming Interface
ATM	Automated Teller Machine
BIN	Bank Identification Number
CA	Certification Authority
CASTOR	CAsk for Storage and Transport Of access Restricted secrets
CPF	Cadastro Pessoa Física
DE	Data Elements
DF	Dedicated Files
DSS	Data Security Standard
DUKPT	Derived Unique Key Per Transaction
EC2	Elastic Compute Cloud
ECMA	European Computer Manufacturers Association
EF	Elementary Files
EMV	Europay Mastercard Visa
FMC	Fundamental Modeling Concepts
GB	GigaByte
GMT	Greenwich Mean Time
GPRS	General Packet radio service
GPS	Global Positioning System
HSM	Hardware Security Module
HTTPS	HyperText Transfer Protocol Secure
HW	Hardware
IBM	International Business Machines
IDE	Integrated Development Environment
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronic Engineers
IP	Internet Protocol

ISO	International Organization for Standardization
JAIS	Journal of the Association for Information Systems
JSON	JavaScript Object Notation
MF	Master File
MK	Master Key
MNO	Mobile Network Operator
MUCS	Model for Ubiquitous commerce supportMVC Model View Controller
NDEF	NFC Data Exchange Format
NFC	Near Field Communication
NIST	National Institute of Standards and Technology
NSU	Número Sequencial Único
OTA	Over The Air
P2P	Peer To Peer
PAN	Personal Area Network
PCI	Payment Card Industry
PDA	Personal Digital Assistant
PIN	Personal Identification Number
PIPCA	Programa Interdisciplinar de Pós-Graduação em Computação Aplicada
PKI	Public-Key Infrastructure
POS	Point Of Sale
QR	Quick Response
RAM	Random Access Memory
RCA	Root Certificate Authority
REST	Representational State Transfer
RFID	Radio-Frequency IDentification
RG	Registro Geral
RN	Requisito de Negócio
RUP	Rational Unified Process
SAP	Systems, Applications and Products
SBP	Sistema Brasileiro de Pagamento
SE	Secure Element
SIM	Subscriber identity module
SMC	Secure Memory Card
SMS	Short Message Service

SO	Sistema Operacional
SOAP	Simple Object Access Protocol
TAM	Technical Architecture Modeling
TDEA	Triple Data Encryption Algorithm
TDES	Triple Data Encryption Standard
TEF	Transferência Eletrônica de Fundos
TSM	Trusted Service Manager
UC	Use Case
UML	Unified Modeling Language
UNISINOS	Universidade do Vale do Rio dos Sinos
URL	Uniform Resource Locator
USB	Universal Serial Bus
USSD	Unstructured Supplementary Service Data
VIP	Virtual Internet Protocol
VPN	Virtual Private Network
WAP	Wireless Application Protocol
WS	WebService

LISTA DE SÍMBOLOS

R$ Símbolo monetário da moeda brasileira (Real)

US$ Símbolo monetário da moeda americana (Dólar)

SUMÁRIO

1 INTRODUÇÃO

O dinheiro como conhecemos hoje é resultado de uma evolução ao longo da história da humanidade. A troca da produção excedente por outra mercadoria (escambo), bastante comum no início da civilização, não possuía nenhuma equivalência de valor. Naturalmente, algumas mercadorias passaram a ser mais procuradas, e consequentemente, eram aceitas por todos, assumindo então o papel de moeda (BANCO CENTRAL, 2012). Posteriormente, evoluiu-se para o surgimento de moedas e cédulas de papel, cheques e cartões de débito e crédito, também conhecidos como “dinheiro de plástico”.

Com a evolução da tecnologia, é natural que antigos meios de pagamento sejam evoluídos ou mesmo substituídos por equivalentes mais práticos e/ou seguros. Um caso clássico é a utilização do cheque, que teve sua participação caindo gradualmente na última década. De acordo com a Serasa(2010), possuidora de um vasto banco de dados sobre consumidores, houve uma redução de 57% no volume de cheques compensados na última década. Esta queda ocorreu a partir da implantação do Sistema Brasileiro de Pagamento (SBP) e também pela popularização dos cartões de crédito e débito (BANCO CENTRAL, 2004).

Com a tecnologia embarcada em praticamente todas as nossas ações do dia a dia, é natural que o dinheiro seja substituído pelo seu análogo digital, aqui chamado de moedeiro eletrônico ou carteira digital, do inglês *digital wallet*. De acordo com (VISA, 2012), uma carteira digital compreende todos os serviços de pagamento eletrônico, geralmente realizados através de um telefone móvel, que fornece acesso às diversas contas do usuário, da mesma maneira que os diversos cartões que possuímos em nossa carteira física. Por definição, uma carteira digital deve possuir a seguintes características (VISA, 2012):

- Armazenamento seguro de informações pessoais;
- Suporte a múltiplos meios de pagamento (cartões de crédito, débito e fidelidade, por exemplo);
- Suporte a diversas tecnologias distintas;
- Possibilidade de seleção do cartão que o usuário irá efetuar um determinado pagamento.

Mobey (2011) fornece outra definição de carteira digital, realizada por um fórum desenvolvido para facilitar a adoção e desenvolvimento de um serviço financeiro móvel, em

que o caracteriza como uma funcionalidade de um dispositivo móvel que pode interagir de maneira segura com algum tipo de bem digital. Esta funcionalidade pode ser acessada somente através de um dispositivo móvel, que também pode gerenciá-la, e é totalmente controlada pelo usuário.

Um conceito relacionado com moedeiro eletrônico é o de pagamento móvel, do inglês *mobile payment*. Para Dahlberg (2007), pagamento móvel é todo aquele pagamento no qual uma das partes da transação é realizada em um dispositivo móvel (como um *smartphone*) através de uma rede sem fios. Inicialmente, era realizado através de SMS (*Short Message Service*), evoluindo para aplicações WAP (*Wireless Application Protocol*), USSD (*Unstructured Supplementary Service Data*), que é um protocolo de comunicação para troca de mensagens entre um dispositivo móvel e um servidor remoto, e mais recentemente, NFC (*Near Field Communication*), que permite a transferência de informações através da aproximação de dois dispositivos compatíveis.

ZWASS (1996) define comércio eletrônico como o compartilhamento de informações comerciais, o estabelecimento de relações comerciais e a realização de transações financeiras através das redes de telecomunicações. Já o termo *mobile-commerce*, também conhecido como *m-commerce*, é definido por (TIWARI e BUSE, 2007) como qualquer transação que envolva a transferência de propriedade ou direitos para utilização de bens e serviços, iniciada e/ou completada através de um acesso móvel, mediada por um computador e com a ajuda de um dispositivo eletrônico.

Outra definição que surge é comércio ubíquo, do inglês *ubiquitous commerce (u-commerce)* (WATSON, PITT, et al., 2002), que caracteriza-se pela realização da operação em qualquer lugar, a qualquer tempo (*anywhere, anytime*), através "do uso de redes ubíquas para suportar comunicações personalizadas, ininterruptas e transações entre uma empresa e suas diversas partes interessadas (*stakeholders*) para oferecer um nível de valor além do comércio tradicional", ou seja, é considerada uma extensão do comércio eletrônico. De acordo com (ZHANG, LIU e LI, 2009), *u-commerce* pode ser visto como uma extensão lógica do *e-commerce* e do *m-commerce*, sendo que *m-commerce* representa uma parte importante do *u-commerce*, pois possibilita que a comunicação entre negócios e pessoas aconteça a qualquer hora em qualquer lugar, através do uso de dispositivos móveis.

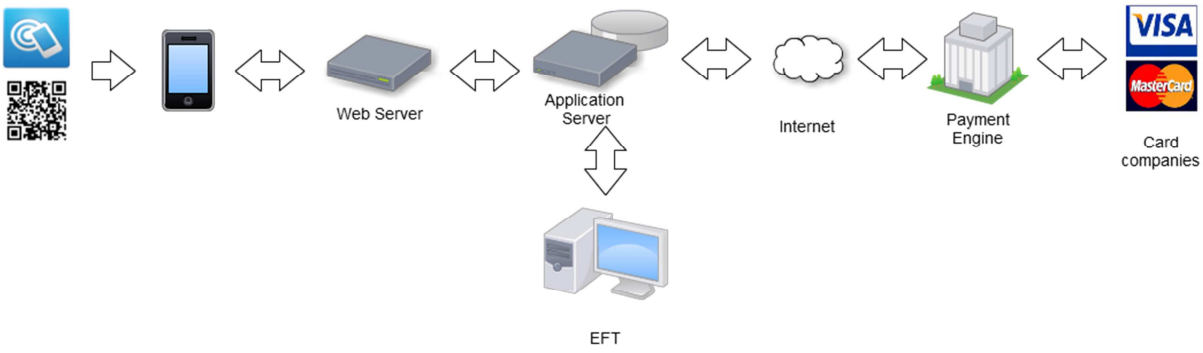
Diversas implementações de uma moeda digital já foram realizadas, sobretudo na Ásia, onde o sistema é utilizado para micro pagamento (*tickets* de trem/metrô) e compras de valor reduzido (até US$ 50). Um dos desafios desta área é expandir o uso, atualmente focado

no micro pagamento, para pagamentos efetuados no nosso dia a dia. Isto será possível se o moedeiro eletrônico incluir, além das tradicionais carteiras de *tickets*, a informação dos nossos cartões de crédito ou débito.

Outras informações que podem ser movidas para este novo meio são carteira de identidade, CPF, carteira de habilitação e passaporte, fornecendo um meio muito mais seguro para armazenamento destes dados. Este assunto é estudado com detalhes por Al-fedaghi (2006), onde uma carteira eletrônica com as informações pessoais é proposta. Além disso, uma aplicação de carteira digital também pode fornecer informações de contexto ao usuário, exibindo ofertas em pontos comerciais próximos, ou ao estabelecimento comercial, listando usuários próximos, permitindo uma comunicação direta entre o usuário e os estabelecimentos em que esteja cadastrado, sem que isto se torne invasivo.

Dessa maneira, UniPag consiste em uma proposta de carteira digital, com amplo suporte aos dispositivos móveis encontrados no mercado brasileiro. O trabalho deve ser construído de acordo com as boas práticas encontradas na literatura, além das práticas já consolidadas do mercado de transações eletrônicas (PCI/EMV). Os conceitos de comércio ubíquo também devem ser utilizados no desenvolvimento da proposta. Por fim, a aplicação deve suportar a integração dos pedidos efetuados e o pagamento, seguindo uma tendência do mercado. Para ilustrar o trabalho proposto, considere o cenário apresentado na **Erro! Fonte de referência não encontrada.**, onde é exibida a visão geral das entidades envolvidas em um pagamento eletrônico. O usuário A deseja efetuar algum tipo de pagamento. Observe o elemento carteira digital, que constitui o foco desse trabalho. Ele pode ser utilizado para realizar pagamento diretamente ao estabelecimento comercial, ou para efetuar transações entre dois usuários, o chamado pagamento *peer to peer* (P2P). Diversas tecnologias podem ser utilizadas para a comunicação entre as partes envolvidas, como *QR CODE* e *Bluetooth*.

Figura 1 Visão geral de um pagamento eletrônico com carteira digital



Fonte: Elaborado pelo autor.

UniPag tem como principal contribuição científica realizar o estudo de diversas soluções de carteira digital, pesquisando os pontos necessários para implantação da aplicação, como regras de segurança e gerenciamento do elemento seguro, listando os principais pontos positivos e adicionando novas funcionalidades, como sensibilidade ao contexto e *product order*. Além disso, podemos destacar a contribuição tecnológica de desenvolver, em parceira com uma empresa da área de transações financeiras, uma solução de moedeiro eletrônico que possa ser empregada no mercado.

1.1 Motivação

A primeira implementação de um sistema de comércio móvel foi realizada na Finlândia em 1997: uma máquina de refrigerantes foi programada para dispensar o produto através do recebimento de mensagens SMS. No mesmo ano, o primeiro serviço de *home banking* foi lançado também na Finlândia, utilizando o uso de SMS como meio de acesso. (ROSS, 2012).

Deste então, diversas alternativas para o pagamento móvel tem sido utilizadas, sempre acompanhando a evolução tecnológica dos telefones móveis. Com a crescente popularização dos dispositivos móveis, não apenas na forma de telefones, mas também na forma de *tablets*, é cada vez maior a quantidade de aparelhos com tecnologia suficiente para oferecerem um serviço de carteira digital. A recente disponibilização de dispositivos com tecnologia NFC permite que um dispositivo móvel emule a funcionalidade de um cartão de crédito, possibilitando o desenvolvimento de novas aplicações e funcionalidades (ROLAND, 2010). De acordo com (TECHCRUNCH, 2012) aproximadamente um milhão de novos dispositivos por semana são enviados às lojas já com esta tecnologia.

Muitos projetos-piloto na área de carteira digital foram desenvolvidos ao redor do mundo (INNOPAY, 2010). Entretanto, o único caso de sucesso, com uma base instalada de mais de 50 milhões de telefones, é a solução Osaifu-keitai, e está restrito ao mercado japonês (BOYD, J. 2005). A carteira digital Osaifu-keitai foi desenvolvida pela maior operadora de telefonia móvel do Japão, a NTT DoCoMo, que fornece seus aparelhos já com a tecnologia NFC.

As transações eletrônicas através da Internet serão responsáveis pela movimentação de aproximadamente US$ 963 bilhões em 2013 (TECHCRUNCH, J.P. MORGAN, 2011). Entretanto, diversas projeções a respeito da utilização em massa de uma carteira digital com utilização de NFC tem sido realizadas ao longo dos últimos anos, com o momento de ampla

adoção da tecnologia sendo sempre prorrogado. Segundo (REVEILHAC, 2009), em 2013 haveria 700 milhões de dispositivos móveis com NFC no mercado, número muito superior ao cenário atual. Com o estágio atual da tecnologia e utilização cada vez maior de telefones inteligentes (*smartphones*) e *tablets*, espera-se que os próximos anos sejam de extrema importância no desenvolvimento de uma solução para pagamento através do uso de uma carteira digital.

Desta maneira, a principal motivação de UniPag é o desenvolvimento de uma solução para carteira digital para utilização em um grande número de equipamentos, sem estar limitado à uma única tecnologia, através da utilização de tecnologias como NFC, QR CODE e *Bluetooth*. A utilização destas tecnologias distintas permite que o pagamento entre duas partes seja executado mesmo entre dispositivos com sistemas operacionais diferentes, ampliando o número de usuários que a solução irá atender.

1.2 Objetivos

As diversas tentativas de implementação de um sistema de carteira digital no mercado contribuem para um estudo profundo dos erros e acertos enfrentados pelos mais variados mercados ao redor do mundo (INNOPAY, 2010). Assim, este trabalho busca realizar um estudo geral do mercado, com ênfase em quatro modelos selecionados, buscando verificar suas características positivas e negativas, para então gerar um modelo final. A este modelo gerado, serão adicionadas funcionalidades como sensibilidade ao contexto e interface para solicitação de pedidos. Portanto, o objetivo principal do trabalho é o desenvolvimento de um modelo de carteira digital, utilizando tecnologias como NFC e QR CODE. Este modelo deve ser facilmente adaptável ao maior número possível de dispositivos, independente do sistema operacional ou hardware empregado. Deve possuir integração com o sistema de pedidos do estabelecimento comercial, e possibilitar o pagamento entre dois usuários que utilizem a aplicação. Também será implementado um módulo que permite a integração com um sistema de pagamentos já existente.

Como objetivos mais específicos, é possível destacar:

- Realizar estudos na área de comércio ubíquo, através de estudos dos trabalhos considerados estado da arte;
- Pesquisar os meios de pagamento móvel eletrônico e suas melhores práticas;

- Desenvolvimento de um protótipo da solução, que possa ser utilizado em diferentes dispositivos móveis;
- Realizar uma avaliação deste propósito, utilizando para isto uma metodologia em que serão elencados diversos cenários de uso. Nestes cenários de utilização, serão utilizados os mesmos critérios usados para avaliar os trabalhos relacionados, avaliando os benefícios da utilização do protótipo frente ao uso do dinheiro convencional, segurança transmitida pelo modelo ao usuário, heterogeneidade, eficiência e simplicidade.

Para conclusão destes objetivos, também se faz necessário o estudo da infraestrutura necessária para atender a um sistema com estas características, incluindo regras de segurança e contingenciamento.

1.3 Estrutura do Texto

O restante do trabalho encontra-se organizado em três capítulos, divididos da maneira a seguir:

- **Capítulo 2**: Revisão Bibliográfica;

  Apresenta diversas definições necessárias para o entendimento do projeto. Constitui a fundamentação teórica do trabalho, bem como uma revisão bibliográfica, cobrindo assuntos como computação ubíqua, comércio ubíquo, transações eletrônicas financeiras, regulamentação brasileira para transações financeiras eletrônicas, regulamentações mundiais sobre transações *offline*, carteira digital, tecnologias utilizadas pelas soluções de pagamento e seus padrões de segurança;

- **Capitulo 3:** Trabalhos Relacionados;

  Descreve os trabalhos relacionados, comparando os modelos estudados e termina com uma lista de lacunas a serem preenchidas pelo modelo a ser desenvolvido;

- **Capítulo 4**: Modelo UniPag;

  Detalha o modelo proposto, definindo sua arquitetura e os serviços necessários. Descreve os módulos Comercial, responsável pela comunicação da aplicação com o servidor de pedidos do estabelecimento comercial, Financeiro, que permite ao usuário efetuar um pagamento eletrônico, Carteira Digital, responsável pela

interface do usuário com o elemento seguro e Comunicação, responsável pela comunicação do modelo com os sistemas e periféricos externos;

- **Capítulo 5**: Implementação;

  Descreve os passos executados para a modelagem e implementação do protótipo para o sistema operacional Android, bem como ferramentas utilizadas na modelagem e desenvolvimento, como IDE Eclipse, SDK Android e dispositivos utilizados;

- **Capítulo 6**: Avaliação;

  Descreve a avaliação do protótipo, através de duas diferentes metodologias. A primeira avaliação é realizada através da avaliação por cenários, onde o protótipo é avaliado frente a cenários reais de utilização. Na avaliação de usabilidade, o protótipo é testado por usuários e são avaliadas características como efetividade, eficiência e satisfação;

- **Capítulo 7**: Conclusão.

  Apresenta as considerações finais, contribuições do trabalho desenvolvido e aprendizado adquirido ao longo do trabalho. Também são apresentadas sugestões para continuidade do trabalho.

2 REVISÃO BIBLIOGRÁFICA

Este capítulo tem como objetivo realizar uma revisão dos principais assuntos relacionados com trabalho, em que conceitos de pagamento eletrônico, móvel e ubíquo são revistos, bem como tecnologias e itens de segurança necessários para realizar estas operações. As possíveis tecnologias que tornam possível o pagamento móvel também são apresentadas.

2.1 Pagamento Eletrônico

Crédito é uma maneira de vender ou adquirir bens ou produtos sem que o comprador possua em mãos o dinheiro necessário, baseado na confiança que o pagamento será efetuado no futuro (INVESTOPEDIA, 2012). A utilização de um cartão de crédito é apenas um meio de automatizar este processo. Segundo Sienkiewicz, (2001), os primeiros cartões de crédito foram emitidos no início do século XIX. Seu uso era restrito a postos de gasolina, hotéis e empresas, que ofereciam estes cartões para seus melhores clientes, que podiam então usufruir dos seus serviços sem a necessidade de dinheiro ou cheque (BANCO CENTRAL, 2011). Estes cartões não possuíam uma abrangência muito grande, estando sua utilização restrita a algumas partes dos Estados Unidos. Inicialmente, apenas compras à vista eram permitidas, isto é, não era possível o parcelamento da fatura.

O primeiro cartão de crédito genérico, permitindo que consumidores efetuassem compras em múltiplos estabelecimentos, foi emitido em 1950 (DINERS CLUB, 2012). Ao efetuar uma reserva em um restaurante em Nova Iorque, o empresário Frank McNamara descobre que está sem sua carteira e viu-se obrigado a solicitar que sua esposa pague o jantar. Meses depois, Frank volta ao estabelecimento e, ao pagar sua conta, apresenta seu cartão *Diners Club*, e efetua o pagamento com a sua assinatura. Este é considerado pela indústria do pagamento como o marco inicial do dinheiro de plástico. Ainda na década de 50, a empresa American Express iniciou suas atividades, com a emissão de seus cartões de crédito, para ser utilizado em ramos de viagens e entretenimento (WOOLSEY, 2005).

Estas duas empresas operavam de uma maneira conhecida como *closed loop* (caminho fechado), onde a empresa emissora do cartão (*issuer*) autoriza e é responsável por todas as etapas da transação. A responsabilidade de cobranças do consumidor e pagamentos para o estabelecimento comercial também é da emissora do cartão. Embora tenha alcançado um relativo sucesso, este modelo de negócio ainda era muito restrito, pois obrigava aos estabelecimentos possuírem um contrato com cada um dos bancos emissores de cartões, e acabava não oferecendo muitos atrativos ao usuário final, que necessitava ter diversos cartões

para poder ser aceito em um maior número de estabelecimentos. Este modelo é apresentado na Figura 2.

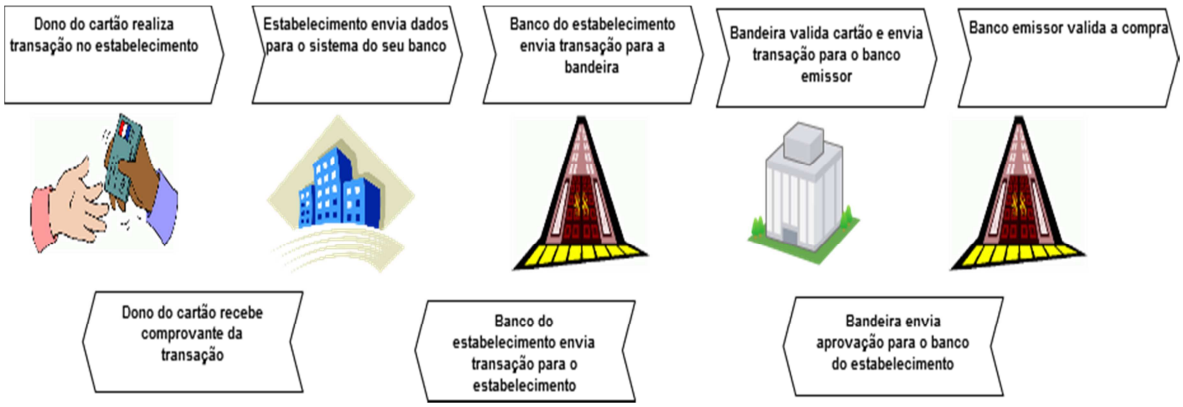
Apenas em 1966 foi criado o primeiro cartão de crédito genérico, quando o *Bank of America* criou sua unidade de cartões de crédito, permitindo que a franquia de sua marca *BankAmericard* (posteriormente rebatizado de Visa) seja utilizada em diversos bancos nos Estados Unidos. Na mesma época, outros bancos americanos se uniram e formaram a *Interbank Card Association* (posteriormente conhecido como Mastercard), para competir com o *BankAmericard*.

Figura 2 Modelo de transações financeiras closed loop

Fonte: Baseado em Mastercard (2008)

Estas duas novas entidades criadas operavam de uma maneira conhecida como *open loop* (caminho aberto). Neste modo, o banco do emissor do cartão não necessita ser o mesmo banco do usuário ou do estabelecimento comercial (*merchant*). Assim, as transações entre diferentes bancos necessitam ser processadas através de um sistema centralizado, que autoriza e quita as transações (*settle*). O banco do comerciante envia as informações para o banco do emissor, e o sistema centralizador realiza a transferência de dinheiro entre as duas partes. A transferência da transação do banco do comerciante para o banco do emissor e o consequente débito do emissor para o dono do cartão é conhecida como *interchange*, e é acompanhada de uma pequena taxa (MASTERCARD, 2008). O processo *open loop* (Figura 3) também é conhecido como sistema de pagamento *four party*, constituído do banco do estabelecimento, o banco do emissor, o comerciante e o consumidor final.

Figura 3 Modelo de transações financeiras open loop



Fonte: baseado em Mastercard (2008)

Cada emissor possui suas próprias taxas (emissão do cartão, anuidades etc.) com o usuário final, e também suas taxas cobradas do estabelecimento comercial. Entretanto, todos os bancos compartilham a mesma taxa para o *interchange*, estabelecido de acordo com a bandeira, tais como Visa ou Mastercard. Para uma mesma bandeira, esta taxa pode variar, de acordo com o ramo do estabelecimento comercial, ou seja, um hotel pode ter uma taxa de *interchange* maior que uma casa noturna.

De acordo com Banco Central (2004), um cartão de débito é um instrumento eletrônico de pagamento que permite o pagamento de bens e serviços através do débito *online* do valor, diretamente na conta do portador do cartão. Este cartão é sempre emitido pela instituição financeira onde o usuário possui uma conta bancária.

Um cartão de crédito é um instrumento eletrônico de pagamento que permite ao seu portador adquirir bens e serviços na rede credenciada. O portador do cartão possui um limite de crédito para as suas compras. Geralmente o cartão de crédito é adquirido junto a um banco, que em parceria com as administradoras de cartão, realiza a venda, gerencia o crédito e a cobrança das faturas. Este cartão também pode ser emitido diretamente pela administradora. A relação jurídica entre o emissor do cartão e o portador é feita através de um contrato de adesão, onde são avaliados os riscos de inadimplência do usuário. O valor total de crédito é disponibilizado de acordo com o risco calculado (BANCO CENTRAL, 2004). Também existe o chamado cartão de loja (*private labels)*, que funciona como um cartão de crédito vinculado a um determinado estabelecimento, tendo seu uso restrito a esta rede de lojas.

Para completar uma operação utilizando um cartão de crédito, são necessários cinco participantes, descritos a seguir (BANCO CENTRAL DO BRASIL, 2004):

- **Portador**: Pessoa (física ou jurídica) interessada em adquirir bens ou contratar serviços pagando através do cartão de crédito. Pode ser o titular da conta de cartão de crédito ou apenas portador do cartão adicional;
- **Estabelecimento:** Pessoa jurídica interessada em vender ou prestar serviço recebendo o pagamento feito pelos seus clientes através do cartão de crédito;
- **Adquirente:** Empresa responsável pela comunicação da transação entre o estabelecimento e a bandeira. Para isso, aluga e mantém os equipamentos usados pelos estabelecimentos como, por exemplo, o POS. As maiores adquirentes no Brasil são Getnet, Redecard, Cielo (antiga Visanet Brasil) e Hipercard;
- **Bandeira:** Empresa responsável pela comunicação da transação entre o adquirente e o emissor do cartão de crédito. As maiores bandeiras no Brasil são Visa, MasterCard e Hipercard. Para identificar qual é o emissor do cartão, as bandeiras usam os seis primeiros números do cartão, chamados de BIN *(bank identification number)*;
- **Instituição financeira**: Principalmente bancos, que emitem o cartão de crédito, definem limite de compras, decidem se as transações são aprovadas, emitem fatura para pagamento, cobram os titulares em caso de inadimplência e oferecem produtos atrelados ao cartão como seguro, cartões adicionais e plano de recompensas.

Em algumas operações existe também a participação de um subadquirente. Ele está inserido entre o estabelecimento comercial e o adquirente, e é normalmente utilizado por empresas que não possuem os requisitos e infraestrutura necessários requeridos por um adquirente. Desta maneira, um subadquirente concentra todas as transações de uma rede, e é reconhecido pelo adquirente como um único estabelecimento.

A rápida aceitação dos cartões a partir da década de 60 levou à necessidade de automatização das transações. Assim, foram criados os terminais POS (*Point of Sale*), os *checkouts* TEF (*eletronic funds transfer – EFT*) e os terminais de autoatendimento bancário (*Automatic Teller Machine – ATM*).

Segundo Graham, B. (2003), o primeiro ATM foi criado ainda na década de 40. Entretanto, seu projeto foi descontinuado, já que não havia demanda para o produto na época. Apenas em 1969 foi instalado o primeiro ATM, na sede do *Chemical Bank*, em Nova Iorque.

As primeiras máquinas funcionavam de maneira *offline*, ou seja, o dinheiro sacado não era debitado da conta do usuário automaticamente. Assim, seu uso estava restrito a alguns usuários.

2.1.1 Regulamentações e Legislações

O setor financeiro no Brasil é regulamentado pelo Banco Central que define a seguinte regulamentação geral (BANCO CENTRAL, 2012):

> Em termos regulatórios, o setor está sujeito a três focos de ação no cenário nacional. As atividades restritas a instituições financeiras e de sistema de pagamentos são reguladas pelo Conselho Monetário Nacional e pelo Banco Central do Brasil. Os aspectos concorrenciais são de responsabilidade do Banco Central do Brasil, no que diz respeito às atividades de instituições financeiras, e do Sistema Brasileiro de Defesa da Concorrência (SBDC), composto pelo Cade (Conselho Administrativo de Defesa Econômica); pela Secretaria de Direito Econômico e pela Secretaria de Acompanhamento Econômico. A indústria de cartões de pagamento, na medida em que seu funcionamento estabelece relações consumeristas, está sujeita também ao Sistema Nacional de Defesa do Consumidor – SNDC, integrado pela SDE, por meio do seu Departamento de Proteção e Defesa do Consumidor – DPDC – e pelos Procons, devendo observância ao Código de Defesa do Consumidor (CDC). No âmbito não governamental, às entidades civis de defesa do consumidor.

A troca de mensagens das transações financeiras a partir de um POS, TEF ou ATM é feita utilizando o padrão ISO (*International Organization for Standarization*) 8583 (ISO, 1993). Esta especificação define o formato das mensagens e um fluxo de comunicação para que diferentes sistemas possam trocar mensagens financeiras.

Tipicamente, uma mensagem ISO possui os seguintes campos:

- **Tipo de mensagem**: Identifica se a mensagem é de compra, consulta ou administrativa (carga de parâmetros, por exemplo) entre outros;
- **Mapa de Bits**: Identifica quais campos de dados da mensagem ISO estão presentes;
- **Campos de dados**: Possui as informações da transação, de acordo com o mapa de bits.

A Tabela 1 exemplifica uma troca de mensagem entre um equipamento remoto e um *gateway* de pagamento. Conforme citado anteriormente, o equipamento remoto pode ser um POS, TEF ou ATM.

Embora a ISO 8583 seja um padrão, ele acaba sempre passando por modificações na sua estrutura. Assim, alguns campos da mensagem, como por exemplo, número do

estabelecimento e NSU (número sequencial único) acabam sendo sempre utilizados. Já outros campos acabam sendo adaptados para uso próprio.

Tabela 1 Exemplo de mensagem ISO

Bit	0700	0710	Tamanho (Bytes)	Tipo	Descrição
			4	N	Código da mensagem
			16	B	Primeiro mapa de bits
3	**M**	**ME**	6	N	Código de processamento
7	**M**	**M**	10	N	Data e hora GMT (MMDDhhmmss)
11	**M**	**ME**	6	N	NSU local
32	**M**	**ME**	LLVAR	N	Código da operadora
39	**-**	**M**	2	N	Código de resposta
43	**M**	**-**	LLVAR	A	Número de série do terminal
62	**M**	**M**	LLLVAR	A	Dados Genéricos

Fonte: Getnet

2.1.2 Segurança

A segurança nas transações financeiras eletrônicas sempre foi uma preocupação de todas as partes envolvidas em uma transação eletrônica. Conforme Bhatla et al (2003), a fraude em um cartão de crédito é definida como:

> Quando um indivíduo utiliza o cartão de crédito de outra pessoa para razões pessoais, sem que esta pessoa saiba que seu cartão está sendo utilizado. Além disso, a pessoa utilizando o cartão não possui nenhuma conexão com o dono do cartão, e não possui nenhuma intenção de entrar em contato com o dono do cartão ou pagá-lo, de acordo com a compra realizada.

Os tipos mais comuns de fraudes relacionadas aos cartões de crédito são listados a seguir (BHATLA et al, 2003):

- ***Application fraud*:** Falsificação de informações pessoais, posse de informações pessoais de terceiros ou interceptação de um cartão antes que este seja entregue ao usuário final;
- **Cartão perdido ou roubado:** Maneira mais fácil de obter um cartão de crédito sem necessitar de conhecimento tecnológico, e também a mais difícil de combater;
- **Posse da conta:** Ocorre quando o fraudador obtém acesso ilegal à conta do usuário e solicita um novo cartão, atualizando dados cadastrais;
- **Cartões falsos:** Usando equipamentos para clonagem de cartões, o fraudador pode criar cópias de cartões pré-existentes, em uma técnica conhecida como *skimming*.

Do ponto de vista do estabelecimento comercial, existem dois tipos de fraudes, que são iniciadas tanto pelos comerciantes como seus empregados.

- **Cooperação:** Ocorre quando o estabelecimento comercial ou seus empregados repassam as informações sobre seus clientes para os fraudadores;
- **Triangulação:** O fraudador cria um site, clonando uma página conhecida de vendas *online*. Quando o usuário realiza uma compra, o fraudador captura seus dados e utiliza para realizar alguma compra em outro endereço.

Por fim, o advento das transações eletrônicas através Internet deu origem a uma série de novas possíveis fraudes, de uma maneira mais fácil do que as listadas anteriormente. As mais comuns são (BHATLA et al, 2003):

- **Clonagem de Sites:** Todo o website, ou apenas a parte referente ao pagamento dos pedidos, é clonado. O comprador insere seus dados normalmente, e estes dados são utilizados para compras em outros locais;
- **Sites de estabelecimentos falsos:** Alguns sites solicitam ao usuário a digitação do número do cartão de crédito, para validação do acesso e informações como idade e endereço. Estes dados então são vendidos através da internet;
- **Geradores de cartões de crédito:** Com a utilização de algoritmos, é possível gerar novos números de cartões de crédito e suas respectivas datas de validade, a partir de um único número de conta do usuário.

Todas as diferentes formas de fraude relatadas acima acabam impactando de alguma maneira as diversas entidades envolvidas em uma transação eletrônica. A fraude normalmente não é cobrada do portador do cartão (*cardholder),* que possui a seu favor a legislação do seu país. O dono do cartão deve apenas reportar ao banco sobre compras indevidas, e este irá realizar a investigação necessária.

Os estabelecimentos comerciais são os mais afetados, principalmente em transações fraudulentas sinalizadas como cartão não presente. Hsu (2011) define transações de cartão não presente como aquelas em que o cartão não foi passado em um leitor de cartões, como por exemplo, aquelas realizadas através da Internet. Neste caso, o dono do cartão irá realizar uma disputa da transação junto ao seu banco, e o banco emissor irá enviar uma solicitação de cancelamento (*chargeback)* ao estabelecimento comercial, através do seu adquirente. Como o

comerciante não possui nenhuma evidência da compra realizada (assinatura, por exemplo), ele terá que absorver todo o prejuízo da transação.

Para maximizar a segurança nas transações financeiras, foi criado um fórum internacional, chamado de *Payment Card industry Data Security Standa*rt (PCI DSS). Esta organização tem como objetivo aumentar o controle das organizações que fazem parte da cadeia de pagamento, evitando expor os dados sensíveis do usuário, tais como número do cartão de crédito. A Tabela 2 lista os 12 requisitos necessários para que uma empresa possua o certificado PCI-DSS, atualmente em sua versão 2.0.

Para a segurança das transações de débito e crédito realizadas com chip *smartcard*, existe um padrão mundial, chamado EMV (Europay, Mastercard e Visa). No final de 2011, existiam mais de 1.5 Bilhões de cartões com esta tecnologia emitidos no mundo. Os cartões com a tecnologia EMV possuem um microprocessador embarcado, possibilitando um nível de segurança que não é possível em cartões convencionais (tarja magnética), além de permitirem uma maior customização, como a instalação de diferentes aplicativos. Quando inseridos em um dispositivo compatível, é estabelecida a conexão entre o leitor e o circuito do chip. O chip então recebe a tensão necessária para seu funcionamento através desta conexão, e a aplicação do terminal pode trocar mensagens (APDUs – *application protocol data units*) com o cartão (EMV, 2009).

Tabela 2 Requisitos para aderência ao PCI-DSS

Construir e manter uma rede segura	1	Instalar e manter um firewall para proteger a informação do dono do cartão
	2	Não utilizar valores padrão para senha e outros parâmetros se segurança
Proteger informações do dono do cartão	3	Proteger informações armazenadas do usuário que estejam
	4	Encriptar informações do usuário que trafeguem em uma rede aberta ou pública.
Manter um programa de gerência à vulnerabilidade	5	Manter programas e antivírus atualizados
	6	Desenvolver sistemas e aplicações seguras
Implementar um forte controle de acesso	7	Restringir acesso aos dados do usuário aos programas que o necessitem
	8	Assegurar que cada pessoa possua um login de acesso único
	9	Restringir acesso físico aos dados do usuário
Monitorar e testar as redes regularmente	10	Rastrear e monitorar todo acesso aos recursos da rede e dados do usuário
	11	Testar regularmente a segurança do sistema e processos
Manter um sistema de informações de segurança	12	Regularmente, enviar informações sobre processos de segurança para todos os usuários.

Fonte: https://www.pcisecuritystandards.org/security_standards/

O padrão EMV também defina as regras de utilização dos cartões sem contato (*contactless*) (EMV, 2009). Este tipo de operação é realizada ao aproximar um cartão compatível de um leitor que possa efetuar a leitura de cartões sem contato. Esta aproximação cria um campo magnético, que gera a tensão necessária para o microprocessador funcionar. Toda a troca de mensagens é realizada através de radio frequência (RFID), utilizando protocolos como NFC. (ISO/IEC 18092 / ECMA-340 e ISO/IEC 21481 / ECMA-352)

O valor limite para as transações *contactless* pode variar de acordo com a solução apresentada (*Mastercard Paypass* ou *Visa Paywave*, por exemplo) ou também de país para país. É comum que as soluções inicialmente possuam um valor limite baixo, suficiente para pequenas compras no dia a dia (cafés, restaurantes), e este valor é adaptado, de acordo com a aceitação da solução pelos usuários.

Além destes rígidos padrões de mercado, que ajudam a qualificar as empresas e os meios de captura, os terminais utilizam as seguintes tecnologias para assegurar a segurança das transações:

- **Criptografia de PIN (*Personal Identification Number*) utilizando TDES:** A criptografia de senha do usuário pode ser realizada utilizando algoritmos como TDES (*Triple Data Encryption Algorithm* – TDEA), onde o algoritmo DES (Data Encyption Standart) é aplicado três vezes (WILLIAM, 1999). Este algoritmo é utilizado na sua forma ISO-3, onde são utilizados dados do cartão do usuário para formar o criptograma (*PIN block*). Neste algoritmo, todas as transações de um usuário irão gerar o mesmo *PIN Block (ISO 9564–1 Format 0)*;

- **Criptografia de PIN utilizando DUKPT (*Derivd Unique Key per transaction*):** Outro método de criptografia de senha utilizada pelos terminais é chamado de DUKPT (ANSI X9.24). Neste caso, uma chave de criptografia é derivada de uma chave inicial. O servidor remoto (*gateway*) também deve ser capaz de gerar esta derivação de chaves através da semente. Caso o usuário realize duas transações com um mesmo cartão em um mesmo terminal, elas não terão o mesmo criptograma;

- ***Tamper-Proof*:** Um dispositivo considerado *tamper-proof* possui uma série de circuitos internos que tornam o dispositivo inutilizável caso seja detectado alguma espécie de invasão física. Quando isto acontece, todas as chaves de criptografia e

eventuais dados sensíveis armazenados são apagados, não permitindo que um usuário mal intencionado tenha acesso a estes dados.

- **Criptografia de dados utilizando AES (Advanced Encryption Standard):** Os equipamentos possuem bibliotecas próprias para realizar a criptografia de mensagens utilizando o padrão AES, padrão criado pelo NIST (*National Institute of Standards and Technology*) para substituição da criptografia DES (ZHANG, 2004).

2.2 Pagamento móvel e ubíquo

Nos últimos anos, o avanço da tecnologia e o surgimento de novos smartphones levaram à evolução do pagamento eletrônico, permitindo que este seja também realizado em dispositivos móveis. Segundo Dahlberg (2007), pagamento móvel é todo aquele pagamento no qual uma das partes da transação é realizada em um dispositivo móvel (como um *Smartphone*) através de uma rede sem fio. Inicialmente, era realizado através de SMS evoluindo para aplicações WAP, USSD (*Unstructured Supplementary Service Data*), e mais recentemente, NFC. Essas tecnologias serão melhores descritas mais adiante, na seção 2.2.2

2.2.1 Modelos

De acordo com Mobey (2006), foram identificados três diferentes modelos de negócio para pagamento móvel:

- **Modelo centralizado na operadora:** Neste cenário, cada operadora de telefonia móvel é responsável pela emissão dos chips SIM. Todo o controle e gerência sobre o Elemento Seguro. (*Secure Element* – SE) é de sua responsabilidade. A operadora permite aos bancos e demais provedores de serviço a utilização do SE de acordo com suas necessidades. Cada estabelecimento comercial necessita realizar um contrato com cada uma das operadoras de telefonia, de modo a atingir o maior número possível de usuários. É uma boa alternativa para soluções a nível nacional, mas é complexa de ser implementada a nível mundial, pois necessitaria de acordos com as operadoras de todos os países.

- **Modelo centralizado nos bancos/provedores de serviço:** Os bancos ou outros provedores de serviço são os responsáveis pela emissão de um *Security Memory Card* (SMC), um cartão de memória equipado com elemento seguro. O usuário, em posse deste SMC, deve registrá-lo junto a uma instituição financeira, que poderá utilizá-lo como elemento seguro ou alguma outra funcionalidade. Da

mesma maneira que no modelo centralizado na operadora, o comerciante deve ter um contrato com cada um dos diferentes provedores de serviço, que podem existir em maior número do que as operadoras de telefonia móvel.

- **Modelo de operação por terceiro:** Neste modelo, uma entidade independente e neutra é responsável pelo serviço de gerenciamento do serviço. Esta empresa pode oferecer o elemento seguro na forma de um chip embarcado, mas também pode gerenciar o elemento seguro na forma de SIM card ou SMC. Um estabelecimento apenas necessita contrato com esta entidade independente. Caso exista mais de uma destas entidades, o contrato deverá ser feito com cada uma delas. Mesmo assim, espera-se que este número seja menor que o total de operadoras de telefonia móvel de um determinado país. É necessário também que o elemento seguro possua total compatibilidade entre todas as entidades. Este é o modelo utilizado atualmente no Japão, onde a entidade independente é chamada de *Felica Network*.

A principal diferença entre estes modelos está no tipo de utilização e gerência do Elemento Seguro. Esse componente será melhor detalhado na seção 2.3.1. Também é comum alguns autores identificarem um 4º membro neste modelo, através da colaboração entre instituições financeiras e operadoras de telefonia móvel. Este não é um modelo muito utilizado, pois acarreta uma divisão do lucro entre mais empresas devido ao maior número de envolvidos no processo transacional.

2.2.2 Tecnologias

Diversas tecnologias permitem a utilização do dispositivo móvel como um meio de realizar transações financeiras, como *Bluetooth*, Wi-Fi, NFC, QR CODE, SMS e USSD.

Bluetooth (IEEE Standard 802.15.1-2002) é um protocolo de comunicação sem fio que opera na faixa de 2400 – 2480 MHz. A tecnologia *Bluetooth* permite a conexão entre dois dispositivos distintos, como telefones móveis e aparelhos de som. Esta característica pode ser utilizada para o pagamento móvel P2P entre dois dispositivos, através da criação de uma rede pessoal (PAN – *Personal Area Network*). Esta funcionalidade pode ser explorada para a transferência de dinheiro sem necessidade de conexão a uma entidade centralizadora. Atualmente o protocolo encontra-se em sua revisão 4.0, onde foram reforçadas características de segurança, consumo de energia e tempo de pareamento entre dois dispositivos. Um rápido pareamento aliado a uma maior segurança torna possível a sua utilização para pagamento móvel entre dispositivos.

Wi-Fi (IEEE 802.11) é um protocolo de comunicação sem fio padrão nos computadores. Permite a conexão de computadores à internet, através de um ponto de acesso sem fio. Como vários dispositivos móveis possuem atualmente um adaptador *wireless*, e os principais sistemas operacionais móveis permitem que o aparelho seja configurado como uma rede ad-hoc, é possível utilizar este meio para o pagamento móvel P2P entre dois dispositivos. Atualmente, muitos dispositivos móveis já possuem a versão IEEE 802.11N da especificação, permitindo taxas de até 300 MB/S. O estabelecimento de conexão entre dois dispositivos é feita de maneira rápida, e a alta taxa de transmissão permite uma rápida interação entre os dispositivos envolvidos.

NFC (ISO/IEC 14443) é um protocolo de comunicação sem fio, através de radio frequência. Permite a comunicação entre dos dispositivos de maneira rápida, através da aproximação de dois equipamentos compatíveis. Possui três distintos modos de operação. No modo *Card Emulation* o dispositivo NFC é reconhecido pela leitora externa como um cartão *smartcard* sem contato. A informação é lida do cartão e repassada para a leitora; No modo *Peer to Peer* (P2P) é possível a troca de dados entre dois dispositivos NFC. Pode ser utilizado para troca de informações para pareamento *Bluetooth*, chat entre os dois dispositivos e troca de contatos ou arquivos. Já em modo *Reader/Writer*, um dispositivo NFC pode ler ou escrever dados de uma *tag* NFC.

QR CODE (ISO/IEC 18004:2006) são códigos de barras bidimensionais que podem ser decodificados utilizando um celular equipado com uma câmera fotográfica e um software específico para decodificação. O código lido pode representar um texto puro, um endereço da internet (URL), número de telefone, uma localização GPS (*Global Positioning System*) ou um contato. Sua primeira utilização foi na indústria automobilística, na qual era utilizado para catalogar e gerenciar seu inventário. Atualmente, são utilizados em propagandas de revistas, cartões de visita e até mesmo em comerciais de televisão.

O protocolo SMS (ISO/IEC 20000-1:2011) permite que um dispositivo envie uma mensagem (requisição da transação) diretamente para outro dispositivo móvel, ou para uma entidade centralizadora, que então faz a comunicação com a outra parte envolvida. Entretanto, este tipo de mensagem não possui nenhuma garantia de entrega por parte da operadora, o que pode inviabilizar o seu uso para situações críticas, como é o caso do pagamento móvel. Também não implementa nenhum tipo de criptografia.

USSD (ETSI EN 300 957, V7.0.1) é um protocolo utilizado pelas operadoras de telefonia para comunicação com suas centrais de comunicação. Pode ser utilizado para

navegação em páginas WAP e serviços baseados em menus. Permite a troca de mensagens de até 182 caracteres. Durante seu funcionamento, é estabelecida uma conexão com o servidor remoto, e esta sessão é mantida durante a troca de informações. É um protocolo de baixo custo para a operadora, fácil utilização, e bastante confiável (alta disponibilidade do serviço). É suportado pela maioria de equipamentos móveis, até mesmo nos modelos mais simples, permitindo que o pagamento móvel seja efetuado por um grande número de usuários.

2.3 Carteira Digital

Segundo (MOBEY, 2011), uma carteira digital é uma funcionalidade em um dispositivo móvel que é capaz de interagir com valores financeiros, de uma maneira segura. Embora possa estar armazenada no dispositivo ou de maneira remota, ela apenas pode ser utilizada e gerenciada a partir do aparelho móvel. O termo carteira digital (tradução direta do inglês *digital wallet*) tem sido utilizado para definir uma série de pagamentos eletrônicos móveis, através de *smartphones* ou *tablets* (VISA, 2012).

Segundo (OLSEN, 2012), uma carteira digital é um artefato digital pessoal que contém instrumentos para pagamento eletrônico, como cartões de pagamento, espaços para *ticket* e comprovantes, cartões de identificação como passaportes, carteiras de motoristas e cartões de seguro, e também itens pessoais como fotos e lista de compras. Pode conter também um moedeiro eletrônico, que é uma versão digital do dinheiro físico, permitindo assim o pagamento eletrônico entre dois usuários.

Através de uma autenticação, a carteira digital permite o acesso a uma série de serviços, como por exemplo:

- **Serviços financeiros**
    a. Aplicações de *Internet banking*
    b. Cartões de crédito
    c. Histórico de transações realizadas
- **Serviços de Identidade**
    a. Assinaturas digitais
    b. RG/CPF eletrônicos
    c. Carteira de motorista
    d. Cartão de acesso (cartão-ponto etc.)

- **Informações de comércio**
    a. Cupons de desconto
    b. Cartões fidelidade

Algumas destas informações são normalmente cadastradas pelo usuário ao preencher um formulário de compras *online*. Com esta informação já armazenada na carteira digital, seria possível automatizar este processo, preenchendo estes dados de maneira rápida e transparente.

Diversas tecnologias podem ser utilizadas para efetuar a compra de produtos utilizando o conceito de carteira digital, como NFC e QR CODE. Caso a conexão com a Internet esteja sempre disponível, também é possível efetuar o pagamento de maneira *online*, eliminando a necessidade de armazenamento de dados do cartão no dispositivo móvel. No caso de uma implementação de moedeiro eletrônico de maneira totalmente *offline*, é necessária a utilização de um elemento seguro, que garante a segurança da informação armazenada no dispositivo (MOBEY, 2006).

As transações efetuadas no conceito de carteira digital utilizando NFC estão sujeitas aos mesmos limites das transações com cartões de crédito *contactless***.** Este limite pode ser diário ou por transação. Também pode ser requisitado que o usuário efetue uma transação de maneira *online*, caso o cartão já tenho passado do seu limite diário de transações *offline* (número total de transações) ou o valor total acumulado das transações *offline* seja superior ao seu limite.

2.3.1 Elemento seguro

Uma das principais características em uma solução de carteira digital é a presença do elemento seguro. De acordo com Mobey (2005), um elemento seguro é uma plataforma, onde aplicações podem ser instaladas, personalizadas e gerenciadas de maneira remota, preferencialmente *over-the-air* (OTA*).* É uma combinação de hardware, software, interfaces e protocolos que permitem armazenamento seguro e o uso de credenciais para pagamentos, autenticação e serviços. Ele não deve ser utilizado apenas para a infraestrutura de chaves públicas (PKI, *public key infrastructure*), mas também como um elemento de armazenamento e processamento de credenciais, que podem ser utilizadas para autenticação ou pagamento (MOBEY, 2010).

Existem várias formas de se implementar um SE. As três maneiras mais utilizadas pelo mercado são (MOBEY, 2005):

- ***SIM Card*:** O cartão SIM (*Subscriber Identity Module*), utilizado pelos dispositivos móveis, é considerado seguro e pode ser utilizado para armazenamento das informações sensíveis. Esta opção necessita de uma dependência do banco com as operadoras de telefonia;
- **SMC:** Um cartão de memória seguro inclui espaço para armazenamento, um cartão inteligente (*smart card*) e um controlador para acesso ao dispositivo;
- **Chip embarcado:** Neste caso, o elemento seguro está inserido internamente no equipamento.

Um elemento seguro pode conter várias aplicações, e estes aplicativos podem ser de fornecedores diferentes. Ele deve suportar a reinicialização, já que um dispositivo móvel pode ser vendido para outra pessoa, que também fará uso desta funcionalidade.

2.3.2 Gerenciador da Plataforma

O gerenciador da plataforma, também conhecido como TSM (*Trusted Service Manager*) é o responsável pela gerência das chaves de criptografia usadas no Elemento Seguro. A *master key* (MK) é gerada durante o processo de personalização do chip, que deve ser realizado em um ambiente seguro e controlado (MOBEY, 2006). O gerenciador da plataforma é o único que é capaz de realizar a mudança desta chave. O TSM também habilita aos provedores de serviços realizarem a distribuição e gerência das aplicações de maneira remota.

São atribuições do gerenciador da plataforma (MOBEY, 2006):

- Autorizar empresas a instalarem aplicativos no Elemento Seguro, através de atualizações OTA ou outro tipo de processo;
- Desabilitar o serviço ou alguma aplicação, quando achar necessário, como, por exemplo, por questões de segurança;
- Fornecer um serviço ao usuário final, permitindo que este desabilite por completo a funcionalidade do dispositivo, em caso de roubo ou perda;
- Fornecer um serviço de recuperação, permitindo que os dados do cliente sejam repassados para um novo elemento seguro.

O gerenciador da plataforma pode ser visto como uma terceira parte confiável, e deve possuir os mesmos níveis de segurança que demais partes envolvidas no pagamento eletrônico

possuem, necessitando para isto um grande investimento. Caso o gerenciador da plataforma também seja o responsável pelo Elemento Seguro, a elaboração de um modelo de negócio com os provedores de serviço e o usuário final é facilitada (MOBEY, 2006).

2.4 Comercio móvel e ubíquo

A carteira digital descrita anteriormente é uma solução que pode se beneficiar de um ambiente de comercio ubíquo. Comércio ubíquo refere-se ao uso de redes ubíquas para suportar comunicações e transações personalizadas e ininterruptas entre uma empresa e seus vários investidores para fornecer um valor agregado além do comércio tradicional (WATSON et al., 2002). O comércio ubíquo pode ser visto como uma extensão lógica do comércio eletrônico e do comércio móvel, sendo considerado uma nova fase (JUNGLAS, WATSON, 2006).

A evolução dos meios de pagamento eletrônico e as diversas tecnologias que permitem o pagamento móvel contribuem para o surgimento do comércio móvel e ubíquo. Comércio ubíquo (*u-commerce*) é definido como o uso de redes ubíquias para suportar comunicações e transações personalizadas e ininterruptas entre organizações e seus vários clientes, provendo um valor agregado superior ao do comércio tradicional (WATSON, PITT, et al., 2002). De acordo com Manvi, S (2011), *u-commerce* representa um novo meio de comércio, sendo considerado promissor para futuras aplicações, apresentando um grande e promissor mercado.

Embora o conceito de comércio ubíquo seja relativamente novo, diversos modelos já foram desenvolvidos. Em Franco el al (2010), um modelo de comércio ubíquo, batizado de MUCS (*model for ubiquitous commerce support*) é proposto. O objetivo principal deste modelo é identificar oportunidades de negócios entre usuários que estejam envolvidos em um ambiente de computação ubíqua.

O comércio ubíquo é definido por quatro características principais (WATSON, PITT, et al., 2002), que são:

- **Ubiquidade:** permite que os usuários acessem a redes a partir de qualquer lugar a qualquer momento. Também permite que o usuário seja encontrado em qualquer lugar a qualquer momento;
- **Unicidade:** permite aos usuários a identificação unívoca, identidade, suas preferências associadas e localização;
- **Universalidade:** significa que os dispositivos móveis são universalmente utilizáveis e multifuncionais;

- **Unissonância:** assume que os dados são integrados e consistentes em diferentes aplicativos.

De acordo com Tiwari e Buse (2007), o comércio móvel (*m-commerce*) é caracterizado por algumas características únicas, que o colocam em vantagem sobre demais métodos de transações financeiras. Estas características são:

- **Ubiquidade:** Permite a utilização do serviço em qualquer lugar, a qualquer hora;
- **Imediatismo:** Captura o cliente no momento da sua intenção de compra, fazendo com que este realize a chamada compra por impulso;
- **Localização:** Um dispositivo móvel pode informar sua posição através do uso do GPS, da triangulação das redes da operadora de telefonia ou mesmo da rede Wi-Fi. Sua localização pode ser utilizada para oferecer serviços específicos ao contexto;
- **Conectividade instantânea:** Grande parte dos telefones móveis inteligentes (*smartphones*) é vendida junto a um plano de dados. Assim, estes equipamentos estão sempre *online*, prontos para realizar alguma transação financeira;
- **Pró-atividade:** Graças à conectividade permanente, é possível enviar ofertas diretamente ao dispositivo móvel de usuário;
- **Autenticação rápida:** Caso o dispositivo móvel esteja equipado com um *chip* SIM, é possível utilizá-lo como forma de autenticar o usuário, em conjunto com uma senha, não necessitando de outra forma de autenticação (biometria, autenticação *online* etc.).

Segundo Manvi (2011), a principal diferença do comércio eletrônico tradicional para o comércio ubíquo é a utilização de diversos meios diferentes para efetuar o pagamento, como dispositivos móveis, PDAs, televisões, etc. As informações do usuário, geradas através da interação com cada um destes componentes, devem ser armazenadas, fornecendo um perfil do usuário. Este perfil pode ser utilizado para fornecer sugestões de compras ao usuário, através de um sistema de recomendação.

Já de acordo com Junglas (2006), as principais diferenças entre comércio móvel e o comércio ubíquo estão no conceito e na tecnologia. Enquanto que o comércio ubíquo possui como base as quatro características citadas anteriormente, o comércio móvel possui como

principal caraterística a utilização de redes móveis. Outra diferença é a utilização de um novo ambiente computacional (ambiente de computação ubíqua), que se difere do comércio móvel em termos de aplicações, redes, dispositivos e sincronização de dados.

De acordo com Weiser (1991), um ambiente de computação ubíqua é definido como um ambiente onde os computadores estão embarcados em praticamente todos os objetos utilizados no dia a dia, de maneira que o usuário irá utilizá-lo sem perceber. Todos estes objetos estarão conectados através de uma rede ubíqua. Segundo Lyytinen et al. (2004), a computação ubíqua permite às pessoas estarem conectadas e interagir entre si sem nenhuma restrição de tempo ou espaço.

A Tabela 3 resume as diferenças entre o modelo tradicional de comércio móvel e o comércio ubíquo.

Tabela 3 Diferenças entre *m-commerce* e *u-commerce*

		M-Commerce	U-Commerce
Conceito	Características	*Mobile* *Wireless*	Ubiquidade Unicidade Universalidade Unissonância
Tecnologia	Aplicação	Número limitado de aplicações	Grande número de aplicações
	Rede	Cobertura limitada de redes e diferentes tipos de padrões	Múltiplas redes e possibilidade de acessar redes e aplicações através destas redes.
	Dispositivos	Dispositivos móveis como PDAs e telefones móveis	Vários dispositivos, inclusive não convencionais, como objetos do dia a dia.
	Dados	Integração e sincronização limitada.	Integração e sincronização integrada.

Fonte: Baseado em (JAIS, 2008).

Uma solução de carteira digital deve estar disponível para o maior número possível de usuários. De nada adianta a solução estar presente apenas em um determinado tipo de dispositivo móvel (sistema operacional/modelo) se este aparelho não representar a plataforma dominante do mercado, ou se os usuários deste modelo não forem o público alvo do projeto a ser desenvolvido. Assim, uma aplicação de moedeiro eletrônico deve estar disponível para um grande número de dispositivos eletrônicos, desde *smartphones* e *tablets* até *setup boxes* (aparelhos de tv digital, cabo etc.) alcançando um maior número de usuários, facilitando a

aplicação do conceito *anywhere/anytime*, permitindo que uma compra seja feita em qualquer tempo.

2.4.1 Sensibilidade ao contexto

A utilização do contexto permite a expansão do número de usuários que irá utilizar o comércio móvel, além de elevar a qualidade do serviço oferecido (VASSILAKIS et al, 2008), aumentando o diálogo entre o usuário e o comerciante. Sensibilidade ao contexto é a habilidade da aplicação monitorar e analisar informações do contexto a partir de várias fontes, permitindo que diferentes ações sejam tomadas e que a aplicação se adapte a diferentes contextos (YAU et al, 2002).

De acordo com Dey (2001), contexto é qualquer informação que pode ser usado para caracterizar a situação de entidades (ou seja, uma pessoa, lugar ou objeto) que são considerados relevantes para a interação entre um usuário e uma aplicação, incluindo o usuário e a aplicação propriamente dita. Contexto é tipicamente a localização, identidade e estado de pessoas, grupos e objetos computacionais e físicos.

Segundo Huang (2011), o contexto pode ser dividido da seguinte maneira:

- **Contexto de usuário:** Inclui toda informação pessoal do usuário. Esta informação pode ser estática (preferências, hábitos) ou dinâmica (localização, estado emocional);
- **Contexto físico:** Refere-se a toda informação do ambiente em que o usuário está inserido, como temperatura, luz, poluição, e também a informações específicas do dispositivo móvel utilizado, como sistema operacional, memória, tamanho de tela etc.;
- **Contexto de rede:** Apresenta informações sobre a capacidade da rede e conectividade, entre outros.

A sensibilidade ao contexto ainda pode ser dividida de acordo com a influência do comportamento do sistema (CHEN, 2000):

- **Sensibilidade ao contexto ativa:** A aplicação automaticamente se adapta ao contexto, mudando o comportamento da aplicação;
- **Sensibilidade ao contexto passiva:** O novo contexto é exibido ao usuário, que pode optar pela sua utilização.

Para evitar o excesso de informações passadas ao usuário, é comum a criação de perfis (*profiles*), que especificam as preferências do usuário, como data/hora e local onde o usuário deseja receber alguma informação, além dos tipos de informações que o usuário deseja (RAZ et al, 2006).

Uma das principais características da computação ubíqua é a sensação de invisibilidade, onde a tecnologia é utilizada praticamente sem a percepção do usuário, em qualquer lugar, a qualquer hora. A utilização destas características no comércio Ubíquo permite ao usuário realizar transações financeiras em qualquer lugar. A correta utilização da tecnologia, junto com a informação de contexto, acaba estimulando a venda por impulso, fazendo com que o usuário compre um produto naquele momento, que dificilmente ele compraria em alguma outra situação.

2.5 Considerações finais

Com base nos itens descritos anteriormente, o trabalho a ser desenvolvido deve possuir as características de comércio ubíquo citadas anteriormente, como ubiquidade, unicidade, universalidade e unissonância. Qualquer informação considerada sigilosa deve ser guardada em um elemento seguro, evitando que esta informação possa ser capturada por um usuário mal intencionado. A aplicação deve permitir o pagamento eletrônico e também efetuar um controle dos gastos do usuário e permitir que sejam armazenados cupons de descontos e fidelidade no dispositivo.

O pagamento eletrônico entre as partes envolvidas deve ser feito de maneira segura, utilizando as boas práticas já consolidadas nos meios eletrônicos de pagamento atuais, e deve utilizar para isto tecnologias como NFC, QR Code ou *Bluetooth*.

3 TRABALHOS RELACIONADOS

Diversos trabalhos foram estudados, com o objetivo de adquirir o conhecimento necessário para a proposição de um modelo. Por fim, foram escolhidos quatro artigos que serviram como base para o projeto proposto. Um dos critérios de seleção dos modelos acadêmicos foram a utilização do dispositivo móvel como carteira digital, que permita o pagamento seguro através da utilização de algum elemento de segurança. A utilização de diversos meios de comunicação entre os dispositivos também foi requisito para a busca dos trabalhos, bem como permitir o pagamento P2P entre dois usuários. Os modelos comerciais escolhidos representam um caso de sucesso (modelo japonês) e também a aposta do Google na área, considerado como um dos potenciais motivadores para ampla adoção da tecnologia.

Foram avaliadas características como segurança, garantindo que a informação trafegada e armazenada nos dispositivos esteja segura contra alguma terceira parte, anonimidade, buscando o mesmo sigilo alcançado ao efetuar um pagamento com dinheiro físico e abrangência de dispositivos, com o objetivo de ter uma solução de carteira digital disponível em um grande número de aparelhos móveis.

3.1 mFerio

Em mFerio (BALAN, 2009) uma solução de pagamento móvel P2P é apresentada. Com o objetivo de substituir por completo o uso de transações com dinheiro físico, o trabalho apresenta como premissa a realização de transações de maneira totalmente *offline*. Como exemplo, é citado o caso onde o usuário deseja realizar o pagamento de uma corrida de taxi ao chegar ao hotel. Entretanto, é comum que a garagem do hotel seja em um ponto isolado, muitas vezes subterrâneo, e não possua nenhum tipo de conectividade para o dispositivo móvel, seja redes WiFi do próprio hotel, GPRS (*General Packet radio service*) ou 3G (*3rd Generation*) da operadora de telefonia. O uso de mensagens de texto SMS também é descartado, já que este é um protocolo sem garantia de entrega, o que inviabiliza o pagamento móvel. A especificação de um meio de pagamento móvel que não necessita nenhum tipo de contrato com a operadora é importante, pois permite que pequenos comerciantes sejam capazes de realizar transações com um custo mínimo, tornando-se muito parecido com o pagamento em dinheiro. Assim, todas as transações são consideradas *offline*, isto é, não necessitam de conexão com uma terceira parte.

O mferio foi avaliado de acordo com alguns critérios criados para caracterização da solução: usabilidade, segurança e auditoria. Dois diferentes critérios foram levados em conta para a avaliação da segurança da solução.

- Segurança física, levando em consideração o canal de comunicação e as chaves de autenticação trocadas entre os dispositivos;
- Segurança do usuário, através da sequência de operações realizadas.

O tipo de segurança física irá depender muito do tipo do ambiente onde o sistema está sendo implantado, pois isto irá depender diretamente das regulamentações locais. (BALAN, 2009) Uma parceria entre a instituição que está implementando o sistema e a operadora de telefonia local pode viabilizar o uso do SIM card do dispositivo como elemento seguro, por exemplo.

Para garantir a segurança na comunicação entre os dois dispositivos, a solução propõe a utilização de NFC. Assim, a segurança é garantida devido à necessidade de aproximação entre os dispositivos, que deve ser menor do que 10 cm, em contraste com outros protocolos como *Bluetooth* e WiFi. Outra característica reforçada pelo autor é a facilidade na conexão entre os dispositivos, que ocorre em uma fração de segundo. Por fim, o usuário sabe exatamente com quem está se comunicando, ao contrario dos protocolos sem fio de larga distância. Uma camada de segurança também é implementada para o acesso da aplicação, onde o usuário deve fazer uso de uma senha, desenho gráfico ou biometria.

Como ultimo critério de segurança, é necessária a utilização de um elemento seguro, que só deve ser invocado quando a autenticação do usuário for validada. Este elemento seguro irá conter os dados do usuário, e mais importante, informações sobre o seu saldo. Este elemento seguro deverá ser do tipo *tamper proof*, ou seja, os dados deverão ser apagados em caso de tentativa de violação.

Por fim, a solução necessita que os dispositivos que participam da transação sejam aproximados duas vezes, realizando um protocolo de dois toques (*two touch protocol*) (BALAN, 2009). Na primeira vez, são trocadas informações iniciais sobre a transação com a utilização de certificados, e uma chave de segurança transiente é criada, que terá apenas esta operação como validade. O elemento seguro do dispositivo que requisitou a operação certifica-se que o usuário possui o saldo necessário, realiza o débito e assina a mensagem. Na segunda aproximação dos dispositivos, a transação é concluída, e o aparelho do usuário que

está recebendo a transação valida a mensagem e adiciona o saldo no seu elemento seguro. Se algum erro ocorrer, a operação deve ser revertida automaticamente para o estado original.

O critério de auditoria tratado pelo artigo busca garantir que nenhuma outra parte (bancos, unidades certificadoras etc.) terá algum conhecimento da transação que foi efetuada. Entretanto, existe a troca de informações entre os dispositivos envolvidos, que ocorre durante uma das etapas de aproximação dos dispositivos. A solução então busca um equilíbrio entre o anonimato dos usuários e a rastreabilidade dos gastos, restringindo as informações de um pagamento aos usuários envolvidos, permitindo então que um usuário comprove seu pagamento através dos seus logs. Assim, a solução não pode ser considerada tão anônima como no uso do dinheiro.

Por fim, o critério de usabilidade do sistema é avaliado. A implementação de um novo sistema de pagamento deve garantir que ele seja tão fácil de usar como os métodos anteriores, caso contrario, pode dificultar a aceitação por parte do usuário final. Mas esta facilidade não deve comprometer a segurança do sistema. As características descritas anteriormente, como o pagamento em dois toques, permitem ao usuário saber exatamente em que ponto da operação ele está, e quantos passos ainda são necessários para concluí-la, de forma similar aos *checkouts* das compras *online*. O saldo do usuário e o valor da transação são exibidos em praticamente todas as telas, e a confirmação da operação deve partir do usuário que está efetuando o pagamento.

O usuário deve sempre autenticar-se na aplicação, inserindo então uma etapa a mais no processo transacional. A aplicação pode ser configurada para sempre estar apta a receber uma transação, ou ser de responsabilidade do usuário selecionar o modo como deseja utilizar a aplicação no momento, para efetuar ou receber um pagamento. Estes dois exemplos ajudam a tornar o uso do sistema mais simples para o usuário, entretanto, são fatores que afetam também a segurança do modelo proposto.

A solução deve permitir que o usuário efetue o pagamento de um valor qualquer, ou seja, deve permitir o pagamento exato. Isto também é possível com o dinheiro físico, entretanto, o pagamento de quantias elevadas ou que possuam valores quebrados muitas vezes leva o usuário a um arredondamento. O sistema também deve possuir o mesmo desempenho, independente do total da transação.

Como falado anteriormente, o sistema deve estar sempre disponível, sem depender de nenhuma infraestrutura, facilitando assim a substituição da moeda física pela moeda virtual.

Como ultimo item na usabilidade, o sistema permite que seja escrita uma nota a respeito da compra realizada, permitindo um controle das transações por parte do usuário.

O mferio foi testado com 104 usuários. Inicialmente, foi dado um treinamento de aproximadamente 5 minutos, explicando a utilização do sistema e o uso do NFC. Após esta etapa, os usuários foram solicitados a realizar algumas transações com o sistema. Os usuários consideraram o produto rápido e fácil de utilizar, e praticamente todos os usuários optaram pelo protocolo de dois toques, mostrando uma preocupação de todos pela segurança envolvida.

3.2 FairCash

FairCASH (KREFT, 2006) é uma solução em que o dinheiro digital comporta-se da mesma maneira que o dinheiro físico. Assim, é criado o conceito de *e-coins* (moeda eletrônica), com valores fixos (0.01 centavos, 0.02 centavos, 0,50 centavos, por exemplo). Cada moeda virtual possui um número serial único durante toda a sua existência. Esta semelhança com o dinheiro físico busca facilitar a sua utilização pelos usuários. As moedas são emitidas por uma espécie de casa da moeda virtual, chamadas de e-mint (KREFT, 2008). O sistema busca atender ao maior número possível de dispositivos móveis, e desta maneira, o modo de comunicação entre dois diferentes usuários não está limitado ao uso de NFC.

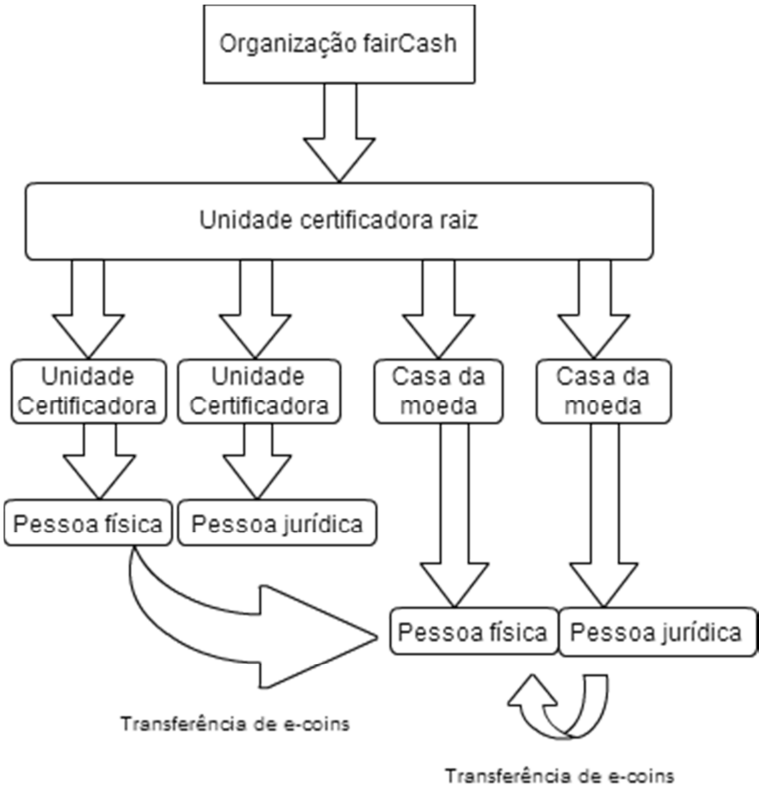
A solução apresentada faz uso de uma organização, aqui chamada de fairCASH, uma unidade certificadora raiz (RCA), múltiplas casas da moeda virtual, que também são unidades certificadoras (CA) e os usuários finais, que podem ser clientes ou estabelecimentos comerciais (KREFT, 2008). Cada participante desta comunidade possui um certificado. A visão geral desta comunidade é exibida na Figura 4.

A solução apresentada permite o pagamento entre dispositivos próximos, através do uso de NFC, mas estende o seu uso para redes locais (Wifi, *Bluetooth*) ou através da internet. O sistema trabalha sempre com transações *offline*, ou seja, mesmo que exista uma comunicação através da Internet, não há comunicação dos dois envolvidos na transação com os outros sistemas (e-mint ou organização fairCASH). A operação em redes de maior alcance adiciona uma preocupação a mais no quesito segurança, pois o usuário pode estar sendo vitima de algum ataque do tipo *Man-in–the-Middle* (HWANG, 2008).

A segurança do sistema é garantida pelo uso de um elemento seguro denominado CASTOR (*CAsk for Storage and Transport Of access Restricted secrets*), que tem como funcionalidade executar as operações da carteira eletrônica e proteger os dados sensíveis,

como suas chaves públicas, privadas e chaves de criptografia (KREFT, 2010). Este elemento seguro deve ser embarcado no dispositivo móvel, o que representa um problema para a implementação do sistema em larga escala, já que o hardware do dispositivo deverá possuir suporte ao chip.

Figura 4Arquitetura fairCash



Fonte: Baseado em (KREFT, 2008).

Devido à característica *offline* das transações, diversas alternativas são propostas para evitar a propagação de moedas digitais falsas. As moedas possuem uma data de validade baixa, sendo necessário realizar a consolidação *online* com frequência. Também existe a possibilidade de verificação *online* da validade da transação, com os números seriais das moedas envolvidas sendo verificados na organização fairCASH, ou de consultar se a carteira digital que está efetuando o pagamento não está em uma espécie de lista negra. Entretanto, estes métodos necessitam que uma conexão à Internet esteja disponível, e o sistema acaba perdendo em praticidade e velocidade.

Embora o sistema possua números seriais para cada uma das moedas digitais em circulação, e seja obrigatório o uso de certificados para realizar uma operação, todas as transações que envolvem um usuário pessoal são feitas de maneira anônima, ou identificadas

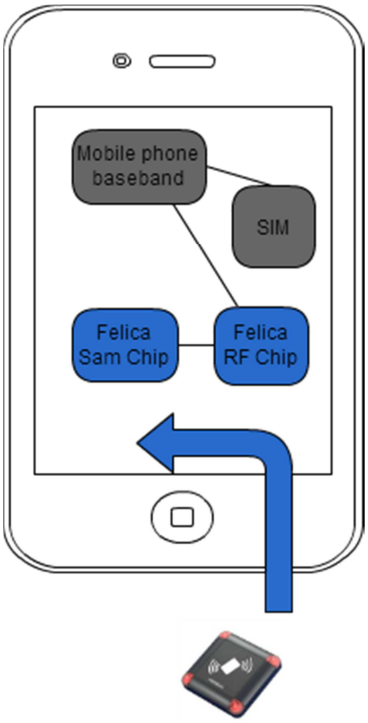
se o usuário assim desejar. Isto garante ao usuário fairCASH receber ou efetuar um pagamento de maneira anônima, da mesma maneira que as transações com dinheiro são realizadas. Entretanto, transações que envolvam um estabelecimento comercial, por exemplo, não satisfazem este critério, pois obrigatoriamente contém um certificado que identifica o comerciante.

3.3 DoCoMo

A utilização de uma carteira digital já é bastante difundida na Ásia, sobretudo no Japão, onde a operadora de telefonia móvel NTT DoCoMo, conhecida pela sua implementação de internet *wireless* em 1999, implementou sua versão de carteira digital, chamada de Osaifu-Keitai (BOYD, 2005). A empresa possui parcerias com os principais bancos locais, bem como agências de viagem e diversas companhias que podem agregar algum valor ao serviço oferecido.

O elemento seguro do sistema é um chip *smartcard* sem contato, desenvolvido pela Sony, chamado de Sony Felica (KOWAKAME, 2011). Este tipo de cartão inteligente, criado em 1995, é amplamente utilizado no Japão, e foi adaptado para o uso em telefones móveis, através de uma parceria entre Sony e DoCoMo. Uma visão geral do hardware da solução é exibida na Figura 5

Figura 5 Arquitetura de um telefone com chip Felica



Baseado em: (FELICA NETWORKS, 2012).

A carga de créditos na carteira digital é feita de duas maneiras distintas. Na mais prática, o usuário pode adicionar dinheiro na sua carteira digital diretamente em seu dispositivo móvel, através da digitação de um PIN e transferir a quantia de uma conta vinculada a um cartão de crédito. Também estão disponíveis máquinas que realizam a recarga em diversas lojas do comércio. Assim, o usuário sempre possui uma maneira para efetuar a carga de créditos, contribuindo para o sucesso do sistema. O sistema utiliza o protocolo NFC para comunicação do dispositivo móvel com as leitoras ou máquinas de recarga de crédito.

Algumas cidades já utilizam um sistema de pagamento sem contato no transporte público. Normalmente, os clientes possuem um cartão inteligente sem contato, e efetuam a carga dos créditos em máquinas disponíveis no mercado local. Assim, uma das primeiras utilizações da Osaifu-Keitai foi no sistema de transporte japonês, mais precisamente na East Japan Railway Co. (JR East). Este sistema é conhecido como bilhetagem eletrônica (TRI, 2012).

O elemento seguro permite a instalação de diversas aplicações, tornando possível o controle de diversas carteiras digitais. Assim, um único dispositivo móvel pode conter um cartão pré-pago, o sistema de bilhetagem eletrônica e um aplicativo para controle de cupons de desconto, por exemplo.

Como segurança, o sistema permite que o usuário configure uma senha (PIN) cada vez que utilizar o sistema. Isto é importante, já que é possível armazenar até US$ 450,00 na carteira digital. Em caso de perda ou roubo do telefone móvel, é possível bloquear imediatamente a sua utilização de maneira remota, através do contato direto com a operadora de telefonia.

Em 2011, aproximadamente 65% dos usuários da operadora DoCoMo (cerca de 37.5 milhões de usuários) possuíam um telefone móvel compatível com NFC, e a solução era aceita em mais de 1.4 milhões de estabelecimentos comerciais tornando este o maior caso de uso de uma carteira digital no mundo (DoCoMo, 2011).

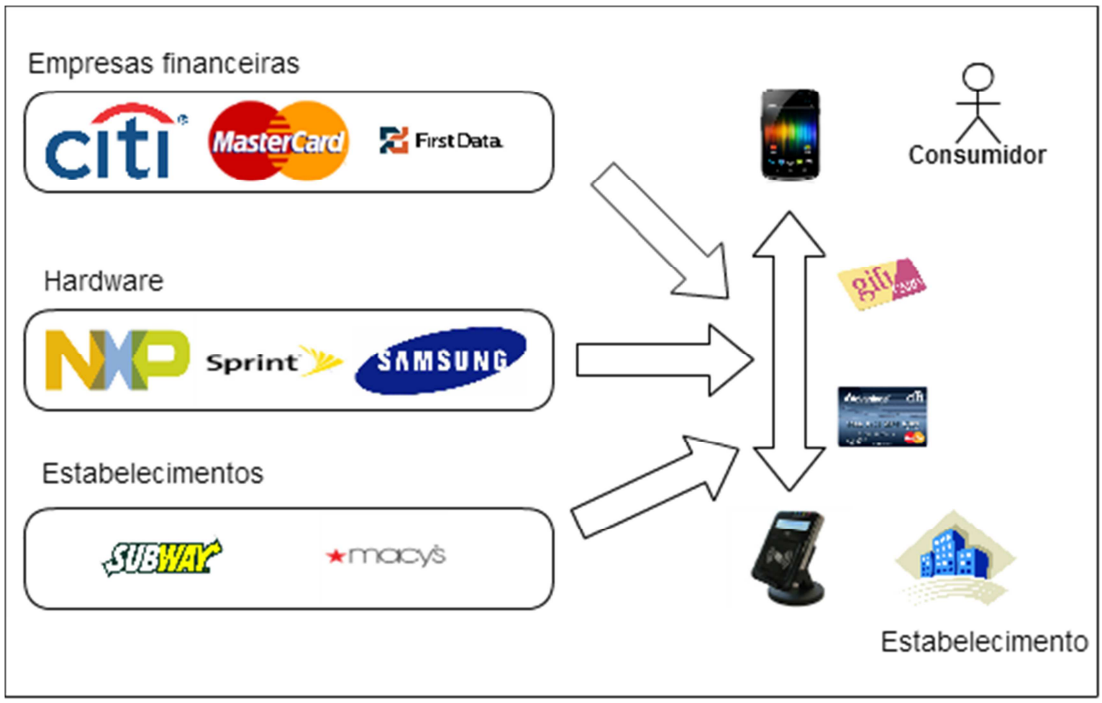
3.4 Google Wallet

No dia 19 de setembro de 2011, o Google disponibilizou uma aplicação para o sistema operacional Android que permite realizar o pagamento móvel através de dispositivos equipados com NFC. Inicialmente disponível apenas para o aparelho Nexus S da operadora de telecomunicações SPRINT, foi realizada uma parceria entre o banco Citibank e a empresa do

setor de pagamentos MasterCard, permitindo sua utilização em mais de 300.000 estabelecimentos que estejam equipados com a solução *MasterCard PayPass*.

A solução permite que um cartão Citibank Mastercard ou um cartão pré-pago do próprio Google seja utilizado no sistema. Logo após o seu lançamento, a VISA anunciou que permitiria o uso de seus cartões no sistema. Uma visão do ecossistema da solução é exibida na Figura 6.

Figura 6 Ecossistema da solução Google Wallet



Fonte: Baseado em (GOOGLE WALLET, 2011).

A aplicação necessita obrigatoriamente que uma senha seja configurada. Quando esta senha é digitada pelo usuário, o elemento seguro do sistema é habilitado, permitindo que o chip NFC do dispositivo seja utilizado. Quando o display do aparelho é desligado, a antena NFC também é desligada, evitando que uma compra indesejada seja feita pelo usuário. Por padrão, o usuário deve digitar a sua senha a cada 5 minutos, podendo configurar este tempo de acordo com sua preferencia.

O elemento seguro é um chip isolado do sistema operacional e do hardware do dispositivo, e que apenas é acessível por programas autorizados. Possui diversos níveis de proteção para a informação armazenada, e proteção contra alteração física isto é, o elemento seguro apaga os dados armazenados caso detecte alguma tentativa de violação (ROLAND, 2012). O sistema não guarda um histórico dos produtos que foram consumidos e pagos com a

carteira digital, mas sincroniza com os seus servidores o nome do estabelecimento e valor da transação. Como opção, a localização do usuário também pode ser salva.

Em poucos meses, diversas possibilidades de comprometer a segurança do sistema foram noticiadas (GOTH, 2012). Como a aplicação salva o PIN diretamente no telefone, e não em alguma área de dados do elemento seguro, é possível copiar este arquivo do dispositivo e tentar realizar algum ataque de força bruta. Entretanto, para ter acesso a este arquivo, é necessário o acesso ao dispositivo com privilégios de administrador Com a posse deste arquivo, e sabendo que um PIN é sempre numérico e possuem quatro dígitos, um ataque de força bruta teria que calcular apenas 10.000 valores (GOTH, 2012). Outra vulnerabilidade encontrada permite que um dispositivo roubado seja utilizado sem que seja obtido o privilégio de administrador no aparelho. Através da limpeza dos dados da aplicação Google Wallet, é possível informar um novo PIN para a aplicação, e uma vez que os dados do cartão de crédito estão ligados ao aparelho móvel, será possível utilizar os créditos do cartão pré-pago normalmente. Assim, é recomendável que a aplicação de carteira digital não seja utilizada em dispositivos em que o usuário já tenha realizado as alterações necessárias para ter o acesso como administrador do sistema, e que a operadora de telefonia móvel e a operadora do cartão de crédito sejam avisadas em caso de perda ou roubo do cartão, para que possam bloquear remotamente a sua utilização.

3.5 Comparação dos modelos estudados

A Tabela 4 tem como objetivo comparar os diversos modelos estudados, destacando pontos importantes para o desenvolvimento de um modelo de carteira digital que atenda ao maior número possível de funcionalidades.

Todos os trabalhos estudados fazem uso de um elemento seguro para armazenamento das informações confidenciais do usuário, além das informações referentes ao saldo. A utilização de um elemento seguro é um ponto essencial no desenvolvimento de um serviço de carteira digital, pois garante a integridade das informações, tornando o dispositivo menos vulnerável a fraudes (MOBEY, 2006).

Apenas o modelo japonês utiliza o cartão SIM como elemento seguro, caracterizando esta carteira digital como um modelo centralizado na operadora, Os demais modelos possuem o elemento seguro embarcado no hardware do dispositivo, e a solução fairCash faz uso de um SE próprio, o que limita a sua utilização em um número maior de dispositivos, sendo necessário embarcar o elemento seguro em um modelo de telefone móvel já existente.

Tabela 4 Comparação entre modelos

	mFerio	fairCash	Osaifu-Keitai	Google Wallet
Elemento Seguro	Sim	Sim (HW próprio)	Sim	Sim
Tipo de Elemento Seguro	Embarcado	Embarcado	Cartão SIM	Embarcado
Suporte à transações *offline*	Sim	Sim	Sim	Sim
Meio utilizado para pagamento	NFC	NFC/*Bluetooth*/WIFI	RFID/NFC	NFC
Divisão Monetária	-	eCoins	-	-
Anonimidade	Não	Anonimo para transações entre usuários. Transações entre usuário e estabelecimentos são rastreáveis.	Transações são rastreáveis através do emissor do cartão de crédito	Transações são rastreáveis através do emissor do cartão de crédito
Autenticação	PIN/Biometria /Desenho	PIN	PIN	PIN
Abrangência (Dispositivos Suportados)	Limitada	Limitada	Ampla	Limitada
Fidelidade/Cupons de desconto	Não	Não	Sim	Sim
SO Suportado	Symbian	Windows Mobile	Symbian/Android	Android

Fonte: Elaborado pelo autor

Os modelos estudados permitem a utilização da carteira digital de modo *offline*, sem necessitar de nenhuma comunicação com o servidor remoto. Entretanto, a solução fairCash necessita comunicação periódica com uma de suas casas da moeda virtuais, para conciliação do dinheiro digital com seu equivalente real. Esta comunicação pode ser realizada através de 3G ou rede WiFi. Este também é o único modelo que possui divisão monetária própria, chamada de *e-coins*. Esta divisão necessita de um grande sistema de gerenciamento, que deve ser responsável por validar a utilização do dinheiro digital e garantir sua integridade, adicionando complexidade ao projeto.

A comunicação através de NFC/RFID está presente em todos os trabalhos estudados, e é uma característica explorada por praticamente todas as soluções de carteira digital. Apenas a solução fairCash permite realizar pagamentos utilizando outros meios, como o pareamento entre dois dispositivos utilizando Bluetooh ou a criação de uma rede ad hoc WiFi.

A anonimidade é um importante critério também em um sistema de carteira digital. Como um de seus principais objetivos é a substituição do dinheiro físico pelo equivalente

digital, toda a sensação de anonimodade que o usuário sente ao realizar o pagamento com o dinheiro convencional deve estar presente na solução proposta. Devido a razões de segurança, como por exemplo, disputa de transações (*chargeback*), faz-se necessário que um usuário A possa provar que realizou uma transferência de dinheiro com um usuário B. Também é interessante que a transação seja rastreável caso a transferência tenha sido efetuada entre uma pessoa física e uma pessoa jurídica. Assim, a solução mFerio permite que o usuário obtenha informações da outra parte envolvida na operação; a aplicação fairCash apenas registra logs quando a transferência envolve pessoa física. O modelo japonês apresenta diferentes níveis de anonimidade, de acordo com a sua utilização. No caso em que efetua a emulação de um cartão de crédito, a transação poderá ser rastreada da mesma maneira que as transações de cartão de crédito convencional. Já as transações realizadas com a aplicação de bilhetagem eletrônica não são rastreáveis. Já o modelo atual do Google Wallet possui os mesmos níveis de anonimidade de um cartão de crédito convencional, ou seja, podem ser rastreadas.

Por padrão, todos os trabalhos estudados necessitam de um PIN para acesso ao software de carteira digital. Entretanto apenas a utilização de uma chave de acesso pode não garantir a segurança da informação (GOTH, 2012). De todos os sistemas estudados, apenas mFerio prevê a utilização de níveis mais avançados de segurança, como biometria ou desenhos na tela do *smartphone*. Embora disponível no sistema operacional Android, utilizado pelo Google Wallet e também pelo Osaifu-Keitai, o reconhecimento de voz ou até mesmo o reconhecimento facial não é utilizado por estas duas aplicações de carteira digital.

Outro importante critério não aproveitado pelos trabalhos estudados refere-se à utilização das informações de contexto. A localização do usuário pode ser utilizada para validar o local onde a transação está sendo efetuada, garantindo que o usuário encontra-se presente no local onde a operação está sendo realizada (MA et al, 2012). Sua localização também pode ser útil para exibir ao usuário locais próximos à ele que aceitem a utilização da sua carteira digital, ou que ofereçam desconto em algum restaurante (TATLI, 2005).

A abrangência dos trabalhos relacionados foi analisada quanto ao tipo de dispositivo que pode receber a carteira digital estudada. Desta maneira, mFerio possui uma abrangência bastante limitada, já que necessita de tecnologia NFC e é baseado no sistema operacional Symbian. Este sistema operacional, de propriedade da finlandesa Nokia, encontra-se descontinuado, dando lugar ao Windows Phone. No caso do fairCash, tem-se uma limitação ainda maior, já que este dispositivo foi idealizado para ser utilizado junto ao sistema

operacional Windows Mobile que não é mais utilizado, e teve seu protótipo desenvolvido para o dispositivo Compaq Ipaq, também descontinuado. Já o modelo japonês possui sua versão de carteira digital presente em mais de 30 dispositivos diferentes, incluindo versões para o sistema operacional Android. Por sua vez, em 2012 o Google Wallet está disponível para oito diferentes tipos de dispositivos, incluindo o tablet Nexus 7, e está restrito ao sistema operacional Android.

3.6 Considerações finais

Com base nas comparações efetuadas acima, foram tomadas as decisões necessárias para especificação de um modelo de carteira digital. A utilização de um elemento seguro é considerada uma boa prática pelas fontes estudadas, agregando segurança ao sistema e contribuindo para a aceitação do modelo no mercado. Este elemento deve estar embarcado no dispositivo, devendo sair de fábrica com as credenciais e aplicações necessárias já instaladas. Esta configuração pode ser alcançada com alguma parceria entre a empresa desenvolvedora da solução de carteira digital e fabricantes de celular, da mesma maneira que é feita a customização da aplicação Google Wallet nos Estados Unidos, que já é enviado de fábrica com a aplicação. A utilização de um elemento seguro próprio, como no caso do mFerio, foi descartada, pois o estudo e desenvolvimento de um elemento seguro não é o foco deste trabalho. A utilização do Cartão SIM como elemento seguro foi descartada, pois envolveria também a operadora de telefonia móvel na configuração e habilitação de aplicações no SE. Também é considerado um ponto negativo o fato de cada operadora de telefonia ter sua própria configuração de elemento seguro, sendo necessário então que as operadoras trabalhem em conjunto para o desenvolvimento de uma solução unificada.

Com a utilização do elemento seguro, é possível realizar o armazenamento de dados sensíveis do usuário de maneira *offline*, fazendo com que o sistema não necessite de nenhum tipo de conexão com um sistema externo para operar. Esta é uma característica importante para o modelo a ser desenvolvido, que permitirá que a transação seja efetuada em qualquer lugar, assim como é feito com o dinheiro convencional.

O modelo UniPag deve utilizar NFC para operações que envolvam a utilização do elemento seguro, mas também deve ser capaz de utilizar a comunicação com outros dispositivos através de outros protocolos, como WiFi, *Bluetooth* e QR CODE. A utilização destas tecnologias permite que a aplicação a ser desenvolvida seja utilizada em um grande número de dispositivos móveis, dos mais modernos smartphones até celulares simples, equipados com uma câmera fotográfica.

A utilização de uma unidade monetária própria foi descartada, já que a sua utilização no modelo fairCash é acompanhada de uma infraestrutura para geração e controle destas moedas, o que aumenta a complexidade do projeto e está fora do escopo deste trabalho. Assim não será necessária nenhuma conversão entre a moeda digital e a moeda real, facilitando a aceitação por parte do usuário final.

O modelo deverá garantir o máximo de anonimidade para o usuário nas transações efetuadas em modo P2P (transferência entre usuários), permitindo que seja gravado um log da operação realizada, contendo informações como local onde a operação foi efetuada e valor da transação. Entretanto, nenhuma informação pessoal deve ser armazenada, evitando então que a transação seja rastreável, assim como em uma operação com dinheiro físico. A autenticação do usuário deve ser feita através de um PIN. Quando disponível no dispositivo móvel, esta autenticação pode será ser realizada em conjunto com outro nível de autenticação, como biometria ou desenho de algum padrão na tela do dispositivo.

A utilização do contexto pode ser explorada. Como exemplo, o usuário pode receber notificações de algum desconto em sua loja preferida caso encontre-se próximo a ela e receber informações dos estabelecimentos de um shopping center, de acordo com seu perfil. Esta característica adiciona uma grande complexidade ao trabalho e não será utilizada neste modelo, sendo indicada como trabalhos futuros. Esta localização também pode ser utilizada para agregar segurança à transação financeira, garantindo que o usuário que está realizando a transação encontra-se de fato no estabelecimento.

Por fim, um ponto importante é a possibilidade da aplicação responsável pela carteira digital realizar algum tipo de integração com o sistema de pedidos do estabelecimento, possibilitando ao usuário efetuar *check-in* em um determinado local e fazer o seu pedido automaticamente, e receber seu almoço diretamente em sua mesa, ou efetuar o pagamento e retirada do produto direto no caixa, sem nenhuma intervenção humana. Estas compras então podem ser pagas com a utilização de um cupom de desconto, e a compra pode gerar pontos de fidelidade, que são armazenados no dispositivo móvel. Nenhum dos trabalhos relacionados possui integração com o sistema de pedidos, e apenas o Google Wallet e Osaifu-Keitai possuem suporte à fidelidade e cupons de desconto.

4 MODELO UNIPAG

Com base na comparação dos modelos anteriores, foram escolhidas as características que devem ser contempladas pelo modelo a ser desenvolvido (Tabela 5). O UniPag deverá ter suporte à um elemento seguro, garantindo a integridade dos dados sensíveis armazenados no dispositivo. Este elemento seguro pode ser embarcado no dispositivo, disponibilizado através de um cartão de memória ou no próprio SIM card, através de uma parceria com as operadoras de telefonia móvel. A utilização do elemento seguro permite que dois usuários do sistema realizem um pagamento entre si de maneira *offline*. Além disso, a solução também permite o pagamento entre o usuário e um estabelecimento comercial. Esta operação pode ser totalmente *offline*, para transações de pequeno valor, ou *offline* para o dispositivo móvel e *online* para o estabelecimento, quando a transação exceder o valor máximo permitido. Optou-se pela utilização de um moedeiro eletrônico com as mesmas características monetárias da moeda convencional, sem a criação de divisões monetárias específicas.

Tabela 5 Características do modelo

Elemento Seguro (SE)	Suporte à transações Offline	Divisão Monetária	Anonimidade	Autenticação	Abrangência	Fidelidade	SO
SIM	Sim	Não	Total (pagamento P2P)	PIN	Ampla	Sim	IOS Android

Fonte: Elaborada pelo autor

As transações entre dois usuários devem ser totalmente anônimas, assim como as transações envolvendo dinheiro convencional. Já as transações envolvendo uma pessoa jurídica são possíveis de serem rastreadas, da mesma maneira que as transações comerciais atuais envolvendo um cartão de crédito ou débito. A autenticação do usuário deverá ser feita através de uma senha numérica (PIN), a ser armazenada no dispositivo de maneira segura, utilizando uma criptografia forte, como AES, a fim de evitar que outro usuário tenha acesso ao seu conteúdo, e por consequência, aos dados sensíveis armazenados no dispositivo. Outros métodos de autenticação podem ser desenvolvidos, como biometria ou desenho de algum padrão na tela. Entretanto, a utilização de um PIN garante que a solução poderá ser utilizada em um número maior de dispositivos.

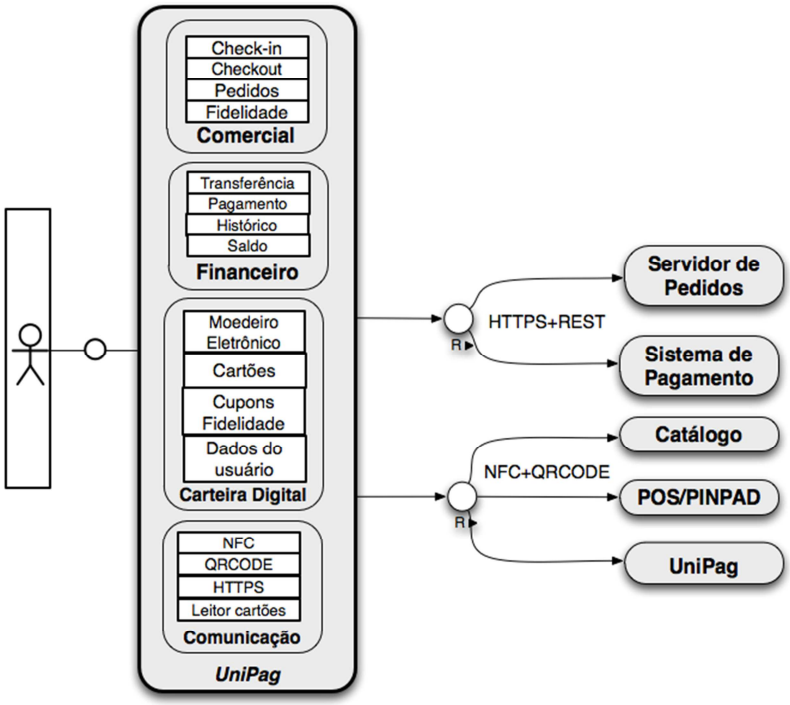
O sistema pode suportar a fidelização do usuário, beneficiando o usuário pela utilização da solução, ou também através da parceria com os estabelecimentos comerciais, premiando o

usuário de acordo com a utilização da solução em um determinado restaurante, por exemplo. O modelo pode ser utilizado em um grande número de dispositivos móveis, pois tem como requisito mínimo a necessidade de uma câmera fotográfica para leitura de QR CODE e que o dispositivo móvel possua a capacidade de instalação de aplicativos. Estas características estão presentes em todos os modelos de smartphones disponíveis.

4.1 Arquitetura do modelo

Uma visão geral da arquitetura proposta para o modelo, com as diversas interações possíveis da aplicação e sistemas envolvidos no pagamento, é exibido na Figura 7. Essa arquitetura foi desenvolvida usando a notação TAM (*Technical Architecture Modeling*) (TAM, 2012), proposta pela SAP (SAP, 2007). Esta notação é uma combinação de FMC (*Fundamental modeling concepts*) e UML (*Unified Modeling Language*), duas ferramentas para modelagem de sistemas (FMC, 2012).

Figura 7 Visão Geral da arquitetura proposta



Fonte: Elaborado pelo autor.

O modelo desenvolvido possui quatro diferentes módulos:

- **Comercial:** Responsável pela comunicação da aplicação com o servidor de pedidos do estabelecimento comercial, permitindo ao usuário consultar e realizar pedidos através de um catálogo disponibilizado *online*. Também realiza a interface do usuário com o programa de fidelidade do estabelecimento.

- **Financeiro:** O módulo financeiro permite ao usuário efetuar um pagamento eletrônico para outro usuário do sistema ou diretamente a um sistema de pagamento já existente. Também permite a comunicação com um leitor de cartões externo, fazendo com que o dispositivo móvel funcione como um terminal de ponto de vendas (POS);
- **Carteira digital:** O módulo de carteira digital é o responsável pela interface do usuário com o elemento seguro. Neste módulo, estão armazenados os cartões de crédito do usuário, seus cupons/cartões de fidelidade, e seu moedeiro eletrônico, que permite o armazenamento de dinheiro virtual. Também é responsável pela retenção dos dados do usuário de maneira segura;
- **Comunicação:** Este módulo é o responsável pela comunicação do modelo com os sistemas e periféricos externos, como o servidor de pedidos (HTTPS+REST[1]), catálogo (NFC+QR CODE), leitor de cartões (USB ou similar), entre outros.

Para ilustrar melhor o funcionamento do modelo e a interação entre os diferentes módulos, considere o seguinte cenário:

"Ao chegar a um estabelecimento comercial, o usuário pode utilizar a aplicação e realizar o *check-in*. Caso o estabelecimento possua integração com o sistema UniPag, o usuário receberá as informações referentes ao servidor de pedidos e rede Wifi do estabelecimento comercial, possibilitando realizar a consulta por produtos diretamente do seu dispositivo móvel. Ao finalizar o seu pedido, o usuário poderá efetuar o pagamento através de seu cartão-presente, disponível no módulo Carteira Digital, ou utilizar um de seus cartões de crédito em conjunto com um leitor de cartões acoplado no dispositivo. Por fim, o estabelecimento comercial poderá ter um programa de fidelidade, que dará ao usuário pontos para a troca de produtos. Estes pontos serão cadastrados no cartão fidelidade do usuário, que se encontra no módulo Carteira Digital.".

4.2 Módulo comercial

Buscando agregar novas funcionalidades ao pagamento móvel, o módulo comercial permite ao usuário realizar consultas e pedidos através de um catálogo *online* fornecido pelo estabelecimento. Este catálogo estará disponível ao usuário após a realização de um *check-in* dentro da aplicação. Este *check-in* irá indicar a sua presença em um determinado local e

[1] http://rest.elkstein.org

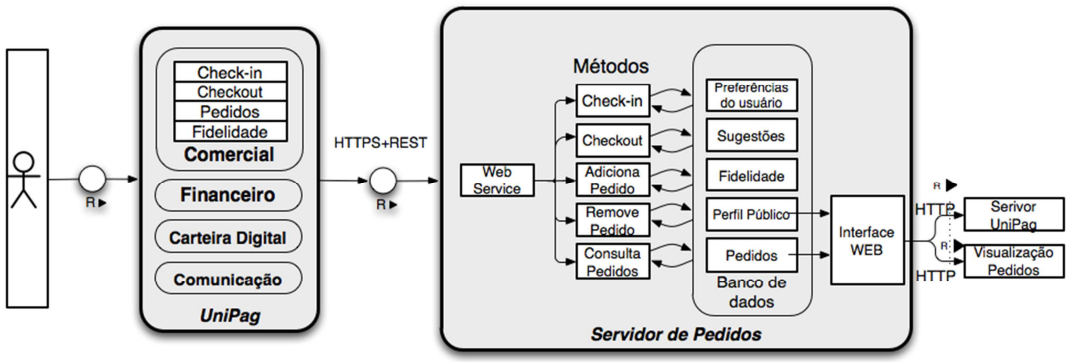
fornecerá acesso ao servidor de pedidos do estabelecimento. Através deste servidor, o usuário pode consultar os produtos previamente cadastrados e efetuar seu pedido diretamente no dispositivo móvel.

O servidor de pedidos pode ser configurado de acordo com o tipo de comércio executado no local. Por exemplo, um restaurante pode cadastrar seu cardápio em uma página web, e incluir *tags* NFC ou QR CODES nos cardápios físicos. Para uma loja de roupas, o servidor do estabelecimento pode ter o cadastro de todos os itens do vestuário, permitindo que o usuário selecione estes itens e estes sejam entregues diretamente no provador, por exemplo. Quando o usuário não estiver presente no estabelecimento, a aplicação pode listar os itens disponíveis e permitir que o usuário efetue a reserva deles remotamente.

Ao realizar o *check-in* no estabelecimento, é executada a chamada ao método *check-in* do Web Service, o servidor de pedidos é avisado da sua presença e os pedidos serão entregues. A arquitetura do servidor de pedidos, bem como comunicação com o dispositivo móvel, é exibida na Figura 8.

A aplicação comunica-se com a o servidor de pedidos através de um WebService (REST), caracterizado na figura pelo módulo Web Service. Este servidor encontra-se na rede interna do estabelecimento comercial, ou remotamente, através da utilização de servidores na nuvem. O dispositivo móvel recebe os dados de conexão à rede do estabelecimento através de uma *tag* NFC ou QR CODE, disponível em algum lugar visível do estabelecimento. O usuário também poderá receber os dados de conexão à rede do estabelecimento através do *check-in* no estabelecimento, onde receberá um identificador único por estabelecimento e poderá consultar uma base para obter esta informação. Neste caso, o usuário deverá utilizar-se da conexão disponível no dispositivo móvel (GPRS, 3G) para efetuar o *check-in*.

Figura 8 Arquitetura do servidor de pedidos



Fonte: Elaborado pelo autor.

O Web Service implementa métodos como *Check-in*, *Checkout*, Adiciona, Remove e Consulta pedidos, conforme exibido na Figura 8. Ao efetuar o *check-in*, algumas informações do usuário são recuperadas do banco de dados, como as preferências e histórico de pedidos. Esta consulta é realizada na base de dados interna do estabelecimento, e somente terá validade caso o usuário já tenha realizado alguma compra no local. Opcionalmente, o servidor pode consultar uma base de cadastros geral da aplicação UniPag, definida na figura como Servidor UniPag, solicitando os dados públicos autorizados pelo usuário, como por exemplo, histórico de pedidos do usuário em outros estabelecimentos e sugestões de outros frequentadores. Estas informações podem então ser utilizadas para fornecer sugestões de compra.

Os pedidos podem ser realizados através do aplicativo, utilizando também as *tags* NFC ou QR CODE, conforme a Figura 9, que exibe uma integração entre as duas soluções, através da confecção de *tags* NFC com QR CODE embutido, viabilizando a solução para um grande número de aparelhos móveis.

Figura 9 *Tag* NFC com QR CODE

Fonte: Elaborado pelo autor

Ao selecionar a *tag*, é exibido no visor do dispositivo uma página web contendo informações sobre o produto, como preço, disponibilidade e produtos relacionados. Com a confirmação do pedido do usuário, uma nova chamada ao Web Service é realizada. O pedido do usuário passa a ser exibido na lista de pedidos do estabelecimento, através da página Web para consultas. O usuário pode realizar consultas e remover algum pedido a qualquer momento diretamente no seu dispositivo móvel. O estabelecimento comercial também pode remover algum pedido da sua lista, informando ao usuário o motivo do cancelamento.

Ao fim de sua permanência, o usuário deve efetuar a operação chamada de *checkout*, onde irá registrar a sua saída do sistema, através de nova chamada ao WebService. Como

retorno, o usuário irá receber o total gasto com os seus pedidos, e terá como opção de pagamento os meios tradicionais, como dinheiro ou pagamento com o meio eletrônico já existente no estabelecimento, e também a utilização dos módulos de pagamento disponíveis na aplicação.

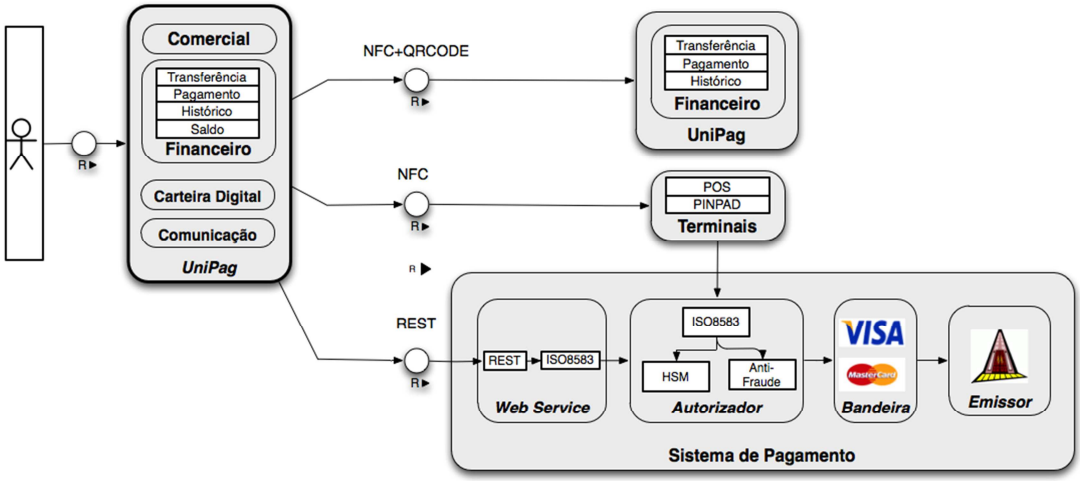
4.3 Financeiro

O módulo financeiro fornece ao usuário as opções para efetuar o pagamento eletrônico, através do seu moedeiro eletrônico ou cartões cadastrados no dispotivo. Através dele, um usuário poderá efetuar as seguintes operações:

- **Transferência:** O usuário poderá efetuar ou receber um pagamento utilizando o seu moedeiro eletrônico, através da comunicação de dois dispositivos móveis que estejam utilizando o aplicativo Unipag;
- **Pagamento:** Através da utilização de NFC, o usuário poderá utilizar sua carteira digital para efetuar um pagamento em terminais disponibilizados pelas redes que realizam operações com cartão de crédito no comércio, desde que estes terminais estejam equipados com a tecnologia NFC. Também permite que o aparelho seja utilizado como um ponto de venda, através da comunicação do dispositivo móvel com um leitor de cartões externo;
- **Histórico:** Todas as transações financeiras executadas pelo usuário estarão disponíveis através desta funcionalidade. O sistema pode permitir que o usuário armazene uma descrição de sua compra junto com uma foto do produto adquirido, facilitando o controle de gastos do usuário.
- **Saldo:** Permite ao usuário a consulta do saldo disponível em seu moedeiro eletrônico ou em seus cartões pré pagos ou cartões presente.

A arquitetura do módulo é exibido na Figura 10.

Figura 10 Arquitetura do módulo financeiro



Fonte: Elaborado pelo autor

Através deste módulo, o usuário pode efetuar o pagamento para outro usuário utilizando o seu moedeiro eletrônico. Esta operação pode então ser concretizada utilizando o protocolo NFC e aproximando os dispositivos, ou gerando um código QR e efetuando a leitura utilizando a câmera fotográfica do dispositivo móvel. Esta operação direta entre dois usuários assemelha-se ao pagamento com dinheiro convencional.

O usuário também pode efetuar o pagamento utilizando um dos seus cartões cadastrados no módulo carteira digital. Estes cartões podem ser de débito, crédito, *gift card* ou pré pago. Após a seleção do cartão, o usuário pode efetuar a transação através de NFC ou código QR. Neste caso, o pagamento será realizado com a aproximação do dispositivo móvel a um terminal POS, pinpad TEF ou um dispositivo Mastercard Paypass, por exemplo. Caso uma interface de pagamento que utilize QR CODE seja desenvolvida e disponibilizada ao estabelecimento, esta também pode ser uma opção para pagamento.

Estas duas operações necessitam de interação com o módulo carteira digital, para acesso aos dados sensíveis da aplicação, presentes no elemento seguro, e com módulo comunicação, para interface da aplicação através de NFC ou código QR.

Além do pagamento utilizando o moedeiro eletrônico ou um dos cartões armazenados no elemento seguro, a solução também permite a integração do pagamento com um servidor de pagamento já existente, através de um leitor de cartões acoplado ao seu *smartphone*. Este leitor pode permitir apenas transações utilizando tarja magnética, ou efetuar a leitura do smartcard e solicitar a senha do usuário, caso seja capaz de ler chips no formato EMV.

Para efetuar o pagamento, o dispositivo móvel deve estar vinculado ao estabelecimento comercial em que se encontra. Desta maneira, ao selecionar esta opção, a aplicação irá requisitar as configurações do estabelecimento comercial ao servidor do estabelecimento, configurando o dispositivo móvel do usuário para efetuar o pagamento móvel dos bens consumidos. São necessárias informações como código do estabelecimento, endereço de conexão e possibilidades de pagamento (à vista, parcelado etc). Isto torna o dispositivo móvel do usuário em um *Point Of Sale* (POS), e permite que cada cliente utilize seu próprio aparelho para realizar o pagamento. Ao finalizar o pagamento e sair deste módulo, a aplicação deve apagar as configurações específicas do estabelecimento, permitindo que o usuário faça um novo pagamento em outro local.

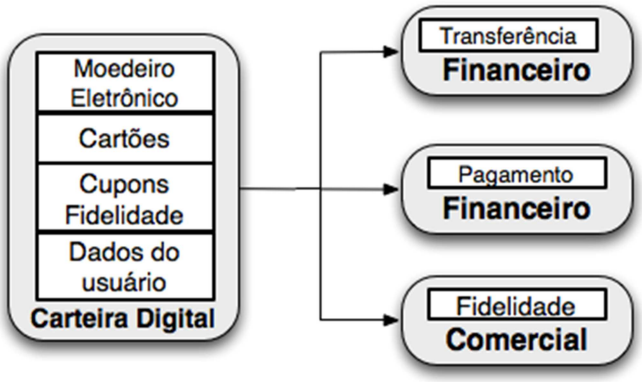
Esta transação é enviada para o sistema autorizador através de uma chamada a um Web Service, que recebe a mensagem e converte para o formato de mensagem esperado pelo autorizador. Informações como perfil de compras do usuário e geolocalização podem ser validadas pelas ferramentas de Anti Fraude. O sistema de pagamento faz uma tradução da senha do usuário para a senha da bandeira utilizando o HSM (Hardware Security Module), um hardware dedicado para realizar criptografia e descriptografia. A transação é então enviada para a bandeira (como VISA ou MASTERCARD), que efetua validações da situação do usuário, como regularidade do cartão e senha. Por fim, a transação é encaminhada para o sistema autorizador do banco emissor do cartão, que realiza as últimas validações do cliente (limite disponível, cadastro, etc.).

4.4 Carteira digital

A principal função deste módulo é armazenar os dados do usuário de maneira segura, através da interface da aplicação com o elemento seguro disponível no dispositivo móvel. Os dados sensíveis referentes aos cartões do usuário e seu moedeiro eletrônico são gerenciados por este módulo. Informações referentes ao cadastro do usuário também podem ser armazenadas no elemento seguro, garantindo a segurança das informações.

É possível gerenciar os cartões cadastrados na aplicação, efetuando o cadastro de novos meios de pagamento ou removendo cartões já existentes. Também é possível consultar o saldo do moedeiro eletrônico e de cartões pré-pagos. Este módulo comunica-se com os demais conforme Figura 11.

Figura 11 Módulo carteira digital



Fonte: Elaborado pelo autor

Os dados do usuário, referentes à senha para utilização da aplicação e suas preferências, são compartilhados entre os diversos módulos da aplicação.

4.5 Segurança

A segurança é um aspecto importante no mercado de transações eletrônicas, conforme discutido no capítulo 2.1.2. Um problema na segurança da informação de uma empresa de transações eletrônicas pode fazer com que a informação de diversos clientes seja disponibilizada de maneira indevida, incluindo informações sensíveis, como números de cartões de crédito, fazendo com que a empresa perca sua credibilidade frente aos seus clientes. Desta maneira, uma solução de comércio eletrônico móvel deve preocupar-se sempre com a segurança dos dados trafegados em todas as etapas de uma transação eletrônica.

O cadastro do usuário deve ser completo, buscando minimizar a utilização da solução por usuários mal intencionados. No mercado de transações eletrônicas, é normal que dados como comprovante de residência e faturamento mensal seja solicitado ao responsável pelo estabelecimento. A solução deve prever também que estes dados sejam solicitados ao usuário final. Também pode ser estipulado um limite máximo de utilização da solução para o usuário inicialmente, caso o usuário ainda não tenha efetuado um cadastro completo. Este limite pode ser no número de transações ou valor total movimentado pela sua conta. Caso deseje continuar a utilizar a solução, o usuário deve então preencher um cadastro completo.

Como alternativa, é possível vincular o cadastro do usuário à sua conta no Facebook, importando dados pessoais e preferências do usuário. Este cadastro do usuário no sistema UniPag deve ser realizado através de uma conexão segura, utilizando para isto a comunicação através de Web Services que utilizem HTTPS.

A comunicação do dispositivo móvel com o servidor de pedidos é feita geralmente com o usuário na rede local do estabelecimento. Esta rede deve estar protegida através de um *firewall*. A comunicação do dispositivo móvel com o servidor segue o padrão de Web Services REST utilizando HTTPS. As informações gravadas nas *tags* NFC e QR CODE são criptografadas.

Para pagamentos efetuados através da carteira digital, a segurança é garantida pela utilização do elemento seguro. Caso exista mais de uma aplicação de carteira digital instalada no dispositivo móvel, cada uma das aplicações possui sua área de memória no SE, evitando a utilização indevida de dados. A comunicação entre os dois dispositivos utilizando NFC é criptografada, e devido à característica de proximidade do protocolo, é garantido que a comunicação está sendo realizada entre os dispositivos desejados.

Para pagamentos efetuados com a utilização de um leitor acoplado ao terminal, sãp necessários alguns cuidados extras. Primeiramente, o cartão do usuário é lido através de um leitor. Este leitor pode ser conectado através da entrada de áudio do dispositivo (*áudio jack*) ou através da interface padrão de dados (USB para dispositivos Android ou conector Dock para dispositivos Apple). Caso o próprio leitor de cartão possuir um chip que realize a criptografia do cartão através de algum algoritmo implementado pelo fabricante, garante-se que estas informações não estejam disponíveis caso um usuário mal intencionado instale algum programa no dispositivo que possa capturar estes dados. Entretanto, o servidor responsável pela captura destes dados deverá ser capaz de descriptografar os dados, seja através da utilização de uma biblioteca fornecida pelo fabricante do dispositivo ou da implementação em código de algum algoritmo de mercado.

Caso opte pela utilização de algum leitor que realize a captura da senha (PIN), este deve ser homologado de acordo com as regras de mercado (PCI-DSS). A mesma regra se aplica para a captura de cartões com chip EMV, com os leitores devendo atender à especificação EMV 4.3. A comunicação do servidor do estabelecimento com o sistema de pagamentos deve ser efetuada através de uma VPN, e toda a informação trafegada entre as duas partes deve ser criptografada.

Por fim, a localização do usuário pode ser utilizada como importante informação para a prevenção de fraudes. Através do mapeamento dos locais onde o usuário normalmente utiliza a aplicação, é possível permitir limites maiores para determinadas compras. Também podemos utilizar esta informação para a verificação de fraudes. É possível comparar a localização do usuário entre utilizações sucessivas da aplicação. Assim, caso o usuário efetue

duas transações em um curto espaço de tempo, mas com localizações completamente diferentes, é possível efetuar o bloqueio da conta do usuário no sistema. Caso o usuário tenha efetuado *check-in* no estabelecimento, mas sua localização não coincida com a localização do estabelecimento, a mesma ação pode ser tomada.

4.6 Comunicação

Diversos protocolos são utilizados para a comunicação entre o dispositivo móvel e os sistemas envolvidos no pagamento eletrônico. Em alguns dos casos, onde não há dependência de uma terceira parte envolvida, é possível escolher o melhor protocolo para comunicação. Já em partes em que é necessária uma integração com um sistema externo, é necessário seguir o protocolo já utilizado.

4.6.1 NFC e QR CODE

Para a comunicação entre dois dispositivos utilizando a aplicação Unipag, para a troca de informações entre o dispositivo móvel e um ponto de pagamento, e também para a leitura de informações externas, como por exemplo, um catálogo, são utilizados os protocolos NFC e QR CODE.

A comunicação através de NFC permite a troca de informações rápida através da aproximação de dois dispositivos. Esta troca de informações deve ser realizada com segurança, e por isso, toda informação trafegada deve estar criptografada.

Para os dispositivos que não possuam NFC, é possível realizar as operações através da utilização dos códigos QR. Embora não possua a mesma facilidade de uso do protocolo NFC, os códigos QR podem ser utilizados por um número maior de aparelhos, já que o único pré requisito no dispositivo móvel é a presença de uma câmera fotográfica.

4.6.2 Web Services

Para realizar o cadastro do usuário a partir do dispositivo móvel, e também para efetuar as requisições envolvendo *tags* NFC ou QR CODE, optou-se pela comunicação através de Web Services. Esta comunicação permite um bom nível de segurança, pois no modelo é utilizado HTTPS.

Dois tipos de protocolos podem ser utilizados para WebServices: SOAP (Simple Object Access Protocol) e REST (Representational State Transfer). De acordo com (UPADHYAYA, 2011), o protocolo REST pode melhorar a flexibilidade, escalabilidade e desempenho dos sistemas, se comparado com o protocolo SOAP, além de consumir menos recursos (bateria, memória, processador) e ser mais fácil de ser implementado

. Em ROEHRS (2012), é realizado um estudo comparativo entre as duas tecnologias, levando em conta principalmente o consumo de bateria frente ao tráfego gerado pela aplicação. O autor conclui que a utilização de REST leva a uma economia de mais de 50% no consumo da bateria. Este fato deve-se principalmente à menor quantidade de dados necessários pelo protocolo.

A comunicação utilizando Web Services é facilitada pela utilização de bibliotecas, disponíveis para os principais dispositivos móveis (iOS, Android e Windows Phone). Os principais sistemas operacionais móveis do mercado não apresentam uma API nativa para utilização de Web Service SOAP. Já o protocolo REST apresenta API nativa, e seu uso é fortemente indicado, conforme (GOOGLE IO, 2010). Pelos motivos expostos, o modelo proposto propõe o emprego de REST.

4.6.3 Protocolo ISO

Para comunicação com o servidor de pagamentos, o modelo UniPag deve empregar o protocolo ISO 8583 (ISO, 1993), conforme descrito no capítulo 2.1.1. É necessária a criação de uma biblioteca de comunicação para todos os dispositivos móveis, pois este não é um protocolo amplamente difundido.

Cada tipo de mensagem trocada entre o meio de captura e a instituição financeira é caracterizado por um tipo de mensagem e um código de processamento. Assim, as mensagens são agrupadas de acordo com a Tabela 6.

Tabela 6 Tipos de mensagem ISO

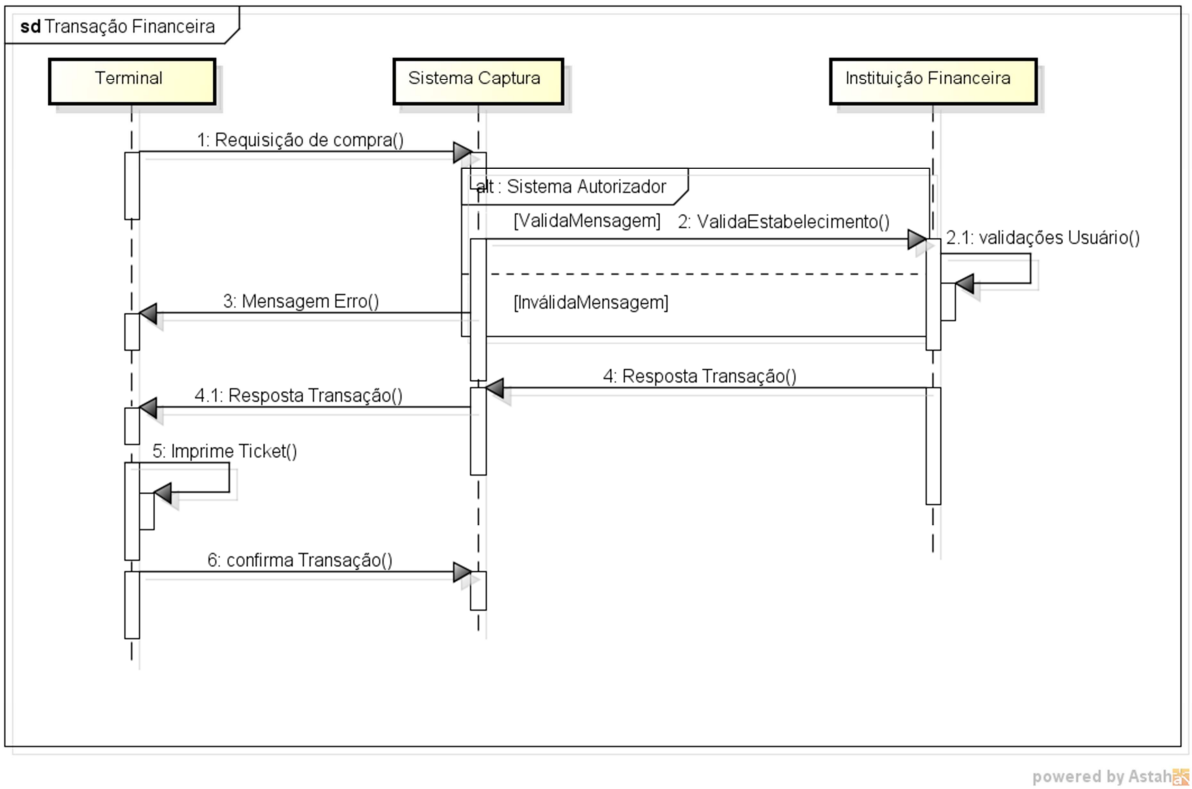
Tipo de mensagem	Sentido	Código(s) processamento	Descrição
0200	Meio Captura ->Autorizador	008000, 003000, 002000	Requisição de compra crédito, débito ou voucher
0210	Autorizador->Meio Captura	008000, 003000, 002000	Resposta à requisição de compra
0202	Meio Captura->Autorizador	008000, 003000, 002000	Confirmação da compra pelo meio de captura
0100	Meio Captura ->Autorizador	0033000	Consulta saldo disponível
0110	Autorizador->Meio Captura	0033000	Retorno saldo disponível
0800	Meio Captura ->Autorizador	0099999	Solicita configuração
0810	Autorizador->Meio Captura	0099999	Retorno Configuração
0802	Meio Captura ->Autorizador	0099999	Confirma configuração
0420	Meio Captura ->Autorizador	0022000	Desfazimento transação
0430	Autorizador->Meio Captura	0022000	Resposta desfazimento

Fonte: Elaborado pelo autor

Cada uma das mensagens descritas acima é caracterizada por campos, chamados de *data elements* (DE) Cada DE possui alguma informação relevante para a transação, como data, hora, valor da transação e número sequencial único. As mensagens de resposta possuem em seu DE 39 o status da transação. No caso em que a transação é aprovada (DE 39 = 0), o terminal irá proceder com o envio da mensagem de confirmação, quando aplicável. Caso a transação seja declinada pelo autorizador, este DE terá um valor diferente de zero, indicando o motivo pelo qual o sistema remoto não autorizou a transação.

Para garantir a integridade das transações e não permitir que nenhuma mensagem fique pendente no sistema, o terminal possui um DE que contém um NSU (número sequencial único), e também um DE contendo o NSU da última transação aprovada. Estes números são enviados pelo meio de captura em cada uma das transações, e o sistema autorizador armazena este valor. Desta maneira, o sistema possui um controle da última transação que foi aprovada, e em caso de não receber uma mensagem de confirmação do meio de captura, a próxima transação deste terminal irá confirmar a transação anterior.

Figura 12 Fluxograma de uma transação financeira



Fonte: Elaborado pelo autor

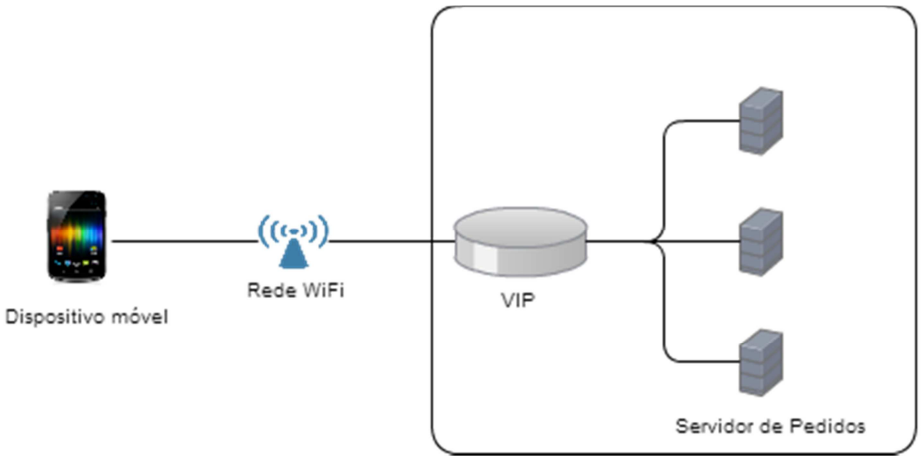
4.6.4 Escalabilidade

Um dos desafios parra a implementação de um modelo para pagamento móvel que envolva a integração entre diversos sistemas é a garantia de disponibilidade dos diversos sistemas envolvidos na transação. O sistema proposto envolve diferentes sistemas, que se encontram em locais variados, aumentando a dificuldade de desenvolvimento de uma solução altamente disponível e escalável.

A infraestrutura necessária para o funcionamento do servidor de pedidos encontra-se inteiramente no estabelecimento comercial, sendo basicamente uma arquitetura cliente/servidor. Esta arquitetura permite que novos servidores sejam instalados e acessados através de uma única referência, com as requisições sendo distribuídos por alguma ferramenta de balanceamento.

Esta solução também contribui para o aumento da disponibilidade do sistema, já que, em caso de indisponibilidade de uma das máquinas, o sistema irá continuar em operação. Entretanto, a instalação de diversas máquinas em um ambiente sem uma boa infraestrutura, como é o caso da maioria dos estabelecimentos comerciais, pode não ser a solução mais indicada. Um exemplo desta arquitetura é exibido na Figura 13.

Figura 13 Infraestrutura interna para servidor de pedidos



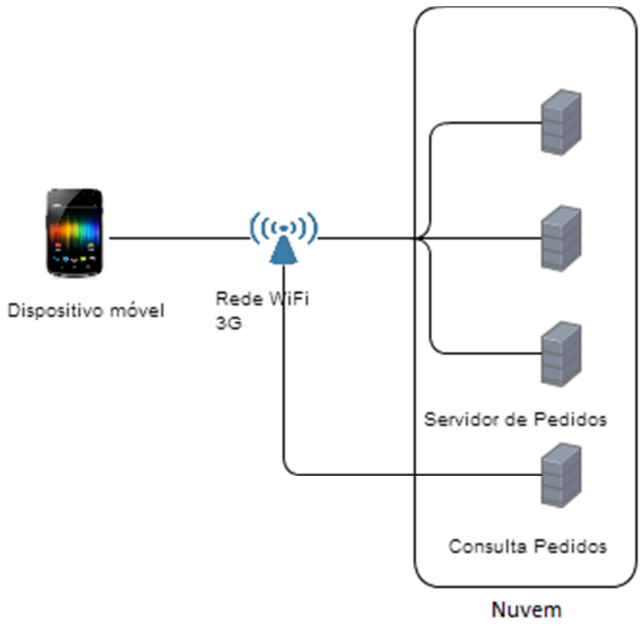
Fonte: Elaborado pelo autor

O hardware descrito como VIP (*Virtual IP*) é o responsável pelo balanceamento da carga entre os N servidores. Desta maneira, um usuário que deseje utilizar seu dispositivo móvel com a aplicação Unipag para conectar-se ao servidor de pedidos irá realizar a conexão através do IP deste hardware, que realiza a distribuição da carga entre as máquinas configuradas para receber este serviço, caso necessite que estas máquinas trabalhem em um serviço ativo-ativo (múltiplas máquinas ativas recebendo conexões). Também é possível configurar apenas uma máquina ativa, permitindo que o VIP realize o envio das requisições para a máquina em *stand by* caso detecte algum problema na máquina primária.

Os servidores podem ser alocados na nuvem, utilizando então um serviço altamente disponível de nuvem computacional, como o Amazon EC2[2], permitindo que as requisições sejam armazenadas com segurança. Além das informações dos pedidos, estes servidores podem ser responsáveis pela interface web que irá exibir as informações dos pedidos no estabelecimento. Como requisito para este modelo de negócio, é necessária uma conexão de internet altamente disponível. Esta arquitetura é descrita na Figura 14.

[2] http://aws.amazon.com/pt/ec2/

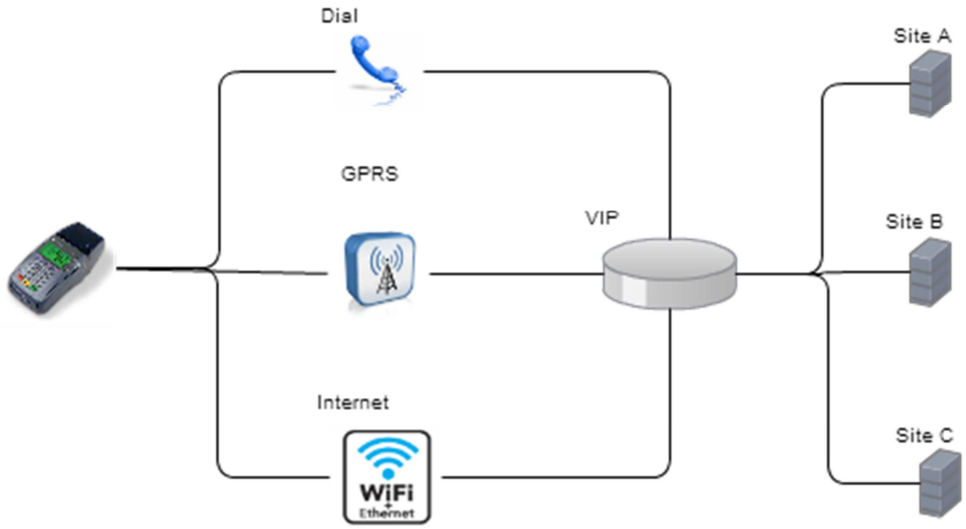
Figura 14 Arquitetura do servidor de pedidos na nuvem



Fonte: Elaborado pelo autor

Ao efetuar a transação financeira através da integração com o sistema de pagamento, a disponibilidade e desempenho do sistema são garantidos pelas instituições financeiras envolvidas, que possuem em sua infraestrutura máquinas que permitem a realização de centenas de transações simultâneas, bem como contingenciamento e distribuição de carga entre diversas máquinas, muitas vezes encontradas em lugares físicos diferentes. Um exemplo da arquitetura dos sistemas de pagamento é exibido Figura 15.

Figura 15 Arquitetura transacional



Fonte: Elaborado pelo autor.

5 IMPLEMENTAÇÃO

Este capítulo apresenta uma descrição dos aspectos relacionados ao desenvolvimento do protótipo do modelo proposto. As diversas ferramentas de desenvolvimento, emuladores, bibliotecas e dispositivos utilizados na implementação são descritos. A escolha do sistema operacional móvel é parte importante para a construção do protótipo. O sistema operacional escolhido deve possuir suporte à aplicações de terceiros e possibilidade de disponibilização do aplicativo *online*. Também deve estar disponível em um grande número de dispositivos, acessíveis à diferentes camadas da população, facilitando a adoção da tecnologia. Por estes motivos, optou-se pela utilização do sistema operacional Android.

O sistema operacional Android passou por diversas revisões desde o seu lançamento. Como a atualização do dispositivo móvel é de responsabilidade do fabricante deste dispositivo, muitos aparelhos não são atualizados. Assim, para manter a compatibilidade com um grande número de dispositivos, e poder fazer uso das versões mais novas da API do sistema, foi necessário estabelecer um limite mínimo de versão do sistema operacional. De acordo com dados disponibilizados pelo Google, (GOOGLE DASHBOARDS, 2013), mais de 90% dos dispositivos apresentam versão superior à 2.3.3. Assim, o protótipo desenvolvido deve suportar os dispositivos a partir desta versão.

A utilização do elemento seguro nos dispositivos móveis apresentou algumas limitações. Normalmente, a manutenção das aplicações presentes no *SE* é de responsabilidade da MNO (*Mobile Network Operator*) ou de uma terceira parte envolvida, chamada de TSM (*Trusted Service Manager*). Desta maneira, não é permitido ao desenvolvedor final realizar qualquer acesso ao elemento seguro sem a devida permissão de uma destas entidades, ou seja, é necessário o conhecimento da chave de acesso ao *SE*, para que seja possível instalar a aplicação desejada. Frente à impossibilidade de acesso ao elemento seguro, optou-se em desenvolver o protótipo Unipag utilizando a emulação do elemento seguro em software. As principais características do elemento seguro devem ser preservadas, como sistema de arquivos e permissões.

Para a geração e leitura de códigos QR, optou-se pela utilização de um aplicativo externo, desenvolvido pelo Google. Desta maneira, o desenvolvimento deste tipo de comunicação é facilitado. Esta forma de leitura de códigos QR é recomenda na API do Android. O leitor de cartões externo acoplado ao dispositivo móvel, utilizado no protótipo, permite apenas a leitura de cartões com tarja. Desta maneira, algumas transações podem ser

negadas pelo banco emissor do cartão, já que grande parte dos cartões emitidos no território nacional possui chip.

Com essas limitações em vista, a seguir são detalhados os requisitos de negócio e casos de uso do protótipo desenvolvido.

5.1 Requisitos de Negócio e Casos de Uso

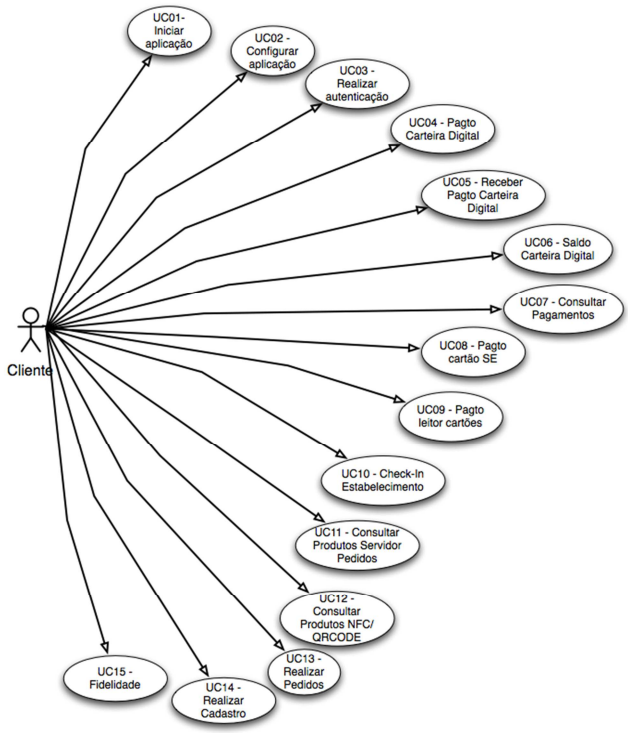
Os diversos requisitos da aplicação tem como base o modelo proposto a partir dos trabalhos relacionados, de acordo com a Tabela 7. Ao todo foram levantados treze requisitos de negócio, que levam aos casos de uso da aplicação, que são descritos na sequência. A Figura 16 resume os casos de uso do protótipo desenvolvido.

Tabela 7 Requisitos de negócio

Regra de negócio	Nome	Descrição
RN.01	Iniciar aplicação	Requisito necessário para iniciar a aplicação
RN.02	Configurar aplicação	Requisito necessário para permitir ao usuário configurar quais funcionalidades estarão disponíveis na aplicação.
RN.03	Realizar autenticação	Requisito necessário para efetuar a autenticação do usuário.
RN.04	Efetuar pagamento moedeiro eletrônico	Requisito necessário para que o usuário efetue o pagamento utilizando o moedeiro eletrônico.
RN.05	Receber pagamento moedeiro eletrônico digital	Requisito necessário para que o usuário receba o pagamento utilizando moedeiro eletrônico.
RN.06	Verificar Saldo moedeiro eletrônico/cartão pré pago/cartão presente	Requisito necessário para que o usuário consulte o saldo disponível em seu moedeiro eletrônico, cartão pré pago ou cartão presente.
RN.07	Verificar Pagamentos	Requisito necessário para que o usuário consulte o histórico de suas transações.
RN.08	Efetuar pagamento cartão cadastrado no elemento seguro	Requisito necessário para que o usuário efetue pagamento utilizando cartão cadastrado no elemento seguro
RN.09	Efetuar pagamento leitor cartões	Requisito necessário para que o usuário efetue pagamento utilizando um leitor de cartões acoplado ao dispositivo móvel
RN.10	Realizar *check-in* no estabelecimento	Requisito necessário para que o usuário efetue o *check-in* no estabelecimento e possa realizar os pedidos no servidor de pedidos.
RN.11	Consultar produtos no servidor de pedidos	Requisito necessário para a listagem e consulta de pedidos no servidor de pedidos do estabelecimento.
RN.12	Consultar produtos através de NFC/QR CODE	Requisito necessário para a consulta de produtos através de *tags* NFC ou códigos QR.
RN.13	Realizar pedido	Requisito necessário para efetuar o pedido de um produto.
RN.14	Cadastrar usuário	Requisito necessário para efetuar o cadastro de um usuário no sistema.
RN.15	Fidelidade	Requisito necessário para o cadastro de pontos no programa de fidelidade do estabelecimento.

Fonte: Elaborado pelo autor

Figura 16 Diagrama de Casos de Uso



Fonte: Elaborado pelo autor

5.1.1 Caso de uso UC.01 - iniciar aplicação

De acordo com o RN.01, este caso de uso é responsável por permitir ao usuário o acesso à aplicação. Na inicialização da aplicação, é importante verificar, caso exista conexão com a internet disponível, por versões novas da aplicação. Verificações iniciais da aplicação, como presença do elemento seguro e leitor de cartões também devem ser realizadas neste ponto, bem como configurar a aplicação de acordo com as preferências do usuário previamente cadastradas.

5.1.2 Caso de uso UC.02 - configurar aplicação

Este caso de uso é necessário para que o usuário configure suas preferências de utilização da aplicação. Ao selecionar esta opção, é exibida uma tela de configurações, permitindo ao usuário selecionar a utilização ou não de uma senha para efetuar as operações, modificar o usuário e a senha, selecionar quais métodos de pagamento serão utilizados (NFC, QR CODE ou ambos) e quais funcionalidades estarão disponíveis (pedidos, carteira digital e pagamento). O menu de configuração da aplicação está disponível no canto superior esquerdo da aplicação, em uma posição padrão para o sistema Android.

5.1.3 Caso de uso UC.03 - realizar autenticação

De acordo com o RN.03, este pré-requisito é necessário para efetuar a autenticação do usuário. Esta autenticação deve ser executada *online*, após o cadastro do usuário no sistema, ou em situações onde a aplicação é instalada em um novo dispositivo móvel. Após esta autenticação inicial, os posteriores acessos ao aplicativo irão necessitar de uma senha, que será validada de maneira *offline*.

5.1.4 Caso de uso UC.04 - efetuar pagamento carteira digital

De acordo com o RN.04, este pré-requisito é responsável por fornecer ao usuário o fluxo de pagamento através dos cartões presentes em sua carteira digital. Ao selecionar esta opção, os cartões cadastrados no elemento seguro são listados. O usuário deve informar o valor total da transação, e selecionar o meio que efetuará o pagamento (NFC ou QR CODE), de acordo com as suas preferências configuradas no UC.02. Por fim, o usuário deve efetuar a transação sem contato, aproximando os dispositivos envolvidos, ou utilizar os dispositivos para gerar e ler o QR CODE.

5.1.5 Caso de uso UC.05 - receber pagamento carteira digital

De acordo com o RN.05, este pré-requisito permite ao usuário receber um pagamento utilizando sua carteira digital, mais precisamente, seu moedeiro eletrônico. Ao selecionar esta opção, o usuário deve escolher o meio que será realizado o pagamento (NFC ou QR CODE) e interagir com o dispositivo móvel da fonte pagadora para efetuar o pagamento. A seleção do meio que será efetuada a transação se dá de acordo com as preferências do usuário, configuradas no UC.02.

5.1.6 Caso de uso UC.06 - consultar saldo carteira digital

De acordo com o RN.06, este caso de uso é responsável por fornecer ao usuário informações sobre o saldo disponível nos seus cartões cadastrados em sua carteira digital. Esta informação não está disponível para todos os tipos de cartões, já que não é possível consultar o saldo de um cartão de crédito ou débito sem estabelecer uma conexão com o banco emissor destes cartões. Desta maneira, esta informação está disponível apenas para cartões do tipo gift-card e pré-pagos, e também para o moedeiro eletrônico do usuário.

5.1.7 Caso de uso UC.07 - consultar pagamentos

De acordo com o RN.07, este caso de uso é responsável pela listagem das transações efetuadas pelo usuário. O armazenamento destas informações é facultativo, e o usuário pode desabilitar esta opção nas suas configurações. Um limite de armazenamento deve ser imposto, como por exemplo, todas as transações efetuadas no último mês. Uma opção,

disponibilizada no UC.02, deve permitir que o usuário apague todos os pagamentos realizados.

5.1.8 Caso de uso UC.08 - efetuar pagamento cartão cadastrado no elemento seguro

De acordo com o RN.08, este caso de uso é responsável pelo fluxo de pagamento através da utilização de um cartão cadastrado no elemento seguro. Neste caso de uso, o dispositivo móvel do usuário irá se comportar como um ponto de pagamento. Ao selecionar esta opção, o dispositivo móvel deverá verificar se existe um leitor de cartões compatível conectado ao dispositivo, e então solicitar ao usuário que insira ou passe o cartão.

5.1.9 Caso de uso UC.09 - efetuar pagamento leitor cartões

De acordo com o RN.09, este caso de uso é responsável pelo fluxo de pagamento através da utilização de um cartão cadastrado no elemento seguro. Neste caso de uso, o dispositivo móvel do usuário irá se comportar como um ponto de pagamento. Ao selecionar esta opção, o dispositivo móvel deverá verificar se existe um leitor de cartões compatível conectado ao dispositivo, e então solicitar ao usuário que insira ou passe o cartão.

5.1.10 Caso de uso UC.10 - realizar *check-in* no estabelecimento

De acordo com o RN.09, este caso de uso é responsável por permitir ao usuário realizar um *check-in* no estabelecimento comercial em que se encontra. Assim, o usuário passa a ter acesso ao servidor de pedidos disponível na rede interna, e pode efetuar pedidos e pagamentos diretamente em seu dispositivo móvel. Para realizar o *check-in*, o usuário deve ter sua conta no aplicativo Foursquare [3]vinculada à aplicação Unipag. Após a operação de *check-in*, é realizada uma consulta do estabelecimento na base Unipag. Caso o estabelecimento possua cadastro, o sistema retorna ao terminal os dados para conexão ao servidor de pedidos do estabelecimento.

5.1.11 Caso de uso UC.11 - consultar produtos no servidor de pedidos

De acordo com o RN.11 este caso de uso permite ao usuário acessar o servidor de pedidos do estabelecimento comercial, e a partir das informações retornadas pelo servidor (UC.09), efetuar suas compras diretamente no seu dispositivo móvel. O servidor poderá retornar os pedidos divididos em categorias, junto com uma descrição do produto e seu valor. Após a consulta do produto, o usuário poderá efetuar o pedido, de acordo com o UC.13.

[3] www.foursquare.com

5.1.12 Caso de uso UC.12 - Consultar produtos através de NFC/QR CODE

De acordo com o RN.12, este caso de uso permite ao usuário acessar as informações dos produtos através da leitura de uma *tag* NFC ou um código QR disponível no estabelecimento comercial. Após a leitura desta informação, o dispositivo móvel irá exibir uma descrição do produto, e o usuário poderá realizar seu pedido através da comunicação com o servidor de pedidos. Após a consulta do produto, o usuário poderá efetuar o pedido, de acordo com o UC.11.

5.1.13 Caso de uso UC.13 - realizar pedido

De acordo com o RN.13, este caso de uso permite ao usuário realizar o pedido de um produto diretamente no seu dispositivo móvel, através da comunicação com o servidor de pedidos. Este produto pode ser lido através de uma consulta ao servidor de pedidos ou através da leitura de uma *tag* NFC ou QR CODE. Após realizar o pedido, o usuário poderá efetuar o pagamento, através de sua carteira digital (UC.04) ou de leitor acoplado ao dispositivo (UC.08).

5.1.14 Caso de uso UC. 14 - cadastrar usuário

De acordo com o RN.14, este caso de uso permite ao usuário realizar o seu cadastro e iniciar o uso da aplicação Unipag. O usuário deve preencher os dados diretamente no dispositivo móvel, e confirmar o cadastro através de um código, enviado por email.

5.1.15 Caso de uso UC.15 - fidelidade

De acordo com o RN.15, este caso de uso permite ao usuário a participação no programa de fidelidade do estabelecimento comercial em que se encontra.

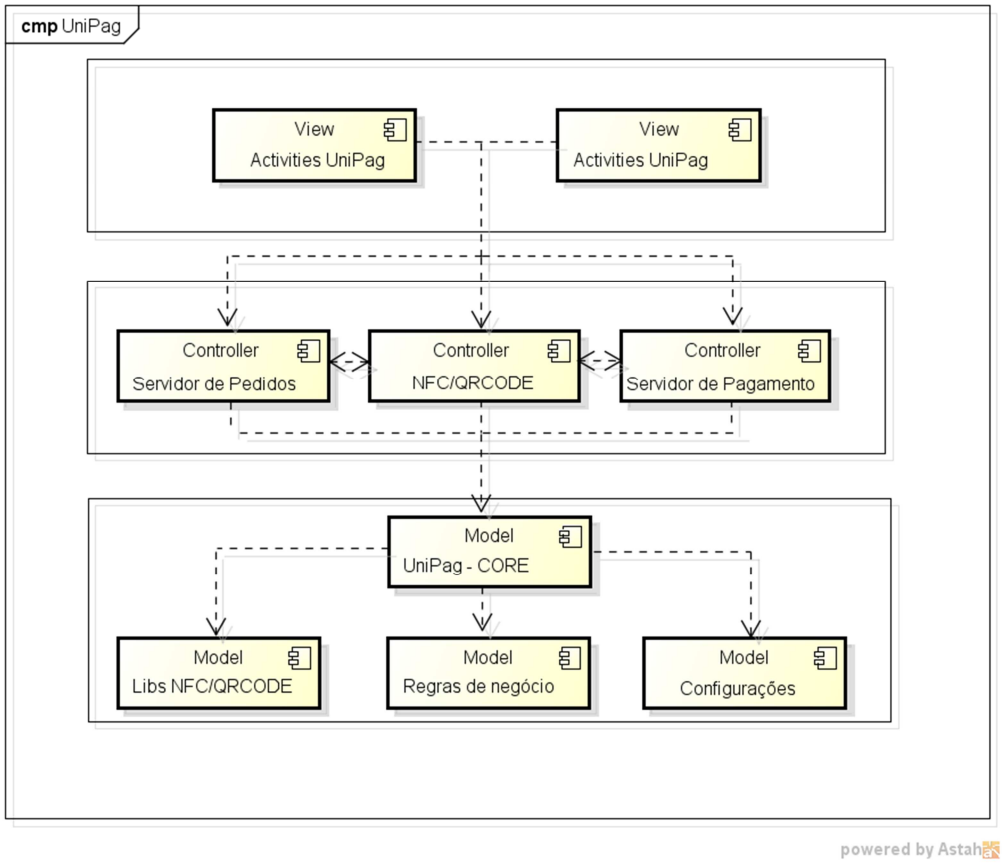
5.2 Modelagem dos componentes

Para modelagem dos componentes, optou-se pela utilização do padrão de arquitetura *Model-View-Controller* (MVC) (REENSKAUG, 1979). O padrão MVC é amplamente utilizado no desenvolvimento de aplicativos, e permite a divisão do projeto em camadas de negócio (*model*), interface com usuário (*view*) e controle (*controller*).

O diagrama de componentes (Figura 17) apresenta na camada de interface com o usuários as *Activities* (telas), responsáveis pelas diversas telas de interface com o usuário e interação com a camada de servidor de pedidos, servidor de pagamento e comunicação (camada *mode*l*)* via NFC, QR CODE ou leitor de cartões externo. A camada *Model* apresenta as regras de negócio, como por exemplo, mensagens ISO e criptografia, configurações do usuário e bibliotecas de acesso aos módulos NFC, QR CODE e leitor de cartões. Diversas

activities da camada *View* são compartilhadas entre as diversas funcionalidades do sistema, como as telas de seleção do meio de pagamento (NFC ou QR CODE), que é apresentada quando o usuário deseja efetuar um pagamento e possuir as duas opções selecionadas em suas configurações. Outra tela compartilhada entre os módulos é a tela de entrada de valor. A seguir, são apresentadas as tecnologias que foram empregadas na implementação do protótipo.

Figura 17 Diagrama de componentes



Fonte: Elaborado pelo autor

5.3 Tecnologias utilizadas

Existem diversas alternativas para o desenvolvimento de software para a plataforma Android. A solução mais utilizada pela comunidade de desenvolvedores, e fortemente sugerida pelo Google, é a utilização de uma versão modificada da ferramenta de desenvolvimento Eclipse[4]. Esta versão possui uma ferramenta que permite ao usuário selecionar quais versões do sistema operacional móvel ele irá desenvolver, além de diversas outras ferramentas disponibilizadas pelo Google.

[4] www.eclipse.org

O desenvolvimento das aplicações Android é realizado através da linguagem Java, o que permite a utilização de uma série de bibliotecas já disponibilizadas atualmente nesta linguagem. Para manter a compatibilidade com o maior número possível de dispositivos, optou-se pela utilização da versão 10 (GINGERBREAD_MR1) como versão mínima da API.

Entre as diversas ferramentas disponibilizadas pelo SDK está um emulador do sistema operacional Android. Este emulador permite a emulação de praticamente todas as funcionalidades disponibilizadas pela API do sistema operacional. Até mesmo o hardware NFC pode ser simulado, através do envio de *intents*. *Intents* são mensagens enviadas por uma aplicação para o sistema operacional, que permite inicializar um componente interno da aplicação ou mesmo em outra aplicação, permitindo que duas aplicações compartilhem funcionalidades. O emulador permite executar a aplicação em qualquer uma das versões disponibilizadas do sistema operacional, simulando diferentes resoluções e quantidades de memória disponíveis.

Além do emulador disponibilizado pelo SDK, foram realizados testes em um dispositivo real. O modelo escolhido foi o Samsung Galaxy X, versão nacional do celular Galaxy Nexus americano. Este dispositivo foi lançado pelo Google em parceria com a Samsung, o que garante constante atualização para a versão mais recente do sistema operacional. Ele possui um display de 4.65 polegadas, 1 GB de RAM e armazenamento interno de 16 GB, além de dispor de hardware necessário para comunicação NFC. Este dispositivo está atualizado com a última versão do sistema operacional disponibilizado pelo Google (API LEVEL 17 - JELLY_BEAN_MR1).

A aplicação Unipag, portanto, foi desenvolvida utilizando o SDK do Android em conjunto com a IDE (*Integrated Development Environment*) Eclipse. Como os dispositivos móveis com sistema operacional Android podem ser customizados de fabricante para fabricante, a IDE permite a utilização de diversos tipos de configurações para testar a aplicação. Isto inclui configurações como tamanho da tela (de 3.5 polegadas até 10.1 polegadas), memória RAM, armazenamento interno e presença de teclado físico. Optou-se utilizar para o desenvolvimento, um iMac com processador i5 e com 4GB de RAM.

Para a implementação do projeto foi utilizado o processo de desenvolvimento de software RUP (*Rational Unified Process* ou Processo Unificado Racional), que tem como abordagem a orientação a objetos em sua concepção e é projetado e documentado utilizando a

notação UML (*Unified Modeling Language*) para ilustrar os processos (IBM, 2013). Este processo tem como características quatro etapas bem definidas:

- **Concepção**: Onde é definido o escopo do sistema e são desenvolvidos os casos de uso;
- **Elaboração**: Complementa o levantamento e documentação dos casos de uso e revisa a modelagem do sistema;
- **Construção**: Desenvolvimento e testes do produto desenvolvido;
- **Transição**: Entrega do software desenvolvido. Treinamento do usuário final.

Para o desenvolvimento destas quatro etapas foram utilizados diversos softwares, descritos na Tabela 8.

Tabela 8 Processo de desenvolvimento RUP

Fase	Descrição	Artefatos	Ferramentas
Concepção	Levantamento dos requisitos de software e seleção dos cenários de utilização	Diagrama de casos de uso dos cenários	Astah Community versão 6.7.0 OmniGraffle 5.4.2
Elaboração	Documentação e geração da análise do sistema	Diagrama dos componentes	
		Diagrama de classes	
Construção	Construção do protótipo	Desenvolvimento do servidor de comunicação do servidor de pedidos Unipag	Eclipse com suporte à JSON[5]/REST
Transição	Disponibilização do software nas camadas cliente e servidor	Deploy do servidor de comunicação. Instalação do aplicativo no emulador Android e dispositivos compatíveis	Servidor de aplicações Apache Tomcat. Eclipse ADT Bundle Samsung Galaxy X

Fonte: Elaborado pelo autor

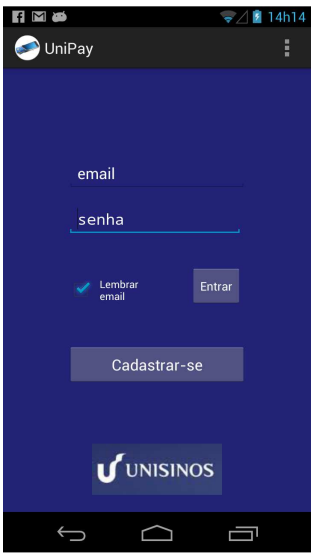
[5] http://www.json.org/

Com as definições de processo de desenvolvimento a ser utilizado, bem comoferramentas necessárias, iniciou-se o desenvolvimento da interface do protótipo.

5.4 interface

A Figura 18 apresenta a tela inicial da aplicação. Ela permite que o usuário efetue o cadastro no serviço Unipag, através do preenchimento de algumas informações pessoais, como email e CPF, entre outras. O usuário será reconhecido no sistema através do seu email pessoal. As telas de interface foram capturadas a partir do dispositivo móvel. Com o *login* efetuado, o usuário poderá acessar as configurações da aplicação. Dentre as configurações disponíveis, está a solicitação ou não de senha para utilizar o módulo de carteira digital. O uso de uma senha é importante, pois na carteira digital encontram-se os cartões cadastrados pelo usuário. Também é possível modificar a senha escolhida anteriormente.

Figura 18 Tela inicial da aplicação Unipag



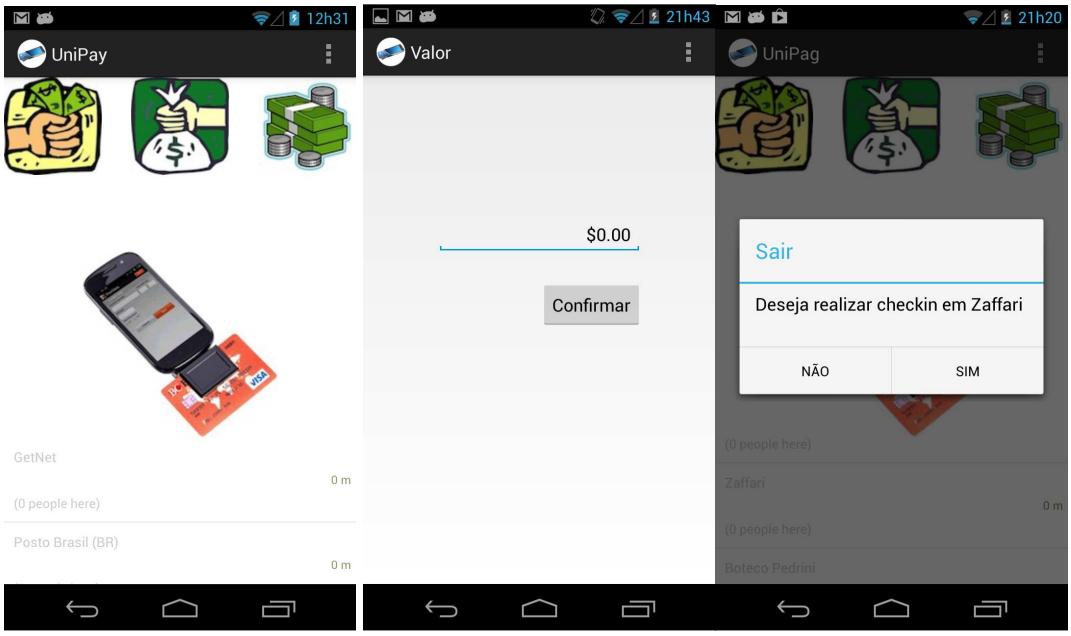
Fonte: Elaborado pelo autor

Os métodos de pagamento disponíveis na utilização de carteira digital também são configurados. Assim, é possível desabilitar a tela de escolhe de meio de pagamento que ocorre em cada uma das transações, selecionando então o meio de pagamento padrão da aplicação. Caso o dispositivo móvel não possua o hardware NFC, a aplicação irá configurar automaticamente o meio de pagamento QR CODE. Por fim, as funcionalidades disponíveis ao usuário podem ser configuradas. Caso ele não vá fazer uso do módulo carteira digital e pagamento, o usuário poderá selecionar apenas a opção de utilização do servidor de pedidos.

O acesso às funcionalidades da aplicação é disponibilizado após o *login* do usuário. A tela lista todas as funcionalidades selecionadas pelo usuário. Na Figura 19a é exibida a tela para o caso que o usuário possui todas as opções selecionadas (módulo financeiro e módulo comercial). A parte central da Figura 19b apresenta a conexão da aplicação com o hardware responsável pela leitura de cartões. Ao selecionar esta opção, o dispositivo irá realizar uma comunicação com o leitor. Caso esteja presente, a mensagem “Passe o cartão na leitora” será exibida. Com o sucesso da leitura, a aplicação irá exibir o nome do usuário, retirado de uma das trilhas magnéticas lidas pelo cartão ou presente no chip, e exibir os quatro últimos dígitos do cartão, respeitando as regras de segurança de transações eletrônicas, que não permitem que o número seja exibido por completo.

Na parte inferior da tela principal, são exibidos os locais perto do usuário onde é possível realizar o *check-in*. Ao selecionar um dos locais, é exibida uma mensagem solicitando a confirmação do *check-in*, conforme a Figura 19c.

Figura 19 Telas da aplicação UniPag

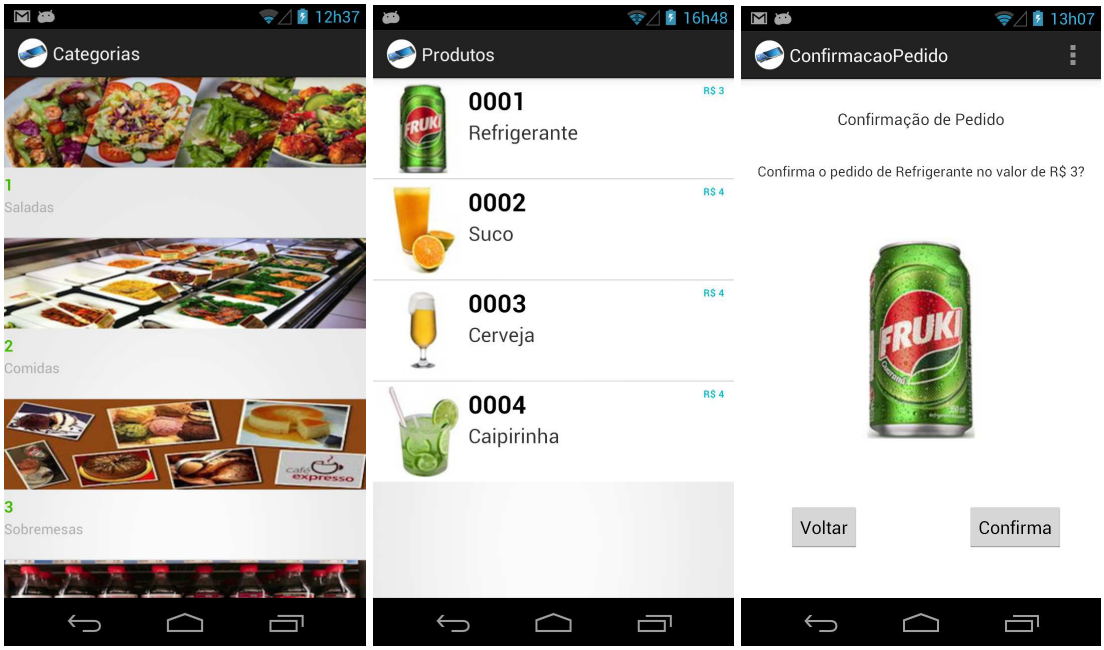


(a) (b) (c)

Fonte: Elaborado pelo autor

A interação do protótipo Unipag com o servidor de pedidos, disponível após a realização de check-in no estabelecimento comercial, possui 3 etapas. Primeiramente, uma consulta é realizada, retornando as categorias de produtos disponíveis no estabelecimento, conforme Figura 20a. Ao selecionar uma das categorias, uma nova consulta é realizada, retornando os produtos cadastrados nesta categoria, conforme Figura 20b. Com a seleção do produto, uma tela de confirmação do pedido é exibida, de acordo com Figura 20c.

Figura 20 (a) Seleção de categorias (b) Seleção de produtos (c) Confirmação de pedido



Fonte: Elaborado pelo autor

O desenvolvimento das diversas classes que comandam o comportamento e fluxo das telas exibidas anteriormente é descrito a seguir.

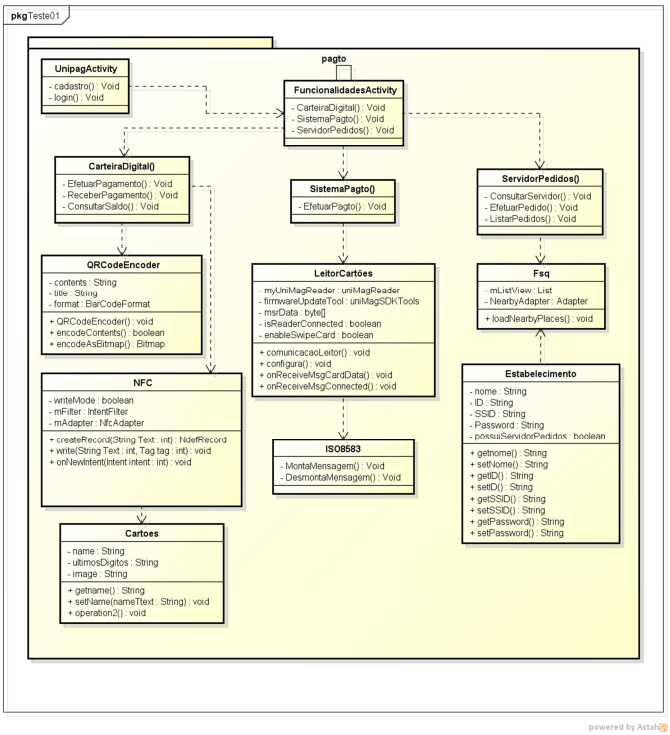
5.5 Classes Desenvolvidas

A Figura 21 apresenta as principais classes desenvolvidas para a aplicação.

- **NFC:** Responsável pelos métodos de leitura e escrita de *tags* NFC;
- **QRCodeEnconder:** Geração e leitura de códigos QR;
- **LeitorCartões:** Realiza a interface com o leitor de cartões externo;
- **ISO8583:** Responsável pela criação da mensagem no formato ISO;
- **Fsq:** classe responsável pela comunicação com a API V2 do Foursquare. A API utiliza conexão com servidores REST, e retorna os dados em JSON (JSON, 2013);
- **Cartões:** Classe responsável pelo armazenamento temporário das informações do cartão do usuário;
- **CarteiraDigital:** Classe que implementa os métodos de pagamento disponibilizados pela aplicação;
- **ServidorPedidos:** Responsável pela comunicação com o servidor de pedidos do estabelecimento

- **SistemaPagto:** Realiza a interface com o sistema de pagamento externa, quando o aplicativo é utilizado em conjunto com um leitor de cartões externo.

Figura 21 Principais classes do sistema a Unipag



Fonte: Elaborado pelo autor

O desenvolvimento dos quatro módulos da aplicação, que fazem uso das classes listadas na Figura 21, é descrito na sequência.

5.6 Implementação do Módulo Comercial

A interface com o servidor de pedidos permite ao usuário visualizar os itens disponíveis no estabelecimento e realizar o pedido diretamente no seu dispositivo móvel. A comunicação com o servidor de pedidos é realizada através dos dados recebidos no momento do *check-in* do usuário no estabelecimento. A partir deste ponto, o usuário irá ser conectado e autenticado automaticamente ao WiFi disponibilizado pelo ponto comercial, e será conectado ao endereço local do servidor de pedidos.

A listagem dos estabelecimentos comerciais foi realizada através da API da aplicação Foursquare. A aplicação permite a listagem de estabelecimentos comerciais de acordo com a localização do usuário. A API permite a consulta de pontos cadastrados através de requisições de Web Services REST, e retorna os pontos comerciais no padrão JSON.

Cada estabelecimento retornado possui um número de cadastro único. Este número é utilizado pela aplicação para a consulta da existência de um servidor de pedidos através do

servidor Unipag. Em caso positivo, os dados de acesso à rede Wifi são retornados. Com o acesso ao servidor de pedidos realizado, as categorias de produtos disponíveis são exibidas. Estas categorias podem ser configuradas de acordo com o tipo de estabelecimento. Após a seleção da categoria, os produtos correspondentes são exibidos, junto com informações descritivas e preço do item. Por fim, uma tela solicitando a confirmação do pedido é exibida. Para ilustrar a estrutura de uma requisição de produtos ao WS, um exemplo é exibido na Figura 22, em formato JSON.

Figura 22 Exemplo de Json para categorias e produtos

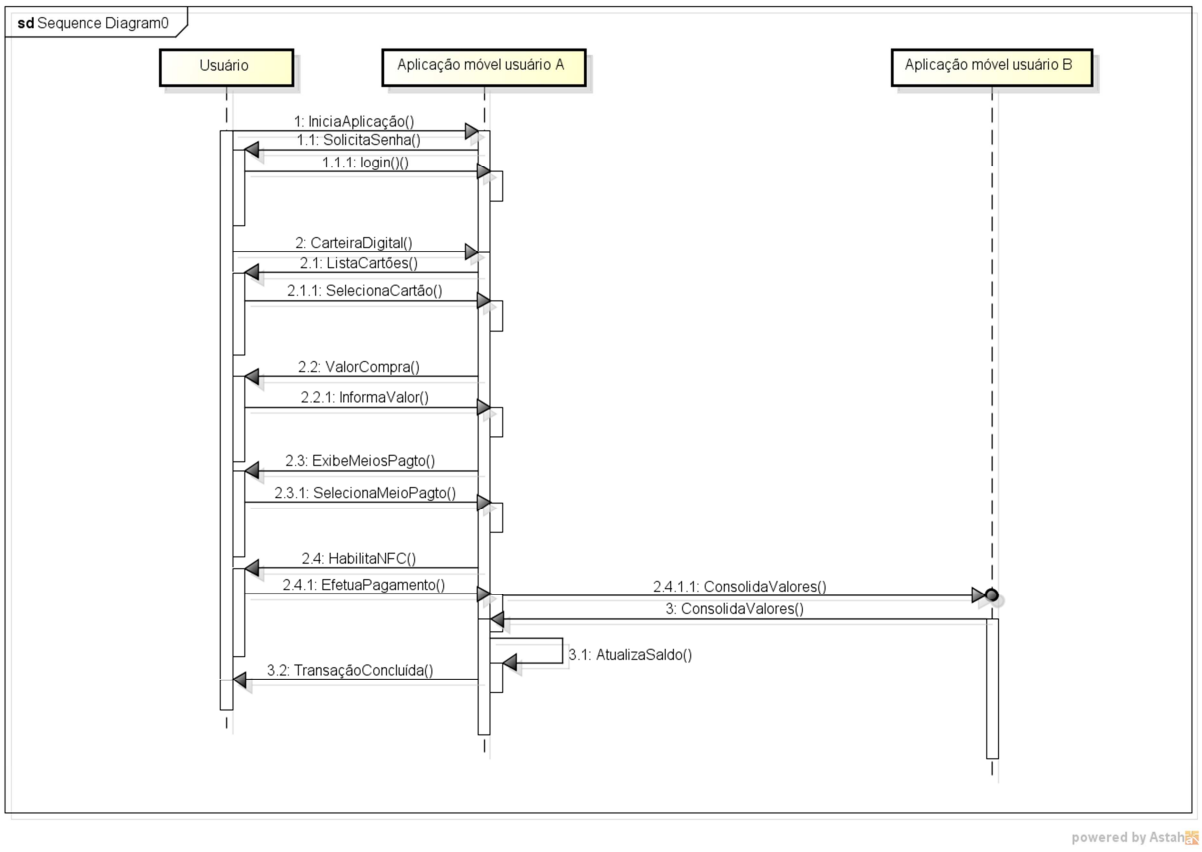
Fonte: Elaborado pelo autor

5.7 Implementação do Módulo Financeiro

A transferência de fundos através do moedeiro eletrônico foi implementada através da emulação do elemento seguro. A interação com diferentes moedeiros eletrônicos (outros usuários do sistema) foi emulada através da utilização de *tags* NFC, compradas através da internet[6]. Em algumas *tags*, foram gravados diferentes valores para a simulação do pagamento utilizando moedeiro eletrônico. Já em outras *tags*, foram gravados valores simulando o recebimento de um pagamento.

O fluxo de uma transação de pagamento utilizando o moedeiro eletrônico é apresentado na Figura 23. São exibidas as opções de pagamento (QR CODE ou NFC), de acordo com as preferências do usuário. O fluxo possui três participantes: o usuário A, responsável pela iniciativa de pagamento; a aplicação móvel do usuário A e a aplicação móvel do usuário B. Para simplificar, foram omitidas as diversas interações do usuário B com seu aplicativo móvel, já que elas são similares às ações realizadas pelo usuário A.

Figura 23 Fluxo pagamento móvel com carteira digita



Fonte: Elaborado pelo autor

[6] www.tagstand.com

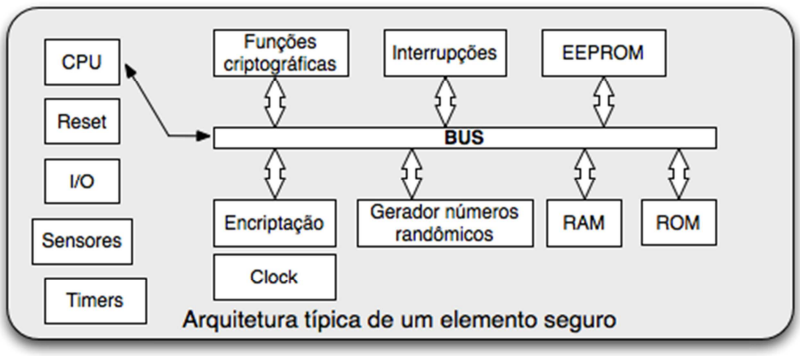
O fluxo de um pagamento utilizando um dos cartões cadastrados na carteira digital pôde ser simulado em conjunto com um terminal POS. O fluxo transacional do terminal de vendas deve solicitar a aproximação do dispositivo móvel para a leitura do cartão, e então comunicar-se com o sistema de pagamento através de uma mensagem ISO. Ao efetuar uma transação com o leitor externo de cartões, a mensagem segue o fluxo da Figura 12, sendo enviada primeiro para o sistema de captura de transações, onde são validadas as informações do estabelecimento, e então enviadas para a instituição financeira, onde informações como dados de cadastro do usuário e saldo são verificadas. Neste caso, uma conexão com a internet é requerida, já que é necessária a comunicação do dispositivo móvel com o servidor de pagamentos.

5.8 Implementação da Carteira digital

Conforme descrito no capítulo 2.3.1, a utilização de um elemento seguro é parte essencial para a segurança da solução de carteira digital. Este elemento seguro pode ser implementado no dispositivo móvel de diferentes maneiras. Não é permitido ao desenvolvedor final realizar qualquer acesso ao elemento seguro sem a devida permissão de uma destas entidades, ou seja, é necessário o conhecimento da chave de acesso ao *SE*, para que seja possível instalar a aplicação desejada.

Frente à impossibilidade de acesso ao elemento seguro, optou-se em desenvolver o protótipo Unipag utilizando a emulação do elemento seguro em software. As principais características do elemento seguro devem ser preservadas, como sistema de arquivos e permissões. A Figura 24 apresenta a arquitetura típica de um elemento seguro. A emulação do elemento seguro armazena as chaves em um arquivo. Esta chave não estará disponível para demais aplicações que estejam executando no dispositivo móvel. Isto é possível no sistema Android, já que cada aplicação possui permissões para leitura e escrita restritas ao diretório em que está instalado.

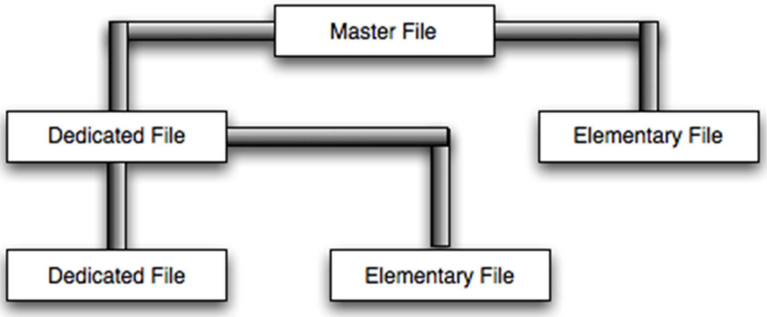
Figura 24 Arquitetura de um elemento seguro



Fonte: Baseado em Smart Card Alliance, 2013.

O sistema de arquivos do elemento seguro(e de um *smartcard* em geral) é organizada de acordo com a Figura 25. Todo sistema inicia com um MF (*Master File*), que seria o equivalente a um diretório raiz do sistema. Em um MF, existem diversos DF (*Dedicated Files*) e EF (*Elementary Files*). Um DF é o equivalente a um diretório, sendo um EF um arquivo dentro do diretório. Desta maneira, o diretório A pode ser responsável pelo armazenamento dos cartões cadastrados na carteira digital do usuário, sendo cada cartão um arquivo. Um diretório B pode armazenar os dados de uma aplicação responsável pelos *tickets* de transporte público. A aplicação deve implementar um sistema similar para o armazenamento das informações.

Figura 25 Sistema de arquivos do elemento seguro



Fonte: Baseado em Smart Card Alliance, 2013.

5.9 Implementação do Módulo de Comunicação

O leitor de cartões externo utilizado para o protótipo foi o IDTech[7]. Ele é conectado através da entrada de áudio do dispositivo móvel. Uma biblioteca é disponibilizada pelo fabricante para utilização do dispositivo, permitindo a leitura das trilhas do cartão. A trilha

[7] http://www.idtechproducts.com/

lida é então formatada dentro do campo correspondente da mensagem ISO e enviada ao sistema de pagamento.

A comunicação utilizando NFC é disponibilizada através da API do próprio sistema operacional. Para os dispositivos Android, esta API está disponível a partir da versão 2.3.3, tornando possível a comunicação com diferentes tipos de *tags*. Também permite a leitura de diferentes tipos de cartões além do padrão NFC, tais como cartões MIFARE[8] e ISO 1443, bastante utilizados em sistemas de bilhetagem eletrônica, além de métodos para leitura e escrita de mensagens NDEF, o formato padrão para transmissão de dados entre dispositivos e *tags*.

Para a leitura de QR CODES, é possível utilizar alguma biblioteca *open source*, como, por exemplo, Zxinglib (2012), que permite a decodificação de códigos QR, e encontra-se disponível para Android e IOS. A mesma biblioteca permite a criação de QR CODES. A comunicação entre o dispositivo móvel e o servidor de pedidos foi implementada através de Web Services, utilizando o padrão REST. Para o envio de dados (lista de produtos e solicitação do pedido) foi escolhido o padrão JSON (JSON, 2013).

A avaliação dos módulos desenvolvidos para o ptotótipo, através de metodologias como utilização de cenários e avaliação de usabilidade, é descrita no capítulo 6.

[8] http://www.mifare.net/

6 AVALIAÇÃO

Para a avaliação do modelo foram utilizadas duas metodologias. Primeiramente, o sistema foi avaliado através de cenários, que simulam o comportamento real da aplicação. Posteriormente, o protótipo passou por uma avaliação de usabilidade, sendo utilizado e analisado por usuários reais.

6.1 Avaliação por cenários

Como primeira análise, foi utilizada a avaliação baseada em cenários. Este modelo de avaliação tem sido utilizado pela comunidade acadêmico-científica para validar projeto em ambientes sensíveis ao contexto, conforme (DEY, 2001), e em ambientes ubíquos, de acordo com (SATYANARAYANAN, 2001; SATYANARAYANAN, 2011). A avaliação por cenários também tem sido utilizada para a análise de aplicativos móveis (DE SÁ, 2008).

6.1.1 Metodologia

Uma das metodologias utilizadas para avaliação do protótipo desenvolvido é a utilização de uma avaliação por cenários. Os cenários foram desenvolvidos com dois objetivos:

- **Testes de todas as funcionalidades da aplicação:** Os cenários devem avaliar o funcionamento de todos os módulos citados no Capítulo 5 (comercial, financeiro, carteira digital e comunicação);
- **Abranger principais métodos de pagamento utilizados pelo usuário:** Os cenários devem contemplar os métodos de pagamento utilizados pelo usuário no seu dia a dia.

Para execução dos cenários, foram utilizados dispositivos reais. Os modelos de celulares usados foram Galaxy X e Galaxy S3, ambos da Samsung, Todos os cenários foram executados em sequência. Ao término da execução, os testes foram repetidos, com o objetivo de realizar testes de execução contínua da aplicação. Foram utilizadas *tags* NFC e programas geradores de códigos QR. Para a execução dos cenários, optou-se pela utilização da infraestrutura de internet disponível no local dos testes.

6.1.2 Cenários propostos

Nesta subseção são apresentados alguns cenários de casos de teste possíveis para avaliar a utilização sistema, os quais avaliam as principais características que o sistema tem por objetivo atender.

(1) Cenário 1 - Pagamento com moedeiro eletrônico

Neste cenário, pretende-se demonstrar a utilização do protótipo para efetuar um pagamento entre dois usuários da aplicação, através da utilização do moedeiro eletrônico, presente no módulo carteira digital. A seguir, é descrito um possível cenário de aplicação do modelo:

"João e Márcio são amigos. Em uma visita à casa de João, Márcio verifica que este possui alguns itens que deseja se desfazer. Como não estava preparado, Márcio não possui dinheiro em sua carteira, e tão pouco utiliza cheques há algum tempo. Os dois amigos possuem um smartphone equipado com a aplicação Unipag e resolvem realizar a transação. Márcio seleciona a opção para pagamento, mais precisamente a opção de moedeiro eletrônico, e João seleciona a opção para receber o pagamento. Após aproximarem os dispositivos, a transação é efetuada com sucesso."

A transação é efetuada sem nenhuma necessidade de conexão à internet, usando a interface NFC dos equipamentos. Caso um dos equipamentos não possuísse NFC, o pagamento também poderia ter ocorrido com QR CODES. O cenário funcionou conforme esperado, apresentando os saldos corretos após a transferência de valores. A Figura 26 apresenta a tela de pagamento com QR CODE.

Figura 26 Pagamento com QR CODE

Fonte: Elaborado pelo autor

(2) Cenário 2 – Pagamento com cartão presente na carteira digital

Neste cenário, pretende-se demonstrar a utilização do protótipo para efetuar um pagamento entre um usuário da aplicação que possua algum cartão de crédito cadastrado no seu módulo de carteira digital. O dispositivo móvel do usuário irá se comunicar com o terminal de ponto de vendas (POS ou PINPAD). Este terminal deverá ter capacidade de efetuar transações sem contato (*contactless*).

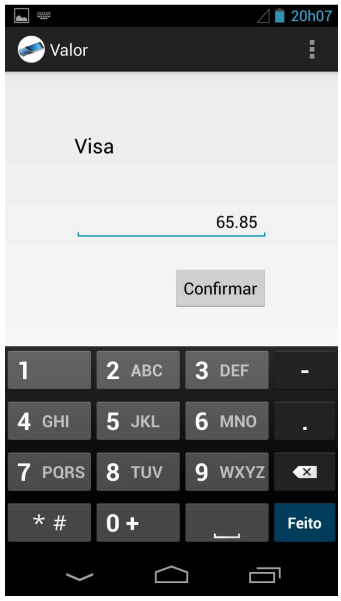
As transações efetuadas nesta modalidade podem ser efetuadas de maneira *offline*, caso o valor total da transação não passe de um limite, chamado pelas empresas adquirentes de *floor limit*. Neste caso, o terminal armazena as transações até que um determinado valor seja efetuado, e então envia as

transações para o sistema autorizador. Nessa situação há o risco da transação ser negada posteriormente por falta de saldo ou crédito. Por definição das bandeiras, o valor limite é de 50 unidades de moeda local. Caso o valor da transação seja superior ao *floor limit*, esta transação é realizada *online*. Atualmente, os sistemas que implementam o pagamento sem contato utilizam *floor limit* igual a zero, forçando todas as transações a serem *online*. A seguir é descrito um cenário hipotético para esta funcionalidade:

"Mario está na fila para o almoço em uma rede de fast food. Após todos escolherem seus lanches, o pedido é finalizado em R$ 68,43. Ao aproximar-se do caixa para efetuar o pagamento, a atendente solicita que Mario insira seu cartão de crédito. Como possui um dispositivo móvel equipado com NFC, e possui seu cartão cadastrado em sua carteira digital, ele executa a aplicação e seleciona seu cartão. Como a transação teve um valor superior às 50 unidades de moeda local, ela é enviada ao sistema de pagamento e aprovada de maneira online."

Para o usuário, esta conexão *online* é quase imperceptível, já que uma transação financeira realizada neste tipo de estabelecimento geralmente é muito rápida, devido ao tipo de comunicação utilizado (geralmente X25 ou *Ethernet*). A Figura 27 apresenta a tela de entrada de valor da compra, após a seleção do cartão a ser utilizado.

Figura 27 Pagamento com cartão de crédito



Fonte: Elaborado pelo autor

(3) Cenário 3 – Pedidos através de cardápio com NFC/QR CODE

Este cenário tem como objetivo demonstrar a utilização do módulo comercial da aplicação, através da utilização de um cardápio equipado com *tags* NFC e QR CODEs. Um cenário hipotético de utilização é descrito a seguir:

"João está de férias passeando na Serra Gaúcha. Por volta das 13:00, ele decide almoçar no restaurante A Cantina. Ao chegar ao restaurante, tem uma surpresa: nenhum garçom vai ao seu encontro para atendê-lo. Ao sentar-se,

verifica que todo o cardápio está disponível diretamente na mesa, na forma de QR CODES. No canto da mesa, João encontra uma tag com o texto Check-in /Checkout. Ao aproximar seu smartphone, equipado com leitor NFC e executando o sistema operacional Android, o usuário é adicionado automaticamente à rede Wifi do restaurante. Como é a primeira vez que utiliza o sistema, o usuário é direcionado para a loja de aplicativos do seu celular, para que o download da aplicação seja realizado. A partir deste momento, João consulta o cardápio apenas lendo os QR CODES existentes em sua mesa. João então captura o QR CODE que está associado ao prato Pizza Margherita. Imediatamente uma foto do prato aparece em seu smartphone. João então confirma a escolha tocando no botão correspondente na tela do celular. Isso faz com que o pedido seja enviado via Wifi, cuja conexão foi estabelecida no momento do check-in, para o servidor do restaurante, que encaminha a solicitação do prato a cozinha. Em seguida, João captura o QR Code que está ao lado do item Taça de Vinho Tinto. Novamente, a imagem aparece em seu telefone celular e ele pressiona o botão confirma. A informação é enviada através da rede Wifi. Após alguns instantes, aparece um garçom carregando uma bandeja com a taça de vinho. Ao terminar a refeição, João aproxima novamente seu telefone da tag NFC Check-in /Checkout, e visualiza na tela do smartphone o detalhamento dos pedidos, o valor total dos gastos, junto com as opções de pagamento. Utilizando o valor disponível no seu moedeiro eletrônico, João efetua o pagamento da refeição."

Este cenário permite uma interação entre o cliente e o estabelecimento comercial, através da consulta e realização de pedidos diretamente no *smartphone*. Pode facilitar a disponibilização de um cardápio em diversas línguas, facilitando a comunicação com o usuário final. Também permite que o usuário utilize a internet do estabelecimento após o *check-in*. Opcionalmente, a realização do pedido através da aplicação pode vir acompanhada de um acompanhamento do tempo de entrega, possibilitando que o usuário saiba quando receberá seu pedido. A simulação do cenário, com a construção de um cardápio contendo *tags* e QR CODES para pedidos de produtos, foi executada com sucesso.

(4) Cenário 4 – Consulta ao servidor de pedidos

Este cenário tem como objetivo demonstrar a utilização do módulo comercial para realizar um pedido de um determinado produto através da consulta ao servidor de pedidos do estabelecimento. Um cenário hipotético é descrito a seguir:

"João está realizando compras em um shopping center. Ao entrar em uma grande loja de departamentos, ele recebe automaticamente um convite para realizar o check-in no estabelecimento. Isto é possível pois a loja possui uma série de tags NFC ativas instaladas na sua entrada. Ao realizar o check-in ele automaticamente recebe a chave de acesso à rede WiFi do estabelecimento comercial e passa a utilizá-la para navegar. Ao invés de percorrer os diversos andares da loja, João consulta os produtos e realiza seu pedido diretamente no seu dispositivo. Ao dirigir-se para a fila de pagamento, é atendido por uma funcionária, que utiliza o módulo financeiro da aplicação Unipag para efetuar o pagamento."

Este cenário permite automatizar os pedidos do estabelecimento comercial, ao mesmo tempo em que permite uma aproximação do usuário com todos os produtos disponibilizados na loja. O pagamento através da aplicação permite que o usuário não enfrente filas, diminuindo seu tempo de permanência e contribuindo para o aceite da solução. O cenário foi simulado com sucesso, com a consulta ao *Webservice* retornando as categorias e pedidos e o pedido sendo efetuado.

(5) Pagamento com cartão através de leitor de cartões externo

O objetivo deste cenário é demonstrar a utilização do protótipo Unipag para efetuar um pagamento através de um leitor de cartões acoplado ao dispositivo móvel do usuário, conforme exibido na Figura 28.

Um cenário hipotético é descrito a seguir:

"Marcos está em um almoço com a família. Ao término do almoço, solicita ao garçom a conta. Há uma fila formada para pagamento direto no caixa, e todos os terminais de pagamento disponíveis no estabelecimento estão sendo utilizados. O ponto comercial possui a solução Unipag, assim como Marcos. O garçom então acopla um leitor de cartões na saída de áudio do dispositivo móvel de Marcos, que o utiliza para efetuar o pagamento com seu cartão de crédito."

O estabelecimento comercial evitou a formação de filas, permitindo uma maior circulação de clientes, além de economizar dinheiro com o aluguel de máquinas extras para as transações com cartão. O cliente fica satisfeito, pois o processo de pagamento foi agilizado.

Figura 28 Leitor de cartões externo conectado ao dispositivo móvel

Fonte: Elaborado pelo autor

6.1.3 Discussão dos resultados

As execuções dos cenários foram realizadas com sucesso, conforme as descrições dos cenários, sem a ocorrência de imprevistos. Todos os cenários foram executados duas vezes, e a aplicação não apresentou nenhuma instabilidade ou demora na execução.

No primeiro cenário, ocorreu o pagamento entre dois usuários da aplicação Unipag, em uma transação eletrônica do tipo P2P. Neste cenário, não houve a necessidade de conexão à internet. A troca das informações da transação foi executada através da tecnologia NFC. A quantia recebida na transação pôde ser prontamente utilizada para um novo pagamento. Além de NFC, os participantes poderiam optar pela utilização de QR CODE.

O segundo cenário permitiu que o usuário utilizasse o protótipo para efetuar uma transação eletrônica em conjunto com um estabelecimento comercial. Este estabelecimento deveria possuir um equipamento POS que capaz de efetuar transações sem contato. O usuário efetuou o pagamento apenas aproximando os equipamentos. Informações de contexto poderiam ser utilizadas para permitir que este pagamento fosse automatizado, já que poderia indicar um pagamento recorrente, como por exemplo, um restaurante que é frequentado pelo usuário várias vezes ao longo do mês.

No terceiro cenário caracterizou a utilização do módulo comercial da aplicação. Neste cenário, o estabelecimento comercial também deveria estar cadastrado, para que fosse possível efetuar o *check-in* e a realização os pedidos através de um cardápio com QR CODE ou NFC. Cuidados foram tomados na confecção de um cardápio que possua várias *tags* NFC, já que o usuário poderia selecionar um produto incorreto caso as *tags* estejam perto fisicamente uma das outras. Este problema é minimizado com a utilização de QR CODES.

O quarto cenário também fez uso do módulo comercial para realizar os pedidos no estabelecimento. Novamente, o estabelecimento necessitou cadastro para que fosse possível efetuar o *check-in* e realizar os pedidos, mas neste cenário não existe um cardápio físico. Os itens disponíveis foram visualizados através do dispositivo móvel, onde o pedido também foi efetuado.

Por fim, o quinto cenário, que também necessitou que o estabelecimento possuísse cadastro, permitiu o pagamento com um leitor de cartões acoplado ao dispositivo móvel. O leitor utilizado no projeto possui conexão com o dispositivo móvel através da entrada de áudio, necessitou ser configurado antes de ser utilizado pela primeira vez. Esta configuração modificou o nível de som do sistema operacional para permitir o correto funcionamento do dispositivo.

6.2 Avaliação de usabilidade

A avaliação da usabilidade vem sendo utilizada com sucesso para a avaliação de aplicações móveis (BIEL, 2010), (ZHANG, 2005). De acordo com a ISO 9241-11, usabilidade é definida como a maneira que um produto pode ser utilizado por um usuário específico para alcançar objetivos específicos com eficácia, eficiência e satisfação em um determinado contexto de uso (ISO, 1998).

Além de definir a usabilidade, a norma ISO 9241-11 também explica como identificar a informação que deve ser considerada na avaliação de usabilidade em termos de desempenho e satisfação do usuário, além de explicar como medidas de desempenho e satisfação podem ser utilizadas para avaliar como qualquer componente do sistema afeta todo o trabalho final, conforme a NBR 9241-11 (NBR, 2002). Os benefícios da usabilidade para os usuários têm sido destacados na literatura (BIAS, 2005)(NIELSEN, 2008). De acordo com Seffah (2004) a baixa usabilidade é o maior responsável pelo fracasso de um software.

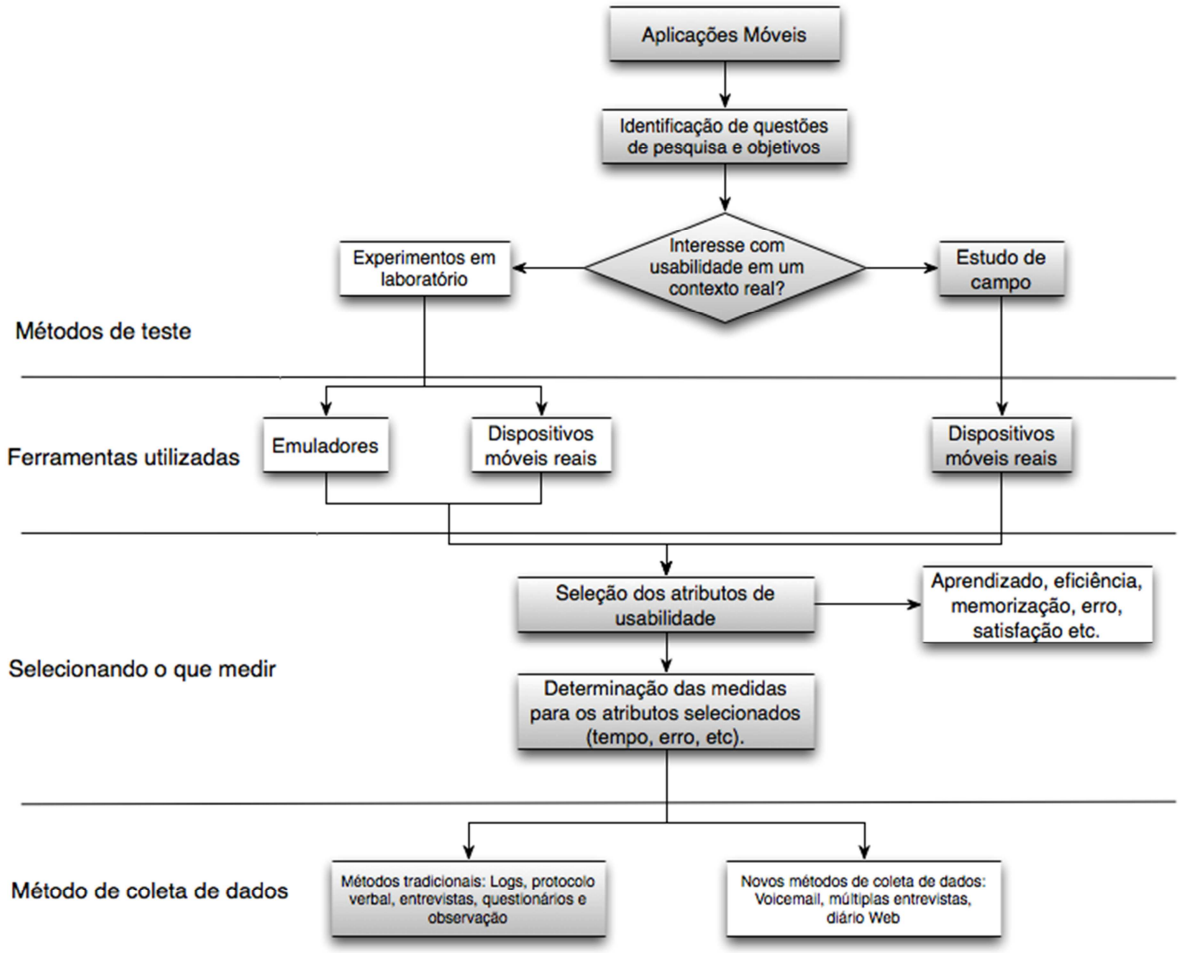
6.2.1 Metodologia

Para a avaliação de usabilidade, foram considerados três importantes atributos, definidos abaixo de acordo com a ISO 9241-11 (ISO, 1998):

- **Efetividade:** Acurácia e completude com as quais usuários alcançam objetivos específicos;
- **Eficiência:** Recursos gastos em relação à acurácia e abrangência com as quais usuários atingem objetivos;
- **Satisfação:** Ausência do desconforto e presença de atitudes positivas para com o uso de um produto.

Para a avaliação destes itens, foi utilizado um *framework* proposto por (ZANG, 2005). Este *framework*, exibido na Figura 29, tem como objetivo facilitar a realização de estudos de usabilidade para aplicações móveis e envolve questões importantes que devem ser levadas em consideração durante a construção de um teste de usabilidade de um aplicativo móvel. As opções utilizadas na avaliação estão destacadas em cinza. Como método de teste, optou-se por estudos de campo, utilizando como ferramentas dispositivos móveis reais. Os atributos selecionados para medição foram efetividade, eficiência e satisfação, e foram utilizados métodos tradicionais para coleta dos dados dos usuários.

Figura 29 Framework para design e implementação de testes de usabilidade de aplicativos móveis



Fonte: Traduzido livremente de Zang (2005).

A avaliação dos itens de usabilidade foi conduzida de acordo com um protocolo, baseado em Kenteris (2009), e o *framework* de ZANG (2005). A avaliação foi realizada através da condução de testes em campo, com dispositivos reais. Como cenário, foi utilizada a loja de conveniências de um posto de gasolina, permitindo que os usuários realizassem seus pedidos como lanches e bebidas diretamente no dispositivo móvel. Ele foi escolhido como local de prova por apresentar as características necessárias para a utilização do módulo comercial (estabelecimento com internet *WiFi* para seus clientes, presença no *Foursquare*) e também do módulo financeiro (possui equipamentos como TEF e POS com tecnologia *contactless*). O estabelecimento comercial também demonstra interesse na adoção de tecnologias que possam facilitar a vida de seus clientes.

Inicialmente, o usuário recebeu uma breve explicação sobre as funcionalidades da aplicação e foi então apresentado a um roteiro de avaliação, contendo as seis tarefas listadas na Tabela 9. Não foi realizada nenhuma demonstração prévia da aplicação.

Tabela 9 Lista de tarefas a serem executadas pelos avaliadores do UniPAg

Número	Descrição
1	Fazer o *check-in* no estabelecimento
2	Realizar um pedido pelo UniPag
3	Fazer o *checkout* usando um NFC
4	Fazer o pagamento usando um cartão de crédito
5	Consultar o saldo do moedeiro eletrônico
6	Fazer uma transferência usando QR CODE para outro dispositivo

Fonte: Elaborado pelo autor

Foram computados os tempos de execução de cada uma das tarefas, a fim de medirmos a eficiência. Também foram computadas as efetividades dos usuários em efetuar as tarefas propostas. Para medir o aprendizado do usuário ao utilizar a aplicação, foi solicitado que, ao término da execução das tarefas, todo o roteiro fosse repetido. Ao fim de todo o processo, o usuário respondeu uma pesquisa de avaliação do protótipo Unipag.

A pesquisa de avaliação foi utilizada para mensurar a satisfação do usuário com o aplicativo desenvolvido. A pesquisa foi desenvolvida de acordo com o Modelo de Aceitação de Tecnologia (TAM), inicialmente apresentado por Davis (1989) e posteriormente revisado por Yoon e Kim (2007). Esta técnica busca modelar a maneira com que os usuários aceitam e utilizam uma determinada tecnologia. Este formulário foi elaborado através da ferramenta Goggle Docs[9], que possibilita o *upload* das respostas e criação de relatórios de maneira *online*.

De acordo com este modelo, no momento em que usuários são apresentados á uma nova tecnologia, algumas características irão influenciar a sua utilização, tais como:

- **Utilidade percebida (*Perceived usefulness*):** Nível que o usuário avalia que determinada tecnologia irá melhorar seu desempenho/experiência
- **Facilidade de utilização (*Perceived ease-of-use*):**Nivel que o usuário avalia que determinada tecnologia poderá diminuir seus esforços/estresse

Para avaliação da percepção de utilidade, foram elaboradas cinco sentenças, e para cada uma delas o usuário pode escolher entre cinco respostas, de acordo com a escala de Likert (LIKERT, 1932). As possíveis respostas são concordo totalmente, concordo,

[9] docs.google.com

indiferente, discordo e discordo totalmente. As sentenças referentes à percepção de utilidade são exibidas na Tabela 10.

Tabela 10 Sentenças referentes à Percepção de utilidade

Número	**2. Em relação à percepção de utilidade do aplicativo 4iPay, indique sua opinião sobre as seguintes afirmações:**
1	As opções de pagamento atendem à minha utilização do dia a dia
2	O servidor de pedidos facilita a escolha de produtos em um estabelecimento
3	O aplicativo agiliza o atendimento em um estabelecimento comercial
4	O aplicativo simplifica a transferência de valores entre duas pessoas
5	Utilizaria o aplicativo se disponível

Fonte: Elaborado pelo autor

Em relação à facilidade de utilização da aplicação, foram elaboradas as sentenças da Tabela 11. Estas sentenças seguem o mesmo padrão de resposta das sentenças de percepção de utilidade.

Tabela 11 Sentenças referentes à Facilidade de utilização

Número	**1. Em relação à facilidade de uso do aplicativo 4iPay, indique sua opinião sobre as seguintes afirmações:**
1	O aplicativo é fácil de usar
2	É fácil realizar um pagamento com carteira digital
3	O *check-in* permite uma interação eficiente com o estabelecimento
4	O sistema permite realizar pedidos de maneira simples
5	O aplicativo permite transferência de valores entre dois usuários de forma prática

Fonte: Elaborado pelo autor

Além das questões relativas ao TAM, foram realizadas as perguntas da Tabela 12, com o objetivo de verificar o perfil do usuário que está realizando o teste.

Tabela 12 Perguntas sobre participantes

Número	Pergunta
1	Idade
2	Profissão
3	Sexo
4	Possui smartphone (marca/modelo)

Fonte: Elaborado pelo autor

O estabelecimento comercial atende em média 50 clientes durante o horário de almoço. De acordo com Louis (1997), para populações consideradas pequenas (menores que

200), deve-se ter como tamanho de amostra ao menos metade da população. Desta maneira, o roteiro de testes foi realizado com 25 participantes.

6.2.2 Resultados obtidos

Os testes dos cenários foram aplicados em um estabelecimento comercial real, durante o horário do almoço, de acordo com os critérios citados na sessão 6.2.1. Foram realizados diversos testes com usuários durante o horário comercial do estabelecimento, principalmente durante o horário de almoço. A Figura 30 mostra o teste sendo realizado com um dos usuários.

Figura 30 Teste realizado no estabelecimento comercial

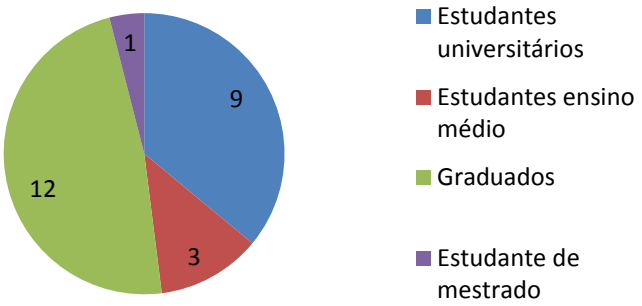
Fonte: Elaborado pelo autor

O perfil do grupo ficou dividido da seguinte forma:

- 9 estudantes universitários;
- 3 estudante de ensino médio;
- 12 graduados em áreas diversas (Engenharia, Computação, Economia, Administração);
- 1 estudante de mestrado.

O gráfico com os percentuais dos perfis dos usuários selecionados é exibido na Figura 31.

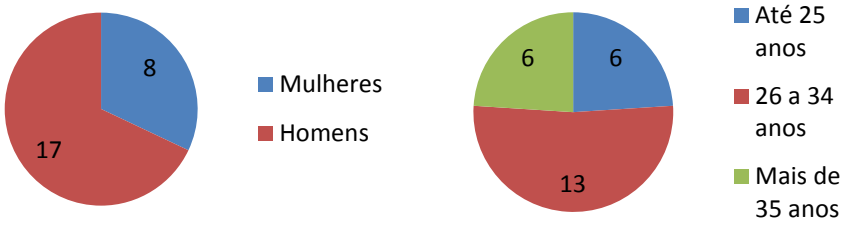
Figura 31 Perfil dos usuários entrevistados



Fonte: Elaborado pelo autor

A divisão por sexo e por idade é apresentada

Figura 32 Divisão por a) Sexo b) Faixa etária

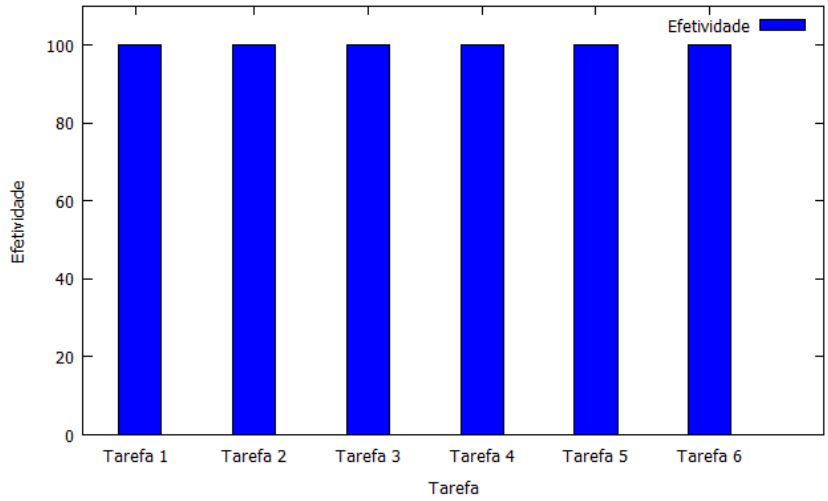


Fonte: Elaborado pelo autor

O sistema operacional utilizado por 30,43% dos entrevistados é o iOS, 47,8% possuem smartphone com sistema operacional Android, 4,34% são usuários de Windows Phone e 4,34% são usuários de BlackBerry.

O primeiro resultado obtido através dos testes realizados diz respeito à efetividade. Conforme o gráfico da Figura 33, todos os usuários completaram as tarefas propostas nas duas etapas de execução do roteiro. Com base neste resultado, concluímos que a aplicação apresenta um alto nível de efetividade.

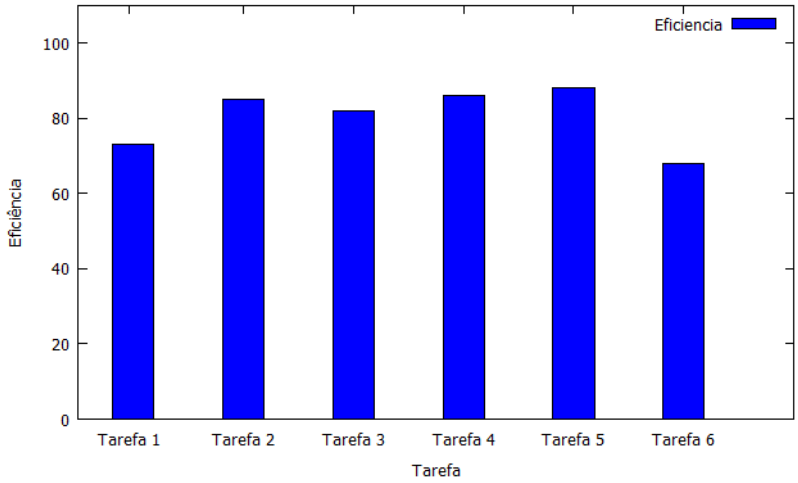
Figura 33 Efetividade de execução das atividades propostas



Fonte: Elaborado pelo autor

O segundo resultado obtido através da análise dos dados coletados nos fornece a eficiência média obtida para execução das tarefas. Este parâmetro é obtido através das médias de cada usuário para a execução dupla das tarefas. O valor obtido é então comparado a um valor de referência pré-definido. O valor de referência foi definido através da coleta dos tempos de execução das tarefas por um usuário especialista, com amplo domínio da aplicação. O resultado obtido é exibido na Figura 34.

Figura 34 Eficiência média na execução das tarefas



Fonte: Elaborado pelo autor

Como todas as tarefas foram executadas pelos usuários duas vezes, foi possível medir o aprendizado que o usuário obteve com a execução contínua da tarefa, através da comparação do tempo de execução das tarefas. A Tabela 13 apresenta os resultados obtidos.

Tabela 13 Aprendizado do usuário

Tarefa	Eficiência média na primeira execução (segundos)	Eficiência média na segunda execução (segundos)	Aprendizado (%)
Tarefa 1	16,88	10,48	62,08
Tarefa 2	15,28	8,2	53,66
Tarefa 3	14	10,12	72,28
Tarefa 4	39,08	30,5	78,03
Tarefa 5	3,8	3	78,94
Tarefa 6	46,84	26,68	66,99

Fonte: Elaborado pelo autor

Para avaliação da satisfação do usuário com a aplicação, foram utilizados os dados coletados através do formulário. As opções de resposta possibilitam desde total aceitação (concordo plenamente) até total discordância (discordo totalmente). O resultado da pesquisa de percepção de utilidade é exibido na Tabela 14.

Tabela 14 Resultado da avaliação de percepção de utilidade

Questão	Discordo totalmente	Discordo	Indiferente	Concordo	Concordo plenamente
1. As opções de pagamento atendem à minha utilização do dia a dia	0% (0)	0% (0)	4% (1)	36% (9)	60%(15)
2. O servidor de pedidos facilita a escolha de produtos em um estabelecimento	0% (0)	0% (0)	0% (0)	4% (1)	96% (24)
3. O aplicativo possibilita agilizar o atendimento em um estabelecimento comercial	0% (0)	0% (0)	0% (0)	12% (3)	88% (22)
4. O aplicativo simplifica a transferência de valores entre duas pessoas	0% (0)	0% (0)	4% (1)	4% (4)	96% (20)
5. Utilizaria o aplicativo se disponível	0% (0)	0% (0)	0% (0)	0% (1)	100% (24)

Fonte: Elaborado pelo autor

De maneira geral, os participantes da avaliação do protótipo consideraram o aplicativo interessante. Um dos pontos mais comentados foi a opção de realizar o *check-in* no estabelecimento e realizar os pedidos diretamente no dispositivo móvel.

As declarações dos participantes para a pesquisa de facilidade de utilização é exibida na Tabela 15.

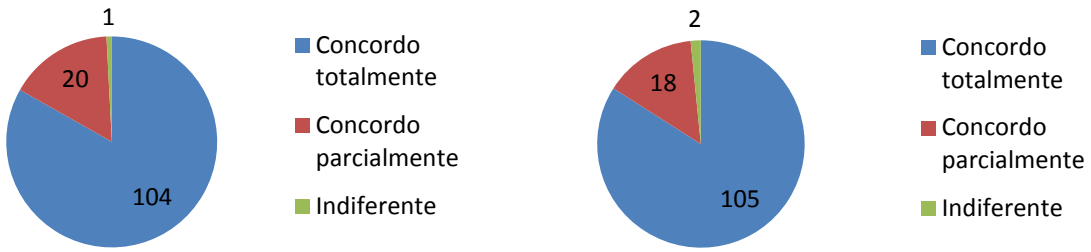
Tabela 15 Resultado da avaliação de facilidade de uso

Questão	Discordo totalmente	Discordo	Indiferente	Concordo	Concordo plenamente
1. O aplicativo é fácil de usar	0% (0)	0% (0)	0% (0)	12% (3)	88%(22)
2. É fácil realizar um pagamento com carteira digital	0% (0)	0% (0)	0% (0)	20% (5)	80% (20)
3. O *check-in* permite uma interação eficiente com o estabelecimento	0% (0)	0% (0)	4% (1)	16% (4)	80% (20)
4. O sistema permite realizar pedidos de maneira simples	0% (0)	0% (0)	0% (0)	4% (1)	96% (24)
5. O aplicativo permite transferência de valores entre dois usuários de forma prática	0% (0)	0% (0)	0% (0)	28% (7)	72% (18)

Fonte: Elaborado pelo autor

Os resultados obtidos pela avaliação de satisfação estão resumidos na **Erro! Fonte de referência não encontrada.**

Figura 35 Resumo da avaliação (a) Facilidade de uso (b) Percepção de utilidade



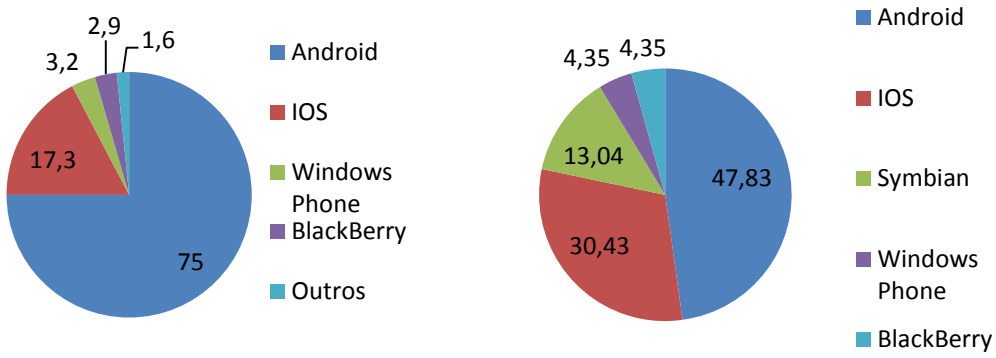
Fonte: Elaborado pelo autor

6.2.3 Discussão

Através da analise dos dados coletados durante a avaliação com os usuários, são apresentados diversos pontos, com o objetivo de discutir e comparar as informações entre diferentes idades, além dos problemas encontrados durante os testes.

A distribuição do sistema operacional utilizado pelos usuários que participaram da pesquisa assemelha-se com a distribuição mundial, de acordo com a pesquisa disponibilizada pelo Gartner (2013). A **Erro! Fonte de referência não encontrada.** apresenta esta comparação.

Figura 36 Distribuição de S.O por dispositivo móvel (a) mundial (b) entrevistados

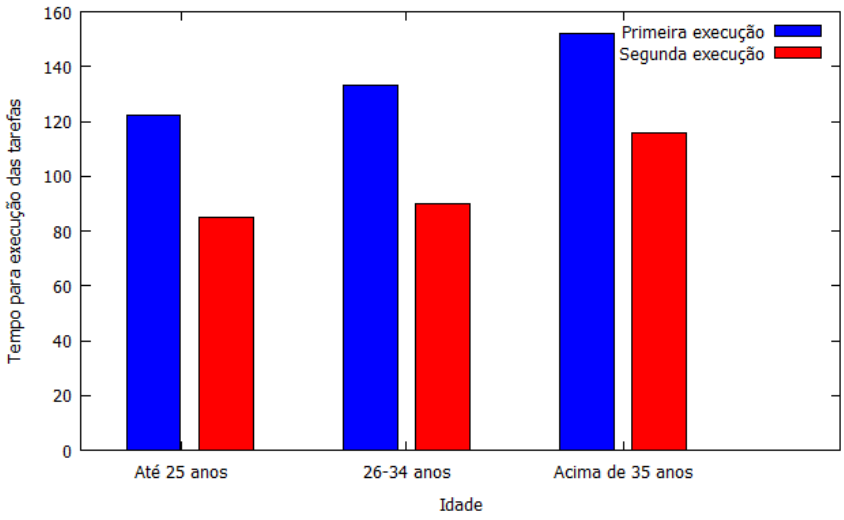


Fonte: Gartner (Março 2013)

Com um percentual de usuários ainda baixo, a plataforma Windows Phone pode ajudar na adoção ampla de um sistema de pagamento móvel. A partir da versão 8 do S.O, todos os dispositivos móveis devem ter NFC, permitindo a criação de um aplicativo que realize o pagamento utilizando um elemento seguro (NFCTIMES, 2012).

Os usuários que participaram da avaliação foram divididos em três faixas de idade, com o objetivo de verificar o tempo médio total de execução das atividades de acordo com a faixa etária. As faixas etárias escolhidas foram até 25 anos, de 26 anos até 34 e mais do que 35 anos de idade. A **Erro! Fonte de referência não encontrada.** apresenta os resultados obtidos.

Figura 37 Tempo médio para execuções, por faixa etária



Fonte: Elaborado pelo autor

Foi verificado que os participantes com mais de 35 anos possuem o maior tempo médio para execução das tarefas. Já para as outras duas faixas etárias, o tempo médio é bastante semelhante. Esta faixa etária também teve o menor percentual de aprendizado, executando as segundas tarefas em um tempo 23,4% mais rápido do que na primeira execução.

A execução das tarefas apresentou ótima efetividade, independente da faixa etária. Todos os usuários obtiveram sucesso na execução das tarefas sem dificuldades, mesmo com o total desconhecimento de algumas das tecnologias envolvidas, como *tags* NFC, QR CODES ou mesmo *smartphones*.

Através da Figura 34, verificou-se que a primeira e a última tarefa apresentaram uma menor eficiência frente às demais. O motivo desta menor eficiência na primeira tarefa é a necessidade da conexão 3G do dispositivo móvel para efetuar o *check-in* no estabelecimento. Desta maneira, mesmo que o usuário selecionasse rapidamente o estabelecimento, ele dependia da conexão da operadora e do tempo de resposta do serviço do *Foursquare*, responsável por realizar o *check-in*.

Já a última tarefa apresentou uma menor eficiência devido principalmente à necessidade de leitura do QR CODE. A aplicação apenas efetua a leitura do código quando o dispositivo móvel está paralelo ao código QR. Qualquer ângulo formado entre as duas partes inviabiliza a leitura. Esta tarefa teria um tempo de execução menor caso o usuário efetuasse o pagamento utilizando NFC, que não apresentou nenhum problema para ser lido na tarefa três.

De maneira geral, o tempo de execução das tarefas foi bastante satisfatório, e encontram-se dentro do esperado para a complexidade das tarefas. Em comparação com um pagamento tradicional, pode-se dizer que mesmo as tarefas com menor eficiência ainda são executadas mais rápidas que os meios de pagamento tradicional. É esperado que a eficiência aumente com o uso contínuo da aplicação, e o usuário se aproxime dos tempos obtidos pelo usuário especialista.

De maneira geral, o ganho de aprendizado após a execução da segunda tarefa foi de aproximadamente 67%, ou seja, em média os usuários efetuaram a segunda tarefa 33% mais rápido do que a primeira vez. O menor ganho verificado foi para a quinta tarefa. Isto é justificado pela facilidade de execução da tarefa, que consiste apenas na verificação do saldo disponível no moedeiro eletrônico.

As atividades foram executadas pelos usuários sem grandes dificuldades. Em todos os casos, foi possível realizar a tarefa solicitada. Algumas vezes, o usuário levou um tempo maior para a execução, como por exemplo, ao solicitar um pedido, pois realizava a navegação entre as diferentes categorias até executar a tarefa.

Dentre os comentários realizados pelos usuários e visualizados durante os testes, destacam-se:

- Enquanto que a maioria das opções a tela principal da aplicação levam à uma segunda tela, a opção de *check-in* é efetuada já na tela principal. Esta diferença levou à alguns usuários levarem um tempo a mais para a execução desta tarefa, pois pressionavam o botão *check-in* e esperavam algum resultado, ao invés de já selecionar o estabelecimento na tela;
- O pagamento com cartão de crédito na opção Mobile POS não indica a posição com que o cartão deve ser passado. Isto acaba elevando o tempo desta atividade, já que o usuário, além de não estar acostumado a executar este tipo de ação, precisa descobrir a maneira de passagem do cartão;
- Durante a passagem do cartão na opção Mobile POS, o usuário acaba segurando o dispositivo de uma maneira diferente, e pressiona o botão de volume do celular. Como o leitor de cartões utiliza a entrada de áudio e a configura, definindo um volume mínimo, esta ação acaba fazendo com que seja necessária a reconfiguração do dispositivo, contribuindo para o aumento do tempo desta atividade;

- O desconhecimento das tecnologias empregadas para o pagamento (NFC e QRCODE) contribuiu para o aumento dos tempos de execução de algumas atividades;
- Foi encontrada dificuldade na leitura de QR CODE com o dispositivo utilizado. É necessário que o dispositivo e o código QR estejam paralelos para uma leitura rápida. O mesmo não acontece para a leitura do código utilizando um dispositivo com IOS. Este problema contribuiu para o aumento do tempo de execução da tarefa de pagamento utilizando moedeiro eletrônico.

Na avaliação de percepção de utilidade, a sentença *O aplicativo simplifica a transferência de valores entre duas pessoas* recebeu uma avaliação de indiferença. Na avaliação de facilidade de uso, a sentença *O check-in permite uma interação eficiente com o estabelecimento* também recebeu uma avaliação de indiferença. Mesmo assim, 100% dos usuários que executaram os testes responderam *Concordo Plenamente* para a sentença *Utilizaria o aplicativo se disponível*, mostrando um altíssimo nível de aceitação da aplicação pelos usuários.

Analisando de maneira geral os dados coletados, conclui-se que o modelo desenvolvido possui uma aceitação por parte dos usuários, mostrando a viabilidade de adoção do modelo proposto.

7 CONCLUSÃO

O trabalho aqui apresentado teve como objetivo apresentar um modelo para pagamento móvel que utilize múltiplas tecnologias, como por exemplo, NFC e QR CODE, permitindo que o pagamento seja efetuado através de diferentes meios, como moedeiro eletrônico, cartão de crédito e integração com o sistema de pagamento do estabelecimento. O protótipo foi desenvolvido no sistema operacional Android, e as características do projeto permitem que ele seja expandido para qualquer equipamento móvel, tornando o modelo genérico e permitindo o pagamento entre usuários de duas plataformas diferentes.

Para elaboração do modelo, foram estudados quatro trabalhos de carteira digital, e as características destes trabalhos comparadas com o modelo Unipag podem ser visualizadas na Tabela 16. O modelo Unipag apresenta como vantagens sua heterogeneidade, suportando um grande número de sistemas operacionais móveis, suporte a diferentes tipos de elemento seguro e transações *online* e *offline*, além de possibilitar uma interação com o estabelecimento através do módulo comercial. Com a possibilidade de efetuar pagamentos através de QR CODES, é possível portar o modelo para diferentes tipos de telefones móveis, inclusive os mais acessíveis à população, já que a maioria dos dispositivos móveis possui uma câmera fotográfica, único requisito para a leitura do código QR.

Tabela 16 Comparação entre os modelos de carteira digital

	mFerio	**fairCash**	**Osaifu-Keitai**	**Google Wallet**	**Unipag**
Elemento Seguro	Sim	Sim (HW próprio)	Sim	Sim	Sim
Tipo de Elemento Seguro	Embarcado	Embarcado	Cartão SIM	Embarcado	Embarcado/Sim Card
Suporte à transações *offline*	Sim	Sim	Sim	Sim	Sim
Meio utilizado para pagamento	NFC	NFC/*Bluetooth*/WIFI	RFID/NFC	NFC	NFC/QR CODE
Divisão Monetária	-	eCoins	-	-	-

Anonimidade	Não	Anonimo para transações entre usuários. Transações entre usuário e estabelecimentos são rastreáveis.	Transações são rastreáveis através do emissor do cartão de crédito	Transações são rastreáveis através do emissor do cartão de crédito	Transações entre dois usuários são anônimas
Autenticação	PIN/Biometria/ Desenho	PIN	PIN	PIN	PIN
Abrangência (Dispositivos Suportados)	Limitada	Limitada	Ampla	Limitada	Ampla
Fidelidade/Cupons de desconto	Não	Não	Sim	Sim	Sim
SO Suportado	Symbian	Windows Mobile	Symbian/Android	Android	Android

Fonte: Elaborado pelo autor

Em relação aos trabalhos relacionados, o trabalho apresentado apresenta limitações quanto à autenticação, limitada atualmente pela utilização de PIN, enquanto os trabalhos relacionados incluem autenticação por biometria e contexto. O modelo está disponível apenas para o SO Android, embora não apresente nenhuma dependência quanto ao sistema operacional. Outros modelos estudados possuem maior abrangência de sistemas operacionais, embora muitos já estejam descontinuados.

Como principal limitação do protótipo desenvolvido, podemos citar a emulação do elemento seguro, devido à necessidade de suporte do fabricante do dispositivo para a sua utilização. Outro problema de importante destaque é a dificuldade de testar o protótipo nos diferentes equipamentos disponíveis com o sistema operacional Android. Devido à característica do SO, cada fabricante possui liberdade para criar sua própria especificação de Hardware. Um teste completo de um software em produção deve prever o maior número possível de dispositivos e configurações diferentes. Nos testes realizados com três modelos diferentes, foram encontradas diversas dificuldades, principalmente em relação ao modelo mais antigo dentre os dispositivos testados.

O protótipo foi desenvolvido utilizando o ambiente de programação Eclipse em conjunto com o SDK do sistema Android, e foi testado em dispositivos reais, como os celulares Samsung Galaxy X, Samsung Galaxy S3 e Motorola Milestone, além do emulador disponibilizado pelo SDK.

A primeira avaliação do protótipo foi realizada, através da criação de cinco cenários de utilização. Estes cenários abragem os principais métodos de pagamento utilizados no dia a dia, e servem para testar as principais funcionalidades da aplicação. Os cenários foram executados com sucesso, sem a ocorrência de imprevistos ou instabilidade na aplicação.

A avaliação de usabilidade do protótipo foi realizada em um estabelecimento comercial, e teve a participação de 25 potenciais usuários da aplicação. Os usuários receberam uma breve explicação do funcionamento do protótipo, e foram convidados a executarem seis diferentes atividades, que contemplavam as principais funcionalidades da aplicação, como pagamento utilizando moedeiro eletrônico, *check-in* e *checkout* no estabelecimento, além da utilização do servidor de pedidos. As tarefas foram realizadas pelos usuários e tiveram seus tempos de execução medidos. Ao término da atividade, os usuários executavam novamente as tarefas. Desta maneira, foi possível medir a eficiência e aprendizado dos usuários. De maneira geral, foi verificado um alto nível de eficiência na execução das tarefas, e os usuários apresentaram um grande aprendizado entre a primeira e a segunda execução.

Para medir a aceitação do modelo, foi desenvolvido um formulário, com o objetivo de medir a percepção de utilidade e facilidade de uso. Os resultados mostraram uma grande aceitação por parte dos usuários, além de destacar a facilidade de utilização do protótipo desenvolvido. Os principais comentários realizados pelo usuário foram destacados, com o objetivo de melhorar a usabilidade da aplicação.

Estudos recentes mostraram que o elemento seguro também é vulnerável (ROLAND, 2013). Assim, uma aplicação de carteira digital deve estar sempre em constante desenvolvimento, buscando a solução dos problemas encontrados de maneira rápida. A entidade responsável pela gerência do elemento seguro deve fornecer um método rápido para atualização da aplicação, a fim de minimizar os impactos.

Durante o desenvolvimento do trabalho, o seguinte artigo foi publicado e apresentado à comunidade acadêmica:

JOST, T. ; COSTA, C. A. da ; RIGHI, R. R. ; ANDRADE, A. . Automation of a Vending System Using Smartphones. In: IADIS WWW/Internet 2012 Conference (ICWI 2012), 2012, Madrd. Proceedings of IADIS WWW/Internet 2012 Conference. Lisboa: IADIS, 2012. p. 415-419.

Para continuidade do trabalho, pretende-se expandir o protótipo para as demais plataformas predominantes do mercado de dispositivos móveis, bem como realizar testes com um número maior de dispositivos móveis e tablets. Com o aumento expressivo da oferta de banda larga para dispositivos móveis no mercado nacional a preços cada vez mais acessíveis, torna-se possível o desenvolvimento de um modelo de carteira digital que realize a consolidação do saldo e o armazenamento dos dados do usuário na nuvem, em servidores seguros e de acordo com as normas do mercado (PCI-DSS). Desta maneira, uma das

principais limitações do modelo é eliminada, já que não é mais necessário o elemento seguro no dispositivo móvel.

Trabalhos recentes sobre pagamento móvel buscam cada vez mais utilizar o contexto do usuário para realizar o pagamento móvel (ROH, 2012)(TOOBA, 2012). O modelo atual utiliza o contexto para fornecer informações sobre os produtos disponíveis ao usuário. Entretanto, este assunto pode ser melhor trabalhado em futuras versões da aplicação, fornecendo ao usuário mais possibilidades de efetuar transações em seu dispositivo móvel.

Cada vez mais, os meios eletrônicos vêm se tornando a forma de pagamento preferida da população. Dentre os meios eletrônicos, o pagamento móvel destaca-se como o mais promissor e com maior possibilidade de crescimento, já que ainda existem poucas soluções disponíveis. O contínuo aumento do uso de dispositivos móveis equipados com elementos de segurança, alinhado com a crescente oferta de internet móvel e constante atualização das normas de segurança para transações financeiras contribuem para que o pagamento móvel seja o futuro das transações financeiras.

REFERÊNCIAS

AL-FEDAGHI, S.S.; TAHA, M.M. **Personal Information eWallet** In: SYSTEMS, MAN AND CYBERNETICS, 2006. SMC '06. IEEE INTERNATIONAL CONFERENCE ON, 4., 2006. Taipei p. 2855-2862, 2006.

BALAN, R. et al. **mFerio:** The Design and Evaluation of Peer-to-Peer Mobile Payment System. In: Proceedings of the 7th international conference on Mobile systems, applications, and services (MobiSys '09). New York, NY, USA: ACM. 22-25 June 2009. p. 22-25.

BANCO CENTRAL. **Diagnóstico do Sistema de Pagamentos de Varejo do Brasil**, 2004. Disponível em <>http://www.bcb.gov.br/?SPB. Acesso em 8 de setembro de 2012

BANCO CENTRAL. História do cartão de crédito – **Museu de valores do banco central**, 2011. Disponível em <http://www.bc.gov.br/?HISTCARTAO> Acessado dia 1 de setembro de 2012.

BANCO CENTRAL. **Origem e Evolução do Dinheiro , Museu de Valores do Banco Central, 2012.** Disponível em: <http://www.bc.gov.br/?ORIGEMOEDA>Acesso em 8 setembro 2012.

BHATLA, T. P. **Understanding Credit Card Frauds**.Junho, 2003. Disponível em< http://www.popcenter.org/problems/credit_card_fraud/PDFs/Bhatla.pdf>. Acesso em 02 de setembro de 2012.

BIAS, R. G; MAYHEW, D. J. **Cost-justifying usability an update for an Internet age.** Amsterdam, Morgan Kaufman.

BIEL, B; GRILL, T; GRUHN, V. Exploring the benefits of the combination of a software architecture analysis and a usability evaluation of a mobile application. **Journal of Systems and Software.** Elsevier Science Inc. New York, NY, USA, v. 83 n. 11 p. 2031-2044 DOI=10.1016/j.jss.2010.03.079

BOYD, J. **Here comes the wallet phone** [wireless credit card]. Spectrum, IEEE , 2009, v. 42, n. 11, p.12,14, Nov. 2005 doi: 10.1109/MSPEC.2005.1526896

CHEN, G; KOTZ, D. **A Survey of Context-Aware Mobile Computing Research**, *2000*. Technical Report. Dartmouth College, Hanover, NH, USA.

D. ZHANG AND B. ADIPAT. **Challenges, methodologies, and issues in the usability testing of mobile applications.** In International Journal of Human-Computer Interaction, 2005, v. 18, n. 3, p. 293–308.

DAHLBERG, T. et al., **Past, present and future of mobile payments research: a literature review. In** Electronic Commerce Research and Applications, Oxford, 2007, v. 7, n. 2, p.165-181.

DAVIS, F. D. Perceived usefulness, perceived ease of use, and user acceptance, MIS Quarterly, v. 13, n. 3,1989, p. 318–341, 1989.

DE SÁ, M; CARRIÇO, L. **Defining scenarios for mobile design and evaluation**. In: Extended Abstracts on Human Factors in Computing Systems (CHI EA '08). ACM, New York, NY, USA. DOI=10.1145/1358628.1358772 p. 2847-2852

DEY, A. K. **Understanding and Using Context. Personal and Ubiquitous Computing**, London, v. 5, n. 1, p. 4-7, February 2001.

DINERS CLUB. Company History, 2012. Disponível em: http://www.dinersclub.com/about-us.html>. Acesso em 14 setembro 2012.

DOCOMO. **Mobility DoCoMo Newsletter 34. 2011**. Disponível em < http://www.nttdocomo.co.jp/english/info/media_center/newsletter/pdf/mobility_doc_34.pdf> Acesso em 03 de novembro de 2012.

EMV: **Europay Mastercard Visa**, 2009. Disponível em http://www.emvco.com/. Acesso em 27 de setembro 2012.

FELICA NETWORKS. **Felica Networks Overview, 2012**. Disponível em < http://www.felicanetworks.co.jp> . Acesso em 03 de novembro de 2012.

FMC, 2012. TAM - **The SAP way combining FMC and UML.** Disponível em http://www.fmc-modeling.org/fmc-and-tam. Acesso em 02 de novembro 2012.

GARTNER. **Market Share Analysis: Mobile Phones, Worldwide, 1Q13. 2013**. Disponível em http://www.gartner.com/newsroom/id/2482816. Acesso em 20 de junho 2013

GOOGLE DASHBOARDS. **Relative number of devices running a given version of the Android platform. 2013. Disponível em** http://developer.android.com/about/dashboards/index.html Acesso em 10 de junho de 2013.

GOOGLE IO. **Developing Android REST client applications**. 2010. Disponível em: <http://www.google.com/events/io/2010/sessions/developing-RESTful-android-apps.html> Acesso em 03 de maio de 2013.

GOOGLE WALLET. **Google wallet Overview, 2011**. Disponível em < http://www.google.com/wallet/index.html>. Acesso em 03 de novembro de 2012.

GOTH, G. **Mobile Security Issues Come to the Forefront** In: Internet Computing, IEEE, 2012, v. 16, n. 3, p.7,9 doi: 10.1109/MIC.2012.54

GRAHAM, B. **The evolution of electronic payments**. 2003, 62f. Trabalho de conclusão de curso. (Engenharia Elétrica). DDivisão de Engenheiros Eletricistas e Eletrônicos, Escola da informação da tecnologia e Engenharia Elétrica, Universidade de Queensland, Australia, 2003.

HUANG, D., LIU, W., & LI, X. **A survey on context awareness** In: Computer Science and Service System (CSSS), 2011 International Conference on. p.144,147, 27-29 June 2011 doi: 10.1109/CSSS.2011.5972040

HWANG, H, GYEOK JUNG, KIWOOK SOHN, SANGSEO PARK. **A Study on MITM (Man in the Middle) Vulnerability in Wireless Network Using 802.1X and EAP.** In **:** International Conference on Information Science and Security (ICISS 2008), junho,2008, p.164-170

IBM. **IBM Ration Unified Process**. Disponível em <http://www-01.ibm.com/software/awdtools/rup>. Acesso em fevereiro de 2013.

INNOPAY . **Mobile Payments 2010 - Market analysis and overview.** Disponível em <http://www.innopay.com> Acesso em 8 setembro 2012

INVESTOPEDIA. **Definition of Credit .** Disponível em <http://www.investopedia.com/terms/c/credit.asp> Acesso em 8 setembro 2012.

ISO. International Standards for Business. ISO Financial Services, nov. 2011. Disponivel em: <http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=31628>. Acesso em: 01 nov. 2011.

ISO**. ISO Catalogue**. **1998. ISO 9141-11: Ergonomic Requirements for Office Work with Visual Display Terminals** (VDTs)—Part 11: Guidelines on Usability.

ISO. I**SO Catalogue. ISO 8583: 1993, 1993**. Disponivel em: <http://www.iso.org/iso/iso_catalogue/catalogue_ics/catalogue_detail_ics.htm?csnumber=15871>. Acesso em: 02 nov. 2012.

JSON. Introducing JSON. Disponível em http://www.json.org/. Acesso em 10 de junho de 2013.

JUNGLAS, I.; WATSON, R. T. The U-Constructs: Four Information Drives. **Communications of the Association for Information Systems**, v. 17, n. 26, p. 2-43, 2006. Disponível em: http://aisel.aisnet.org/cais/vol17/iss1/26.

KENTERIS M, GALAVAS D, ECONOMOU D. An innovative mobile electronic Tourist guide application. Pers Ubiquitous Comput 13(2):103–118 , 2009.

KOWAKAME, Y.; WAKAHARA, T. **A New One-time Authentication System Using a Cellular Phone with FeliCa Chip.** In Intelligent Networking and Collaborative Systems (INCoS), 2011 Third International Conference on. Novembro, 2011.Fukuoka, Japão, p.453,456.

KREFT, H.; ADI, W. **fairCASH - A Digital Cash Candidate for the proposed GCC Gulf Dinar.** In Innovations in Information Technology, 2006 . Novembro, 2006. Dubai, United Arab Emirates. p1,5. doi:10.1109/INNOVATIONS.2006.301916

CHING, Y. C.; KREFT, H. FairCASH: **Concepts and Framework**. In: Proceedings of the 2008 The Second International Conference on Next Generation Mobile Applications, Services, and Technologies. Washington, DC, USA: IEEE Computer Society. 2008. p. 269--274. Disponível em: http://portal.acm.org/citation.cfm?id=1510534.1511887.

KREFT, H; SCHIMMLER, M; WALTER A. **FairCASH Based on Loss Resistant Teleportation**. Alemanha: Shaker, 2011.

LIKERT, R. A Technique for the Measurement of Attitudes. Archives of Psychology, Washington,DC, v. 22, n. 140, p. 1-5, 932. ISSN 1933-01885-001. Disponível em: http://psycnet.apa.org/psycinfo/1933-01885-001.

LOUIS, R; PARKER, R. **Designing and Conducting Survey Research: A Comprehensive Guide**. San Francisco, CA: Jossey-Bass, 1997

LYYTINEN K.; YOO, Y. **Issues and Challenges in Ubiquitous Computing**. In IEEE Pervasive Computing, Los Alamitos, v.1, n.1, p. 61-65, Jan. 2002.

MA, D.; SAXENA, N.; XIANG, T.; ZHU, Y. **Location-Aware and Safer Cards: Enhancing RFID Security and Privacy via Location Sensing** In: *WISEC '12 Proceedings of the fifth ACM conference on Security and Privacy in Wireless and Mobile Networks*. ACM New York, NY, USA. 2012 p. 51-62. doi: 10.1109/TDSC.2012.89

MANVI, S. S., NALINI, N., & BHAJANTRI, L. B. **Recommender system in ubiquitous commerce.** In: *2011 3rd International Conference on Electronics Computer Technology*, v. 4, p. 434–438. doi:10.1109/ICECTECH.2011.5941937

MASTERCARD. **Benefits of Open Payment Systems and the Role of Interchange. 2008.** Disponível em http://www.mastercard.com. Acesso em 13 de setembro 2012.

MOBEY . **Mobile Financial Services Business Ecosystem Scenarios & Consequences** Edited By Mobey Forum Mobile Financial Services Ltd . (2006), 1–16.

MOBEY. **Mobey Forum's Series on Mobile Wallets : Mobile Wallet – Definition and Vision Part 1**. Edited By Mobey Forum Mobile Financial Services Ltd . (2011).

MOBEY. **Mobile Device Security Element - Key Findings from Technical Analysis v. 1.0, 2005**. Edited By Bishwajit Choudhary & Juha Risikko

NBR, 2002 ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR 9241-11: Requisitos Ergonômicos para Trabalho de Escritórios com Computadores. Rio de Janeiro, 2002.

NFCTIMES, 2012. **Microsoft: Expects All Windows Phone 8 Device Makers to Support NFC.** Disponível em http://nfctimes.com/news/microsoft-expects-all-windows-phone-8-devices-makers-support-nfc . Acesso em 23 outubro 2012.

NIELSEN, J. **Usability ROI Declining, But Still Strong**. Disponível em http://www.useit.com/alertbox/roi.html Acesso em 5 de junho 2013

OLSEN, M; HEDMAN, J; VATRAPU, R. **Designing digital payment artifacts.** In: Proceedings of the 14th Annual International Conference on Electronic Commerce (ICEC '12). ACM, New York, NY, USA, p. 161-168. DOI=10.1145/2346536.2346568

RAHIMIAN, V.; HABIBI, J. **MPaySmart: A Customer Centric Approach in Offering Efficient Mobile Payment Services.** In: Asia-Pacific Services Computing Conference, 2008. APSCC '08. IEEE, p. 1038,1043, 9-12 Dec. 2008 doi: 10.1109/APSCC.2008.243

RAZ, A., JUHOLA, J., FERNANDES, S., GALIS, A. **Fast and Efficient Context-Aware Services**. Catalunya: John Wiley & Sons Ltd, 2006

REENSKAUG, T. MVC Xerox PARC 1978-79, 1979. Disponivel em: <http://heim.ifi.uio.no/~trygver/themes/mvc/mvc-index.html>.

REVEILHAC, M.; PASQUET, MARC. **Promising Secure Element Alternatives for NFC Technology.** In: Near Field Communication, 2009. NFC '09. First International Workshop on, p. 75,80, 24-24 Feb. 2009 doi: 10.1109/NFC.2009.14

ROH, J; JIN, S. **Personalized advertisement recommendation system based on user profile in the smart phone.** In *Advanced Communication Technology (ICACT), 2012 14th International Conference on* , p. 1300,1303, 19-22 Feb. 2012

ROHERS, ALEX ROEHRS. **4iPay: Modelo de Sistema de Pagamento Móvel em Comércio Ubíquo**. 2012. Dissertação (Mestrado em Computação Aplicada) - Universidade do Vale do Rio dos Sinos, Coordenação de Aperfeiçoamento de Pessoal de Nível Superior. Orientador: Cristiano André da Costa.

ROLAND, M.; LANGER, J. **Digital Signature Records for the NFC Data Exchange Format.** In Near Field Communication (NFC), 2010 Second International Workshop on, p. 71,76, 20-20 April 2010 doi: 10.1109/NFC.2010.10

ROLAND, M.; LANGER, J.; SCHARINGER, J. **Practical Attack Scenarios on Secure Element-Enabled Mobile Devices.** In *Near Field Communication (NFC), 2012 4th International Workshop on*, p. 19,24, 13-13 March 2012
doi: 10.1109/NFC.2012.10

ROLAND, M.; LANGER, J.; SCHARINGER, J. **Applying relay attacks to Google Wallet.** In *Near Field Communication (NFC), 2013 5th International Workshop on,*, p. 1,6, 5-5 Feb. 2013 doi: 10.1109/NFC.2013.6482441

ROSS, P.E. **Phone-y money.**In Spectrum, IEEE , v. 49, n. 6, p. 60,63, June 2012
doi: 10.1109/MSPEC.2012.6203971

SAP, 2007. Standardized Technical Architecture Modeling Conceptual and Design Level. Disponível em http://www.fmc-modeling.org/download/fmc-and-tam/SAP-TAM_Standard.pdf. Acesso 26 outubro 2012.

SATYANARAYANAN, M. Pervasive computing: vision and challenges. Personal Communications, IEEE, Pittsburgh, v. 8, n. 4, p. 10-17, August 2001. ISSN ISSN: 1070-9916. Digital Object Identifier: 10.1109/98.943998.

SATYANARAYANAN, M. Mobile computing: the next decade. In: 1st ACM Workshop on Mobile Cloud Computing & Services: Social Networks and Beyond. 2010.

SEFFAH, A; METZKER, E. **The obstacles and myths of usability and software engineering**. In: Communications of the ACM - The Blogosphere. v. 47, n. 12, p.71-76, December 2004, 71-76. DOI=10.1145/1035134.1035136

SERASA, 2010. **Uso de cheques cai 57% em uma década.** Disponível em: <http://www.serasaexperian.com.br >. Acesso em 2 de setembro 2012

SIENKIEWICZ, STANLEY J. **Credit Cards and Payment Efficiency.** Disponível em http://www.phil.frb.org/consumer-credit-and-payments/payment-cards-center/publications/discussion-papers/2001/PaymentEfficiency_092001.pdf. Acesso em 5 setembro 2012.

SMART CARD ALLIANCE. Mobile/NFC Security Fundamentals. 2013. Disponível em http://www.smartcardalliance.org/resources/webinars/Secure_Elements_101_FINAL3_032813.pdf Acesso em 11 de junho de 2013.

T. HSU. **Real-time risk control system for CNP (card not present).** In: Proceedings of the 17th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 2011. ACM New York, NY, USA, p. 783-783 , DOI: 10.1145/2020408.2020541

TAM. Tecnology Aceptance Model. (2012). Disponível em: <http://www.fmcmodeling.org/fmc-and-tam>. Acesso em outubro de 2012.

TATLI, E.I.; STEGEMANN, D.; LUCKS, S. **Security Challenges of Location-Aware Mobile Business**. In: Mobile Commerce and Services, 2005. WMCS '05. The Second IEEE International Workshop p. 84,95, 19-19 July 2005 doi:10.1109/WMCS.2005.23

TECHCRUNCH. J.P. Morgan: **Global E-Commerce Revenue To Grow By 19 Percent In 2011 To $680B.** Disponível em < http://techcrunch.com/2011/01/03/j-p-morgan-global-e-commerce-revenue-to-grow-by-19-percent-in-2011-to-680b/>. Acesso em: 7 setembro 2012.

TECHCRUNCH: **NFC Cometh? 1M Android NFC Devices Shipping Each Week, And Prototypes Show iPhone 5 Is Next.** Disponível em < http://techcrunch.com/2012/06/28/nfc-cometh-1m-android-nfc-devices-shipping-each-week-and-prototypes-show-iphone-5-is-next/>. Acesso em: 7 setembro 2012.

TIWARI, R.; BUSE, S. The Mobile Commerce Prospects: A strategic analysis of opportunities in the banking sector. Hamburg: Hamburg University Press, 2007. 33 p. ISBN 978-3-937816-31-9. Disponível em: http://hup.sub.unihamburg.de/opus/volltexte/2008/16/pdf/HamburgUP_Tiwari_Commerce.pdf.

TRI. **Sistema de bilhetagem eletrônica de Porto Alegre**. 2012. Disponível em www.tripoa.com.br. Acesso em 03 de outubro de 2012

TOOBA, Q; SIDRA, S; SHAFIQ, R. **Interactive shopping with mobile wallet.** In: Sustainable Technologies (WCST), 2012 World Congress. London, United Kingdom, p. 32,36, 19-22 Nov. 2012

UPADHYAYA, B.; YING ZOU; HUA XIAO; NG, J.; LAU, A. **Migration of SOAP-based services to RESTful services**. In: Web Systems Evolution (WSE), 2011 13th IEEE

International Symposium on. Williamsburg. p. 105,114, 30-30 Sept. 2011 doi: 10.1109/WSE.2011.6081828

VASSILAKIS, C., LEPOURAS, G., SKIADOPOULOS, S. **Mobile and Context-Aware e-Commerce: Issues, Challenges and Research Directions.** In: Special Issue Editorial Preface, Journal of Electronic Commerce in Organizations, v. 6, n. 1, 2008

VISA, 2012. Digital Wallet Security. Disponível em <http://www.visasecuritysense.com/en_US/_media/digital-wallet-best-practices.pdf> Acesso em 8 de setembro de 2012.

WATSON, R. T. et al. U-Commerce: Expanding the Universe of Marketing. Journal of the Academy of Marketing Science, v. 30, n. 4, p. 333-347, October 2002. ISSN 00920703.

WEISER, M. The Computer for the 21st Century. Scientific American, New York, v.265, n.3, p. 94-104, Mar. 1991.

WILLIAM M. DALEY, **Data Encryption Standard (DES)**, U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, October 1999.

WOOLSEY, B. **The history of American Express.** Disponível em http://www.creditcards.com/credit-card-news/american-express-history-1264.php Acesso em 8 setembro 2012

YAU, S.S.; KARIM, F.; YU WANG; BIN WANG; GUPTA, S. K S. **Reconfigurable context-sensitive middleware for pervasive computing**. In: Pervasive Computing, IEEE , v.1, n .3, p .33,40, July-Sept. 2002 doi: 10.1109/MPRV.2002.1037720

YOON, C. e KIM, S. **Convenience and TAM in a ubiquitous computing environment: The case of wireless LAN**. In: Electronic Commerce: Research and Applications, v. 6, n. 1, Janeiro 2007, p. 102-112., 2007.

ZHANG, D; ADIPAT, B. **Challenges, methodologies, and issues in the usability testing of mobile applications**. In International Journal of Human-Computer Interaction, 2005. v. 18, n. 3, p. 293–308

ZHANG, L.; LIU, Q.; LI, X. **Ubiquitous Commerce: Theories, Technologies, and Applications**. Journal of Networks, v. 4, n. 4, p. 271-278, 2009. DOI:10.4304/jnw.4.4.271-278.

ZHANG, X; PARHI, K. **High-speed VLSI architectures for the AES algorithm**. In Very Large Scale Integration (VLSI) Systems, IEEE Transactions on, v. 12, n. 9 p. 957-967. DOI=10.1109/TVLSI.2004.832943

ZWASS, V. **Electronic commerce: structures and issues**. International Journal of Electronic Commerce, Armonk, NY, USA, v. 1, n. 1, p. 3-23, September 1996. ISSN 1086-4415. Disponível em: http://portal.acm.org/citation.cfm?id=1189795.1189796.

ZXINGLIB. **An android library project of zxing BarcodeScanner. 2012** Disponivel em http://code.google.com/p/android-zxinglib/. Acesso em 03 de novembro 2012.