UNIVERSIDADE REGIONAL DE BLUMENAU

CENTRO DE CIÊNCIAS EXATAS E NATURAIS

CURSO DE SISTEMAS DE INFORMAÇÃO – BACHARELADO

VALIDADOR DE TRANSAÇÕES COMERCIAIS E GERENCIADOR FINANCEIRO PARA DISPOSITIVOS MÓVEIS

ANDERSON ZOZ

BLUMENAU
2010

2010/1-02

ANDERSON ZOZ

VALIDADOR DE TRANSAÇÕES COMERCIAIS E GERENCIADOR FINANCEIRO PARA DISPOSITIVOS MÓVEIS

Trabalho de Conclusão de Curso submetido à Universidade Regional de Blumenau para a obtenção dos créditos na disciplina Trabalho de Conclusão de Curso II do curso de Sistemas de Informação— Bacharelado.

Prof. Francisco Adell Péricas, Mestre - Orientador

BLUMENAU
2010

2010/1-02

VALIDADOR DE TRANSAÇÕES COMERCIAIS E GERENCIADOR FINANCEIRO PARA DISPOSITIVOS MÓVEIS

Por

ANDERSON ZOZ

Trabalho aprovado para obtenção dos créditos na disciplina de Trabalho de Conclusão de Curso II, pela banca examinadora formada por:

Presidente:	Prof. Francisco Adell Péricas Mestre – Orientador, FURB
Membro:	Prof. Paulo Fernando da Silva, Mestre – FURB
Membro:	Prof. Ricardo Alencar de Azambuja, Mestre – FURB

Blumenau, dia 8 de julho de 2010

Dedico este trabalho a todos os membros da minha família, especialmente aqueles que me incentivaram na realização deste.

AGRADECIMENTOS

A Deus, pelo seu imenso amor e graça.

À meus pais, que mesmo longe, sempre estão presentes incentivando minhas conquistas.

Aos meus irmãos, pela confiança e apoio.

A minha namorada, Alessandra Kath, que sempre compreensiva e dedicada, acompanhou cada passo desta caminhada.

Ao meu orientador, Francisco Adell Péricas, por ter motivado a conclusão deste projeto.

Vencer não é nada, se não se teve muito trabalho; fracassar não é nada se se fez o melhor possível.

Nadia Boulanger

RESUMO

Este trabalho apresenta uma nova tendência aos usuários, onde se busca oferecer recursos similares ao do cartão magnético, porem utilizando um dispositivo móvel, obtendo ganhos em segurança, mobilidade e agilidade no processo. As aplicações foram desenvolvidas em linguagem C# utilizando banco de dados *MySQL* e foram publicados na internet o *website* e um w*ebservice* que interagem com os aplicativos desenvolvidos para operadores de caixas e usuário móveis. Todo processo utiliza um conceito avançado de criptografia e Certificados Digitais, o que mostra como aplicar estes recursos em uma rede aberta como a internet.

Palavras-chave: Criptografia. Aplicativo móvel. Gerenciamento financeiro.

ABSTRACT

This project presents a new trend for users, where it tries to offer similar features to the magnetic card, but using a mobile device, achieving gains in safety, mobility and agility in the process. The applications were developed in C# using MySQL database and were published on the internet a *website* and a w*ebservice* that interact with the applications developed for cashiers and mobile users. Every process uses an advanced concept of cryptography and digital certificates, which shows how to apply these resources in an open network like the Internet.

Key-words: Encryption. Mobile application. Financial management.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE SIGLAS

3D - Três dimensões

3G - Terceira geração da internet para dispositivo móvel

DES - *Data Encryption Standard* (Criptografia de dados padrão)

DLL - *Dynamic-link library* (Biblioteca de ligação dinâmica)

ECF – Emisso de Cupom Fiscal

GPS - *Global Positioning System* (Sistema Global de Posicionamento)

PAF - Programa Aplicativo Fiscal

PC - Computador Pessoal

PDA - *Personal Data Assistent* (Assistente pessoal de dados)

PIN - *Personal Identification Number* (Número de Identificação Pessoal)

RSA - Ronald **R**ivest, Adi **S**hamir e Leonard **A**dleman

RSS - *Really Simple Syndication* (Conteúdo Realmente Simples)

SET - *Secure Electronic Transaction* (Transações Eletrônicas Seguras)

SO - Sistema Operacional

SSL - *Secure Sockets Layer* (Protocolo de Camada de Sockets Segura)

SUMÁRIO

1 INTRODUÇÃO

As transações financeiras por meio eletrônico facilitam cada vez mais o dia-a-dia das pessoas, oferecendo agilidade, mobilidade, reduzindo custos e trazendo segurança. Não satisfeito com as opções hoje oferecidas para realização de transações financeiras, identifica-se a possibilidade de inovar, trazendo uma nova alternativa, rompendo o vínculo do usuário com seus cartões magnéticos, *chip*[1], senhas sincronizadas, caixas eletrônicos e até mesmo o uso de computadores, tipo *desktop* ou *notebook*.

> A abordagem de dispositivos móveis (celulares e PDA's), nos remete aos equipamentos presentes no cotidiano das pessoas, que estão se tornando um único aparelho, com a finalidade de atender ao mercado em crescimento e constante, na busca da utilização de formas de comunicação seguras e de preferência on-line. (DALFOVO et al., 2003).

Com a utilização crescente de dispositivos móveis tornando-se cada vez mais populares, atingindo todas as classes sociais, identificou-se então um novo mercado, onde se reaproveita o dispositivo móvel, popular como o celular ou *smartphones*, e os agrega novas funcionalidades, como validar movimentações comerciais, substituindo o atual sistema de cartões magnéticos utilizados para creditar e debitar valores financeiros das contas, oferecidos hoje por bancos e parceiros bancários como Visa, MasterCard, Rede Shop.

O aplicativo aqui desenvolvido oferece o gerenciamento financeiro das contas, onde se permite que o usuário execute os principais serviços oferecidos neste ramo, como consulta de limite e um detalhamento da movimentação financeira.

Atualmente é cada vez mais comum as pessoas utilizarem cartões para efetuar suas compras, principalmente via internet. Com este crescimento na utilização de cartões, gera-se um maior fluxo de dados, aumentando o número de movimentações financeiras, onde se oferece ao usuário a possibilidade de analisar e gerenciar seus gastos para manter-se sempre atualizado sobre suas movimentações. Com isso, além de oferecer um sistema novo de autenticação, se oferece também um serviço capaz de gerenciar as transações de forma unificada e acessível, onde a qualquer momento, o usuário pode consultar seu extrato a partir de seu celular ou terminal *desktop*, tudo em tempo real.

Para estabelecer o funcionamento deste sistema e atender normas de segurança, utiliza-se o *Secure Electronic Transaction* (SET), um protocolo definido para transações em redes

[1] dispositivo eletrônico o que possui milhões de circuitos integrados.

abertas como a w*eb*, onde este utiliza assinaturas digitais para identificação de usuários e algoritmos de criptografia para garantir confidencialidade.

Adotando SET, tem-se como um dos principais ganhos a segurança, pois os dados são enviados diretamente para o emitente sem que o comerciante tenha acesso a eles (Sociedade dos usuários de Informática e Telecomunicações, 2009). Aplicado-se o SET em dispositivos móveis nota-se uma grande evolução no que diz respeito à segurança da informação, pois foi desenvolvido uma aplicação *web* e outra *mobile* que comunicam-se entre si, exigindo um alto nível de segurança atendidos pelo SET.

Este projeto atende os principais requisitos de segurança, e assim pode substituir todos os cartões que hoje ainda encontra-se em circulação, por aplicativos executados em dispositivos móveis, trazendo novas ferramentas para a sociedade, possibilitando benefícios como: ampliar a mobilidade de seus usuários, agilidade nas movimentações, conhecimento de todas as movimentações bem como histórico em tempo real e segurança da informação.

Observada a atual estrutura adotada por bancos, identifica-se uma deficiência para efetuar movimentações financeiras, onde o sistema resume-se em utilizar cartões magnéticos, que ainda para alguns bancos vêm acompanhados de outros mecanismos, como a sincronia de senhas ou *chip*, que se demonstra pouco usual. Como exemplo, tem-se o *Personal Identification Number* (PIN) que funciona de forma sincronizada com um servidor do banco, onde toda vez que o usuário utilizar o serviço bancário, deve informar o código apresentado no dispositivo naquele momento, pois seu código é alterado constantemente. Além disto, de tempos em tempos este código perde a sincronia, obrigando o usuário a sincronizar novamente para voltar a utilizar o serviço bancário.

Identificam-se também na sociedade algumas situações, inusitadas, quando se constata a necessidade de inovar e melhorar a qualidade de vida das pessoas evitando ação de indivíduos maliciosos.

> BLUMENAU - Ao fazer uma manutenção de rotina em um caixa eletrônico instalado no Supermercado Angeloni do Bairro da Velha, um funcionário da Caixa Econômica Federal encontrou dentro do terminal algo que não deveria estar lá: um notebook. Ao tentar acionar a polícia, o funcionário foi agredido e ameaçado por quatro homens, que fugiram em quatro motocicletas, levando o computador. A cena ocorreu ontem de manhã, de acordo com a Polícia Militar. Às 18h, o gerente do supermercado, Valmir Amorim Alves, informou não ter conhecimento sobre o caso. (JORNAL DE SANTA CATARINA, 2009).

Unificando as transações financeiras no celular, busca-se segurança tanto para o cliente quanto para o comerciante, pois evita que ambos transitem com dinheiro, realizando suas negociações somente entre as contas dos usuários, que por sua vez estão previamente

cadastradas e aprovadas, estabelecendo uma relação confiável entre os envolvidos em uma transação, possibilitando o rastreamento da mesma.

1.1 OBJETIVOS DO TRABALHO

O objetivo deste trabalho foi o de construir um aplicativo para dispositivo móvel que estabeleça comunicação segura com um *webservice*, para assim validar e gerenciar movimentações financeiras.

Os objetivos específicos do trabalho:

a) desenvolver um *webservice* para validar e gerenciar movimentações financeiras;
b) criar um aplicativo para dispositivo móvel que estabeleça comunicação segura com o *webservice* utilizando rede aberta;
c) criar um aplicativo de integração com terceiros que estabelece comunicação segura com o *webservice* utilizando rede aberta;
d) aplicar o protocolo SET para comunicação do *webservice* com os dispositivos móveis;
e) criar um *website* possibilitando a consulta de limite e extrato, bem como opções para gerenciamento da conta.

1.2 ESTRUTURA DO TRABALHO

Este trabalho está disposto em quatro capítulos.

No primeiro capítulo apresenta-se a introdução, os objetivos e a estrutura do trabalho.

No segundo capítulo tem-se a fundamentação teórica, destacando-se os conceitos de cada elemento envolvido neste processo, com ênfase em criptografia da informação bem como trabalhos correlatos.

No terceiro capítulo é apresentado o desenvolvimento do aplicativo, incluindo detalhes sobre a especificação, implementação e tecnologia utilizada.

No quarto capítulo apresenta-se a conclusão sobre o trabalho, enfatizando os objetivos alcançados, bem como sugestões para trabalhos futuros como extensão deste.

2 FUNDAMENTAÇÃO TEÓRICA

Atualmente, as pessoas buscam em seu dia-dia maior facilidade, agilidade e segurança quando trata-se de movimentações financeiras. Analisando o cotidiano em um modo geral nota-se que as pessoas estão cada vez mais vulneráveis à ação de indivíduos maliciosos, onde constantemente sabe-se de cartões clonados, ou que alguém foi assaltado depois de sacar dinheiro em caixas eletrônicos. Na tentativa de sanar este problema, sugere-se que as pessoas adotem outros processos para efetuar uma movimentação financeira. Olhando as opções hoje oferecidas, a alternativa mais comum e confiável é a utilização dos cartões magnéticos, porém, decorrente de muitos problemas que este já apresentou, identifica-se a necessidade de trazer algo novo, diferente, acessível e prático, acompanhando esta constante evolução que é o cotidiano das pessoas. Com isso chega-se ao dispositivo móvel que está revolucionando nossas vidas e agora oferece uma nova funcionalidade em seu conjunto de ferramentas, assim trazendo segurança, pois todas as informações que antes poderiam ser facilmente acessadas pelo comerciante, que permite a clonagem de cartões, agora é eliminada, pois todos os dados passam a ser enviadas diretamente ao *webservice*, o que dificulta a ação do comerciante malicioso, além de tratar todas as camadas de segurança estabelecidas no SET o que deixa tão seguro ou até mais seguro que o aplicado no cartão magnético.

Neste capítulo são abordados detalhes de cada componente utilizado para oferecer melhor compreensão da solução apresentada.

2.1 DISPOSITIVOS MÓVEIS

Os dispositivos móveis popularmente conhecidos como celulares, s*martphone*, *Personal Data Assistent* (PDA) estão cada vez mais populares, evoluindo constantemente e oferecendo novas funcionalidades, tornando-se verdadeiros “computadores de bolso”, pois dispõem de recursos antes somente encontrados nos computadores pessoais (PC).

Dentre seus recursos mais recentes, pode-se evidenciar que sua conectividade permite a troca de dados utilizando a internet, que amplia as possibilidades no desenvolvimento de novas aplicações agregando mais valor ao dispositivo móvel.

Segundo Duprat (2010), a banda larga móvel 3G ampliou o acesso de camadas da população que hoje não têm oportunidade de conectar-se à Internet, por exemplo, em áreas rurais e remotas onde o cabeamento não consegue chegar. A banda larga móvel é a principal solução para estas pessoas, utilizando celulares e *smatphones* com a tecnologia agregada.

> Ler e receber e-mails, navegar em redes sociais, conferir um vídeo no YouTube e ouvir músicas são algumas atividades típicas de usuários da internet. A novidade é que ninguém mais precisa de PC para isso. Os smartphones, que chegaram com força ao mercado brasileiro esse ano, irão se popularizar ainda mais em 2010. (RIGUES, 2009).

Nota-se no mercado atual, um, significativo investimento das empresas nesta área, pois existem à disposição vários aplicativos desenvolvidos para dispositivos móveis, como jogos em três dimensões (3D), gerenciador de arquivos, navegadores para internet, aplicativos que emulam um roteador, TV, acesso a mapas com *Global Positioning System* (GPS) entre outros.

Segundo Lafloufa (2010), para evitar queda de sua parcela do mercado ameaçada pela presença de iPhones e pela chegada dos iPads, a Sony está planejando desenvolver um novo dispositivo móvel, que combinaria as funções de *smartphone*, PSP, *netbook* e *eReader*.

Observa-se que, a evolução está acontecendo e as empresas estão cada vez mais empenhadas em seus investimentos, rompendo paradigmas e mudando o mercado, a ponto de gerar fusões entre gigantes.

Com um mercado competitivo, pode-se aguardar grandes evoluções tecnológicas fluindo bem rapidamente, aliadas com preços cada vez mais acessíveis, oferecendo ganhos ao consumidor.

Segundo o site IDGNOW (2010), a Google está trabalhando com empresas como Intel e Sony, entre outras, para o lançamento da Google TV. Seu objetivo é, além de rodar aplicativos desenvolvidos inicialmente para os celulares, a TV com *Android* permitirá navegar na Internet, com acesso a serviços de rede sociais como *Twitter* e sites de fotos como o *Picasa*, apenas pressionando o controle remoto.

> E o que você ganha com um smartphone? Simples: mais produtividade e diversão. Na área profissional, os smartphones permitem checar e responder mensagens com mais facilidade e muitos deles são compatíveis com o sistema de e-mail Exchange, usado em empresas. Além disso, dá para navegar na web com boa velocidade e usar recursos de GPS e mapas, importantes para quem trabalha na rua. (RIGUES, 2009).

Constatada a evolução das tecnologias, que agregam novos valores aos dispositivos móveis em conseqüência de grandes investimentos por parte das empresas, notou-se um maior número de usuários, seja ele empresa ou não, na contratação de pacotes de acesso a internet, sustentando a tecnologia *web* para celular e viabilizando a inserção deste aplicativo no mercado tornando-o ainda mais popular.

Na Figura 1 pode-se observar um emulador de *Smartphone* que possui o Sistema Operacional Windows Mobile.

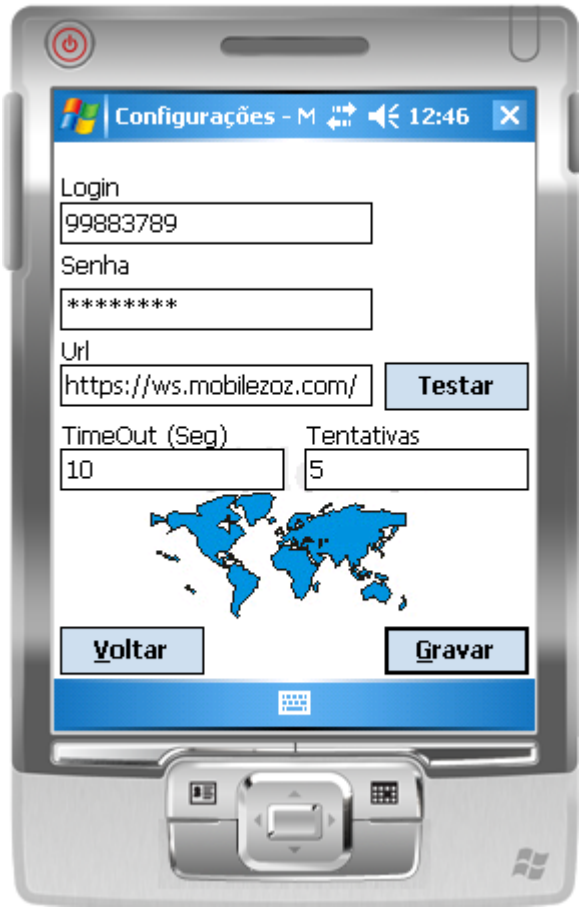

Figura 1 – *Smartphone* rodando MobileZoz.exe

2.1.1 SISTEMAS OPERACIONAIS PARA DISPOSITIVOS MÓVEIS

Com a evolução tecnológica dos dispositivos móveis composto por processadores mais velozes, identifica-se um elemento muito relevante, o Sistema Operacional (SO). Este elemento é composto por um conjunto de programas que inicializam o *hardware*, é ele quem controla todos os recursos do equipamento como *wireless*[2], *bluetooth*[3], terceira geração da

[2] rede sem fio de longo alcance.
[3] rede sem fio de curto alcance.

internet (3G), câmera, criação e execução de vídeos, *touchscreen*[4], GPS entre outros recursos encontrados nestes dispositivos.

Todo dispositivo móvel, seja ele da marca Nokia, HTC, Apple, LG, Samsung e outros possui um *software* conhecido como Sistema Operacional (SO). Alguns como o caso da Apple desenvolveram seu próprio SO, porém outros como HTC por não focalizar no desenvolvimento de SO, buscam parcerias com terceiros, neste caso com a Microsoft utilizando *Windows Mobile* na maioria de seus aparelhos. Esta parceria de empresas especializadas em *hardware* com outra de *software* é boa, pois estimula a concorrência e a evolução desta tecnologia fazendo com que a mesma desenvolva mais rapidamente e reduzindo custos.

Na Tabela 1 observam-se as principais características existentes nos principais Sistemas Operacionais, bem como seus diferenciais em recursos tecnológicos.

Tabela 1– Comparativo em Sistemas Operacionais

							
	iPhone OS 4.x	**iPhone OS 3.x**	**Windows Phone 7**	**Windows Mobile 6.5**	**Android 2.x**	**Palm Web OS 1.x**	**BlackBerrry OS 5**
Lançamento	4° bimestre de 2010	Junho de 2009	4° bimestre de 2010	Novembro de 2009	Outubro de 2010	Junho de 2009	Novembro de 2009
Kernel	Os X Mobile	Os X Mobile	Windows CE	Windows CE	Linux	Linux	Proprietário
Escrito em	C/C++/ Objective-C	C/C++/ Objective-C	C++	C++’	C	C	C++
Open Source/Gratuito?	Não	Não	Não	Não	Sim	Não	Não
Disponível para múltiplos fabricantes	Não	Não	Sim	Sim	Sim	Não	Não
MultiTarefa	Sim (apenas 3G)	Não	Não (com exceções)	Sim	Sim	Sim	Sim
Interface MultiTouch	Sim	Sim	Sim	Não	Sim	Sim	Não
Navegador WEB	Mobile Safari	Mobile Safari	Internet Explorer	Internet Explorer	Chrome	WebOS Browser	BlackBerry Browser
Núcleo do navegador	Safari/ WebKit	Safari/ WebKit	IE/Trident	IE/Trident	Android/ WebKit	WebOS/ WebKit	BB (WebKit em breve)
Grava Videos	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Wi-Fi	Depende da operadora	Depende da operadora	Sim	Sim	Sim	Sim	Sim
Upgrades	Sincronização / Pacotes	Sincronização / Pacotes	Sincronização / Pacotes	Sincronização / Pacotes	OnLine	OnLine	Sincronização / Pacotes
Permite Apps não oficiais	Não	Não	Talvez	Sim	Sim	Talvez	Sim
Suite Office	Apps como QuickOffice	Apps como QuickOffice	MS Office 2010 Mobile	MS Office 2010 Mobile	Google Docs	Apenas Visualizador	Apenas Visualizador

[4] tela sensível à toque.

Analisando a tabela 1 pode-se entender melhor o que cada SO oferece possibilitando uma analise para se encontrar o que melhor se adeque às necessidades de cada usuário.

2.1.2 NAVEGADOR PARA DISPOSITIVEL MÓVEL

Trabalhando com Sistema Operacional, os navegadores são responsáveis por acessar e interpretar as páginas publicadas na internet. Este elemento é muito importante nos dispositivos móveis, porém ainda possui muitas limitações, o que não oferece muita segurança ou agilidade se comparada aos navegadores criados para PC.

Segundo levantamento realizado por Martin (2008), pode-se entender algumas destas limitações encontradas nos navegadores criados para dispositivos móveis:

a) Nokia Browse: o navegador pode ser configurado para abrir sempre na mesma página ou em uma central de favoritos, chamada Marcadores, grava os endereços visitados, e oferece suporte *Really Simple Syndication* (RSS). A navegação com zoom é controlada pelo navegador que permite bloquear *pop-ups*[5] e apagar dados de privacidade de navegação (histórico, *cookies*[6], *cache*[7] e dados de formulários e senhas) além de permitir trabalhar com múltiplas janelas abertas. Como ponto negativo pode-se apontar o não suporte nativo a Flash, este seria melhor se possuísse mais atalhos para navegação e não usa abas para controlar as páginas abertas;

b) Safari: programa abre cada site em janelas individuais. Um botão na parte inferior do navegador indica quantas estão abertas e dá acesso rápido a elas. O *Safari* tem um bom gerenciamento de histórico e de favoritos, mas não lê RSS, como sua versão desktop. Não é compatível com Flash, barrando a navegação em inúmeros sites (menos o *YouTube*, que tem um aplicativo). Como ponto negativo, pode-se apontar a falta de suporte à tecnologia Adobe Flash e não tem leitor de RSS;

[5] pequenas janelas que se abrem automaticamente na sua tela.
[6] arquivos gravados em seu computador de modo que eles mantenham algumas preferências gravadas.
[7] dispositivo de acesso rápido, interno a um sistema.

c) Internet Explorer: quebra a formatação das páginas, transformando cada coluna em uma fileira enorme para rolagem. Não roda *Flash*, não funciona com o *YouTube*, não tem leitor de RSS;
d) Opera Mobile 9.5: não tem atalho para o zoom na tela, não quebra texto para largura da tela e tamanho mínimo da fonte, não abre links com um toque apenas, é preciso pressionar o link por alguns segundos, para então aparecer um menu contextual e conseguir abrir em uma nova aba. Seu ponto positivo é que pode ser baixado para qualquer celular ou *handheld* com *Windows Mobile*, diferente dos demais navegadores. Como ponto negativo, pode-se apontar navegação confusa e modo de visualização em celular que quebra as páginas.

Além destas limitações questões como segurança na utilização de um navegador ainda é algo crítico, não oferecendo suporte para aplicações seguras desenvolvidas para w*eb*.

2.2 PROGRAMA APLICATIVO FISCAL - PAF

Programa Aplicativo Fiscal (PAF) é o programa, que realiza a comunicação com o equipamento Emissor de Cupom Fiscal (ECF) obrigatório em todo comércio varejista, a nomenclatura PAF, surgiu com a unificação de regras que antes era específica de cada estado e agora é padronizada, sendo requisito obrigatório ou não por cada estado, porem oferecendo melhor segurança no controle para Fisco.

> Durante muito tempo cada Estado determinava as normas e regras a serem aplicadas sobre tal aplicativo. Visando centralizar e extinguir essas diferentes normas e regras exigidas pelos diferentes estados sobre o Programa Aplicativo Fiscal, foi publicado pelo fisco o Convênio ICMS 15/08 e o Ato COTEPE 06/08 de âmbito nacional onde é determinado que todo Programa Aplicativo Fiscal deve passar por uma Análise Funcional em um órgão técnico credenciado para que o mesmo possa ser utilizado no varejo. De posse do laudo da análise funcional a Software House deverá cadastrar a versão aprovada do programa aplicativo nos estados onde deseja atuar. Vale ressaltar que alguns estados podem não exigir tal análise. Notamos esta tendência nos estados de São Paulo e Mato Grosso. (Gestão, 2010).

O PAF é responsável por integrar sistemas frente de caixa com finalizadoras de terceiros que é o caso da Visa, MasterCard, etc.

2.3 SECURE ELECTRONIC TRANSACTION - SET

No dia 1° de fevereiro de 1996, a Visa e a MasterCard anunciam juntamente com Microsoft, IBM, Netscape, SAIC, GTE, RSA, Sistemas Terisa e VeriSign o desenvolvimento de normas técnicas para salvaguardar informações sigilosas utilizadas em transações financeiras realizadas em redes abertas. Esta norma foi chamada de *Secure Electronic Transaction* (SET).

Em dezembro de 1997, uma nova entidade empresarial foi formada pelo Visa e MasterCard para melhorar esta estrutura que definiu o protocolo SET, bem como outras funções essenciais que são necessárias para apoiar a implementação desta norma.

> O SET é a especificação de um protocolo destinado a oferecer segurança em transações de pagamento, bem como autenticar todas as partes envolvidas nessa transação, em qualquer tipo de rede. A especificação foi criada com a finalidade de fornecer a confiança necessária para que os consumidores e comerciantes sintam-se seguros em usar seus cartões de pagamento na Internet. Com base em estudos da especificação, esta sendo desenvolvida uma ferramenta para a certificação digital, cujo objetivo é oferecer aos seus usuários maior segurança. (JAKOBSEN, 2000).

O protocolo especifica como cada processo deve ocorrer, tendo como destaque o uso constante de criptografia, garantindo a confidencialidade da informação, impedindo que terceiros interpretem a informação. SET também tem como requisito básico para sua aplicação a utilização de certificados digitais que garantem a autenticidade de cada usuário. Outra grande vantagem encontrada no SET é que as informações não podem ser trocadas entre usuários, ou seja, toda a informação que chega ao servidor *webservice* é processada e autenticada ocorrendo a interação somente cliente-servidor.

> SET assegura ao dono do cartão que as informações de seu pagamento são mantidas seguras e que só podem ser acessadas pelo destinatário desejado. SET cifra as mensagens para garantir confidenciabilidade das informações. A especificação precisa garantir que o conteúdo das mensagens não é alterado durante as transmissões entre emissor e receptor. SET provê assinaturas digitais, que garantem a integridade da informação de pagamento. (PETRY, 2010).

O protocolo SET oferece três vantagens principais, que juntos mostram-se extremamente seguras. Estas vantagens são:

a) privacidade: através de criptografia que torna as mensagens, se interceptada, ilegíveis, pois utiliza algoritmos de Criptografia DES e RSA de forma conjunta;
b) integridade: utilizando hash e assinatura digital, garante-se que as mensagens enviadas são recebidas sem alteração;

c) autenticação: através de certificados garante-se que as partes envolvidas na transação são quem dizem ser.

2.3.1 PROCESSO DE PAGAMENTO UTILIZANDO SET

O processo do SET desenvolvido para cartões de crédito que utilizam o modelo descrito na Figura 2.

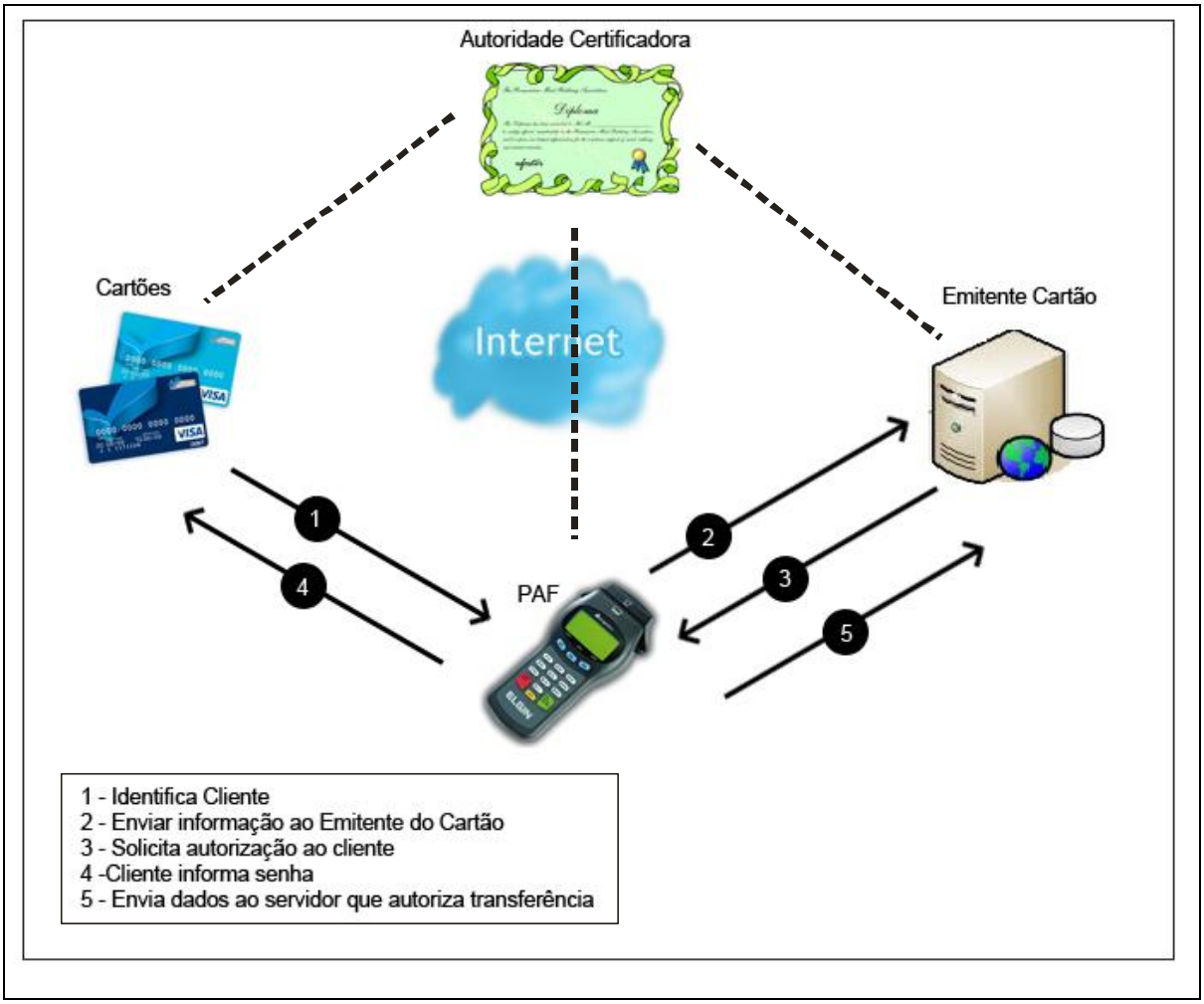

Figura 2 – Processo de pagamento utilizando SET tradicional

Quando utilizado o protocolo tradicional, a seqüência ocorre com a dependência do equipamento instalado no comerciante para validar e transação.

Como observa-se na figura 2, o processo inicia quando o cliente passa seu cartão magnético no leitor ligado ao PAF, esta informação segue com protocolos SET para o emitente cartão utilizando a internet, o mesmo identifica o cliente solicitando a senha de

autorização, esta é informa pelo cliente e enviada para o emitente cartão, que valida a movimentação, assim finalizando o processo.

2.3.2 PROCESSOS UTILIZADOS PARA APLICAÇÃO DO SET

Neste tópico busca-se conhecer cada elemento utilizado pelo SET, visando simplificar o entendimento de sua aplicação.

2.3.2.1 Data Encryption Standard - DES

O algoritmo de criptografia DES foi desenvolvido na década de 70 pelo National Bureau of Standarts em parceria com National Security Agency. O projeto era desenvolver um método padrão para proteção de dados. A IBM criou o primeiro algoritmo de criptografia, chamando-o de LUCIFER. O DES tornou-se oficialmente norma federal americana em novembro de 1976.

Segundo Muniz (1999), DES realiza somente duas operações sobre sua entrada: deslocamento de bits e substituição de bits. A chave controla exatamente como esse processo ocorre. Ao fazer estas operações repetidas vezes e de uma maneira não-linear, chega-se a um resultado que não pode ser revertida a entrada original sem o uso da chave.

DES possuir o poder de criptografar dados, entretanto este já não é um método seguro, podendo ser facilmente quebrada, por isso optou-se em utilizar o TripleDES que consistem em utilizar 3 vezes DES,

> Ao contrário do que se imagina, o 3DES não demora "apenas" o triplo do tempo que é necessário para o DES ser quebrado, já que se você utiliza três chaves (uma para cada passagem do DES), você terá que descobrir qual é cada uma das três chaves e para descobrir uma das chaves você precisará de descobrir a anterior. E como você nunca terá uma maneira de saber se a primeira chave está certa ou errada (a única maneira de saber se as chaves estão corretas é inserir todas as três na ordem certa e ver que o texto gerado é o correto. Então se você acertar duas chaves e errar a última, nunca saberá que acertou as duas primeiras). (SPOT, 2008).

2.3.2.2 RSA

Um dos algoritmos mais seguros de encriptação de informações atuais originou-se dos estudos de Ronald Rivest, Adi Shamir e Leonard Adleman, o RSA, sigla que representa a primeira letra de cada sobrenome de seus criadores.

> O princípio do algoritmo é construir chaves públicas e privadas utilizando números primos. Uma chave é uma informação restrita que controla toda a operação dos algoritmos de criptografia. No processo de codificação uma chave é quem dita a transformação do texto puro (original) em um texto criptografado. Chave Privada: É uma informação pessoal que permanece em posse da pessoa - não publicável. Chave Pública: Informação associada a uma pessoa que é distribuída a todos. (DARLEN, 2007).

2.3.2.3 Assinatura digital – *HASH*

A assinatura digital é um mecanismo criado para identificar se realmente uma informação partiu de um determinado usuário e que esta não sofreu alterações em sua trajetória, este algoritmo tem como característica criar um par de chaves, cifrar com uma chave-pública e decifrar com a chave-privada ou realizar a cifra com uma chave-privada e decifração com uma chave-pública. Obviamente esta forma não assegura o sigilo da mensagem.

> Usualmente, face à ineficiência computacional dos algoritmos simétricos, os métodos para assinatura digital empregados na prática não assinam o documento que se deseja autenticar em si, mas uma súmula deste, obtida pelo seu processamento através do que se denomina uma *função de Hashing*. Uma função de *hashing* é uma função criptográfica que gera uma saída de tamanho fixo (geralmente 128 a 256 bits) independentemente do tamanho da entrada. A esta saída se denomina de *hash* da mensagem (GUILHERME, 2003).

Aplicando algoritmo *Hash*, pode-se validar uma assinatura comparando os resultados da mensagem enviada com a processada localmente, onde, se estas forem idênticas, subentende-se que seu conteúdo manteve-se original.

2.3.2.4 Certificado digital

Conforme Guilherme (2003), um certificado digital nada mais é que um documento eletrônico contendo a chave pública de um usuário e dados de identificação do mesmo. Este

documento deve ser assinado por uma *autoridade confiável*, a Autoridade Certificadora, atestando sua integridade e origem. Usualmente, certificados digitais são utilizados para garantir a integridade e origem de chaves públicas depositadas em bases de dados de acesso público.

2.4 APLICANDO PROTOCOLO SET

Neste seção ver-se-á como aplicar cada elemento descrito acima nas mensagens trocadas em nossos aplicativos.

2.4.1 PRIVACIDADE

O protocolo SET realiza a combinação dos algoritmos DES com RSA, onde utiliza-se uma chave aleatória para gerar a chave do algoritmo de criptografia DES que realizar a cifra da mensagem, em seguida, utiliza-se a chave pública do algoritmo RSA para cifrar a chave aleatória utilizada em DES, garantindo a privacidade da informação, pois caso a mensagem seja interceptada não poderá ser decriptografada.

Na Figura 3 pode-se observar como a junção do algoritmo de criptografia está aplicada no SET.

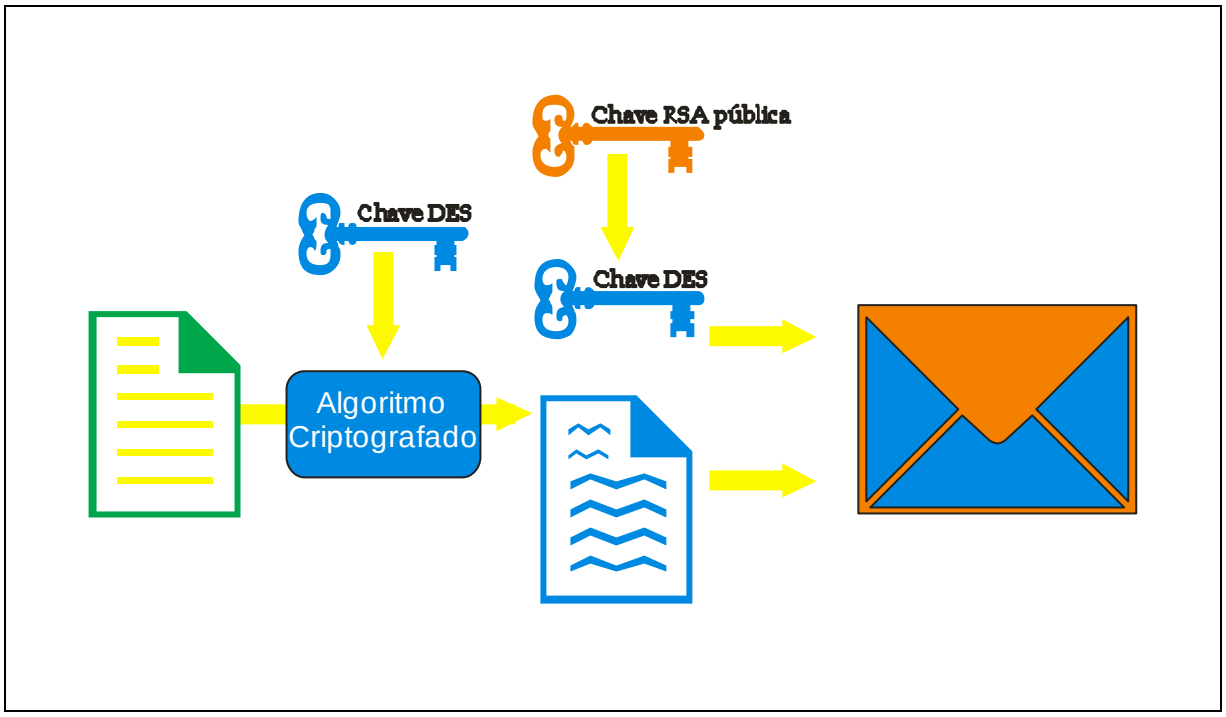

Figura 3 – Criptografia no protocolo SET

Na figura 3 observa-se que qualquer texto pode ser criptografado, onde ao receber esta informação, aplica-se sobre ela a criptografia DES, utilizando uma chave pública, gerada em tempo de execução, feito isso, pega-se a chave gerada e criptogra-se utilizando algoritmo RSA, utilizando sua chave pública, após executado este processo montamos então o envelope que contem os dados criptografados com DES e a chave DES que está criptografada com RSA, tornando-o inelegível se interceptado, podendo ser aberto e interpretado apenas por quem possuir sua chave privada do RSA.

2.4.2 INTEGRIDADE

Conforme na figura 3, utiliza-se a assinatura digital para verificar se as informações não sofreram alteração desde o processo original. Para isso utiliza-se a função *hash* para assinar a mensagem, onde esta informação, quando reprocessada por seu receptor, possa ser verificada e validada. Pode-se observar na Figura 4 como ocorre esta validação.

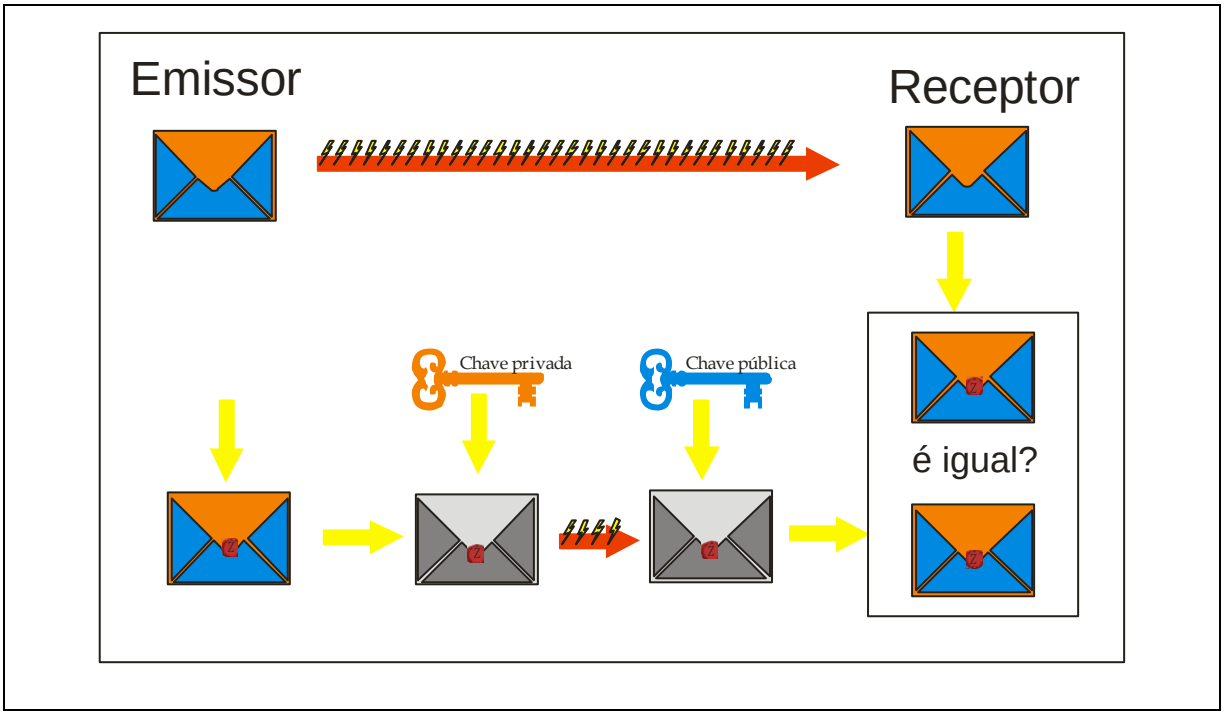

Figura 4 – Processo de validação da assinatura digital.

Na figura 4 pode-se entender o funcionamento da assinatura digital, onde os dados a serem transmitidos passando pelo algoritmo de *Hash* que é enviado do emissor para o receptor, esta informação é armazenada para que posteriormente possamos comparar. Os dados originais gerados no emissor agora pode ser encriptado e enviado, quando o receptor recebe a mensagem e decriptografa deve recalcular o *Hash* e seu resultado é comparado com o *Hash* enviado anteriormente, assim garantindo que aquela informação não sofreu alterações em sua trajetória.

2.4.3 AUTENTICIDADE

O controle de certificados ocorre no servidor *webservice* ao qual foi publicado utilizando certificado *Secure Sockets Layer* (SSL) que realizará o gerenciamento e distribuição das chaves-públicas.

2.5 SEGURANÇA DO PROTOCOLO

Quando trata-se da segurança SET, há estudos que avaliam quanto tempo levaria para realizar a quebra de uma mensagem, onde pode-se ter noção do quanto este protocolo é forte justificando como depois de tanto tempo de sua criação ainda é muito utilizado.

> SET é projetado para ser usado com chaves de codificação-bit 1024, tornando-se uma das aplicações de criptografia mais forte de uso público. O tempo que seria necessário para quebrar a criptografia descrita aqui, especialmente com todos os diferentes níveis de criptografia que estão ocorrendo, é para cima para 2.800.000.000 anos, utilizando 100 computadores cada um com capacidade para processar 10 milhões de instruções por segundo. Mesmo assim, apenas uma única mensagem pode ser quebrada e com a mensagem seguinte, todo o processo teria de recomeçar. Embora possa parecer um exagero, o protocolo é bastante atraente para todos aqueles que desejam realizar negócios difundidos através da Internet, especialmente os emissores de cartões que têm mais a perder com a fraude.(WOLRATH, 1998, tradução nossa)

2.6 FECHAMENTO

Segundo Petry (2010), o protocolo SET foi desenvolvido tendo em vista evitar todos os problemas de segurança que o comércio eletrônico enfrentava. Assim, SET previne qualquer possível ataque ou erro. SET certifica todos os participantes do processo de compra on-line, de modo que os mesmos podem estar seguros de que estão tratando com entidades e consumidores legítimos.

2.7 TRABALHOS CORRELATOS

Verificou-se no mercado a MobileCard que disponibiliza uma ferramenta similar ao que se propõe neste trabalho.

> A MobileCard é uma empresa especializada em adquirência, captura e processamento de transações eletrônicas para dispositivos móveis. Nossos produtos e serviços contemplam uma variedade de soluções que permitem a completa

> integração dos mais variados meios de pagamentos e respectivos serviços aos atuais dispositivos móveis disponíveis no mercado. (MOBILECARD, 2009).

A MobileCard oferece serviços de débito próprio, porem diferenciando-se do que foi desenvolvido pela MobileZoz, a MobileCard oferece um serviço que realiza transações entre aparelhos celulares sem oferecer a integração com sistemas PAF como a Mobilezoz, outra grande diferença identifica-se na forma em que o serviço é oferecido, pois a empresa MobileCard oferece ao usuário a opção de débito, seu mecanismo ocorre como um cartão pré-pago, onde o cliente compra créditos e usa este limite até o fim tendo que recarregar para continuar a utilizar o serviço.

A MoileCard não possui convênio com as bandeiras como Visa, MasterCard, Rede Shop, nem com o sistema bancário brasileiro, onde o mesmo não demonstra interesse nesta parceria, trabalhando de forma independente.

O Banco do Brasil disponibiliza aos seus correntistas algumas das funcionalidades já citadas, mas é incompleto se comparado com o que está sendo desenvolvido neste projeto.

> No Banco do Brasil você pode realizar suas operações bancárias diretamente do celular, com comodidade e segurança. Estão disponíveis as operações de consultas de saldo e extrato; pagamento de títulos bancários e contas (água, energia, telefone, etc); transferências entre contas, DOC/TED; aplicações e resgates; recargas de celulares pré-pagos e empréstimos pessoais. Além destas operações você pode cadastrar seu celular para receber mensagens de texto informando sobre movimentações de conta-corrente e cartão de crédito. (BANCO DO BRASIL, 2009).

Utiliza-se neste trabalho a troca de informações criptografadas, onde se poderá analisar detalhes do projeto desenvolvido por Ramos (2004) em plataforma .NET, que contém informações relevantes ao desenvolvimento deste projeto.

> O protótipo deste trabalho é formado por dois aplicativos autônomos e um *Web Service*, onde o objetivo é realizar o cadastro de mensagens em um banco de dados no *desktop*, para futuramente serem carregadas em um dispositivo móvel (SmartPhone) através do *Web Service*. (RAMOS, 2004).

3 DESENVOLVIMENTO

Neste capítulo estão descritas as particularidades técnicas do sistema proposto, tais como a descrição do mesmo e a apresentação dos requisitos funcionais, não funcionais, diagrama dos principais casos de uso com sua descrição, diagrama de atividades, modelo conceitual de dados e principais *softwares* utilizados no desenvolvimento deste projeto.

3.1 LEVANTAMENTO DE INFORMAÇÕES

Com o crescimento na utilização dos serviços bancários, torna-se complicado gerenciar as movimentações financeiras, onde identifica-se a necessidade de oferecer uma nova opção para pessoas que constantemente fazem uso deste serviço, pois além do tradicional cartão de crédito, há agora uma tecnologia que traz segurança e mobilidade superando o atual sistema de cartões magnéticos.

Sendo assim, chega-se a um projeto pioneiro e inovador, oferecendo possibilidades ainda não utilizadas em grande escala para atender um novo mercado de usuários que procuram mobilidade, agilidade, facilidades e segurança em seu cotidiano, ao qual este projeto visa atender.

3.2 REQUISITOS

O Quadro 1 apresenta os requisitos funcionais a serem implementados nos aplicativos, componentes do sistema e sua rastreabilidade, ou seja, vinculação com o(s) caso(s) de uso associado(s).

Requisitos Funcionais	Caso de Uso
RF01: Cadastrar usuário	UC01
RF02: Cadastrar conta bancária	UC02
RF03: Efetuar login	UC03
RF04: Iniciar movimentação	UC04
RF05: Realizar a escolha de qual conta será o lançamento	UC05
RF06: Realizar a digitação de senha no dispositivo móvel	UC06
RF07: Permitir o cancelamento de uma solicitação	UC07
RF08: Permitir o bloqueio de comerciantes	UC08
RF09: Permitir o estorno de um lançamento	UC09
RF10: Consultar limite de crédito disponível	UC10
RF11: Consultar movimentações financeiras	UC11

Quadro 1 – Requisitos funcionais

O Quadro 2 lista os requisitos não funcionais aplicados neste projeto.

Requisitos Não Funcionais
RNF01: Deverá ser desenvolvido em .Net
RNF02: Deverá utilizar banco de dados MySQL
RNF03: Deverá seguir os padrões definidos no protocolo SET
RNF04: *Webservice* deverá ser publicado em um servidor que possui suporte .Net Framework 3.5 ou superior
RNF05: *Website* deverá ser publicado em um servidor que possui suporte .Net Framework 3.5 ou superior
RNF06: O dispositivo móvel deverá possuir suporte .Net Framework 2.0 ou superior
RNF07: A estação PAF-ECF[8] deve conectar-se a internet
RNF08: O dispositivo móvel deve conectar-se a internet

Quadro 2 – Requisitos não funcionais

[8] Programa Aplicativo Fiscal – Popularmente conhecido como programa frente de caixa.

3.3 ESPECIFICAÇÃO

Esta seção apresenta o(s) diagrama(s) que serão necessários para o entendimento do sistema. Para a modelagem de dados foi utilizado uma versão *student* do Enterprise Architect versão 7.5.845.

3.4 DIAGRAMAS DE CASO DE USO

Esta seção apresenta o diagrama de casos de uso aplicados no sistema. Seu detalhamento encontra-se descrito no Apêndice A.

Na Figura 5 observa-se o diagrama de casos de uso.

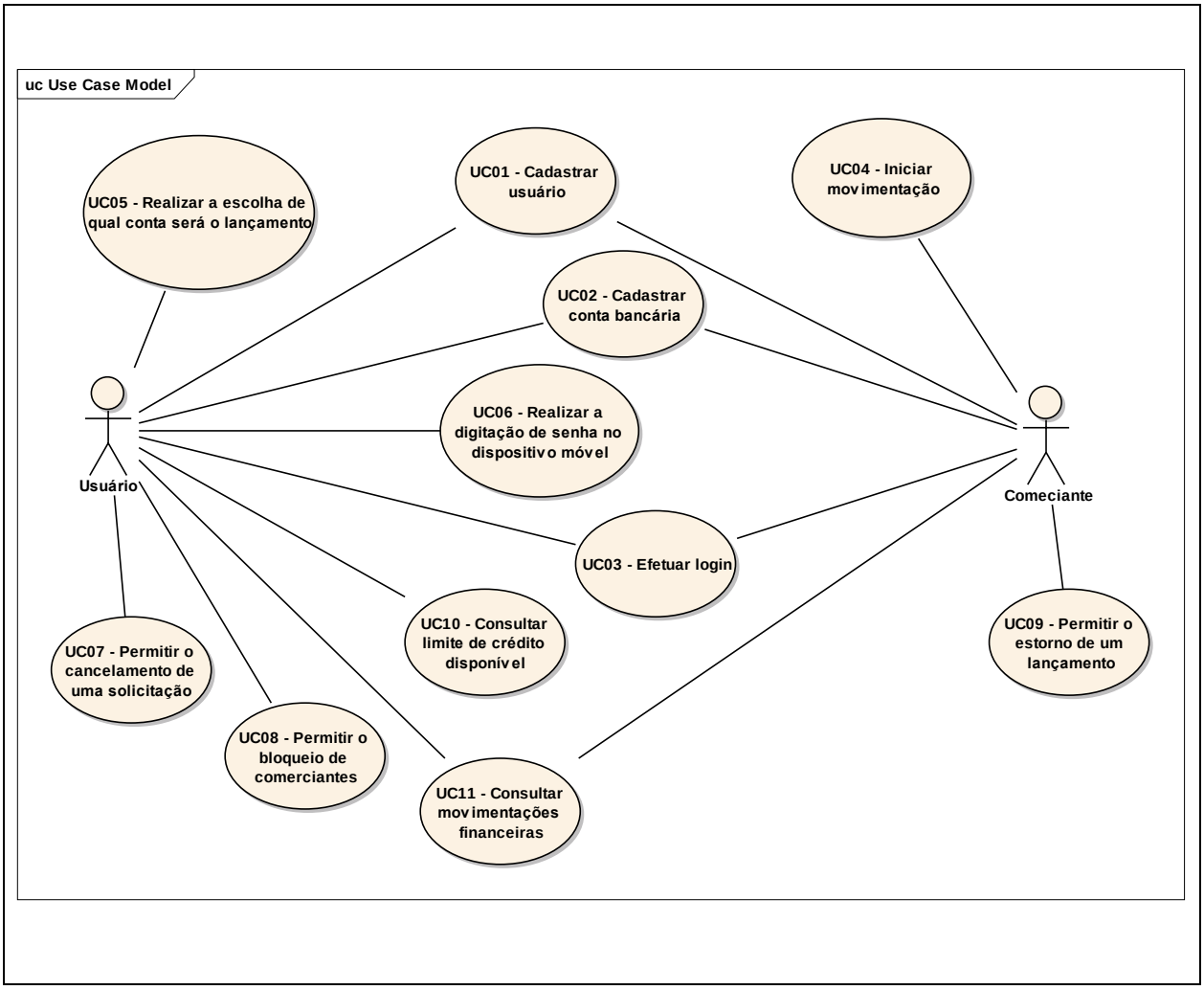

Figura 5 – Diagrama de caso de uso

Os casos de uso estão descritos a seguir:

a) UC01 – Cadastrar usuário – usuário efetua seu cadastramento no *website* para adquirir o acesso ao serviço MobileZoz;
b) UC02 – Cadastrar conta bancária – usuário informa dados das conta(s) bancária(s);
c) UC03 – Efetuar login – usuário efetua login no *website* assim obtendo acesso aos serviços específicos disponibilizados no site;
d) UC04 – Iniciar movimentação – comerciante inicia uma movimentação financeira;
e) UC05 – Realizar a escolha de qual conta será o lançamento – cliente quando possuir mais de uma conta bancária cadastradas, deverá indicar no aplicativo mobile em qual deseja registrar a movimentação;
f) UC06 – Realizar a digitação de senha no dispositivo móvel – cliente deverá informar sua senha para autenticar todas as movimentações;
g) UC07 – Permitir o cancelamento de uma solicitação – cliente tem a opção de cancelar uma determinada solicitação;
h) UC08 – Permitir o bloqueio de comerciantes – cliente tem a opção de bloquear um ou mais comerciantes, onde o comerciante a partir deste momento não conseguirá gerar novas movimentações para o cliente;
i) UC09 – Permitir o estorno de um lançamento – comerciante tem a opção de realizar o cancelamento de um movimento já aprovado pelo usuário no mesmo dia;
j) UC10 – Consultar limite de crédito disponível – cliente pode consultar via dispositivo móvel qual seu limite disponível em cada conta;
k) UC11 – Consultar movimentações financeiras – cliente pode consultar de forma detalhada suas movimentações financeiras através do dispositivo móvel bem como todo usuário acessa estas informações no *website*.

3.5 DIAGRAMAS DE ATIVIDADES

Na Figura 6 se apresenta o diagrama de atividades, que mostra o fluxo do principal processo executado no PAF.

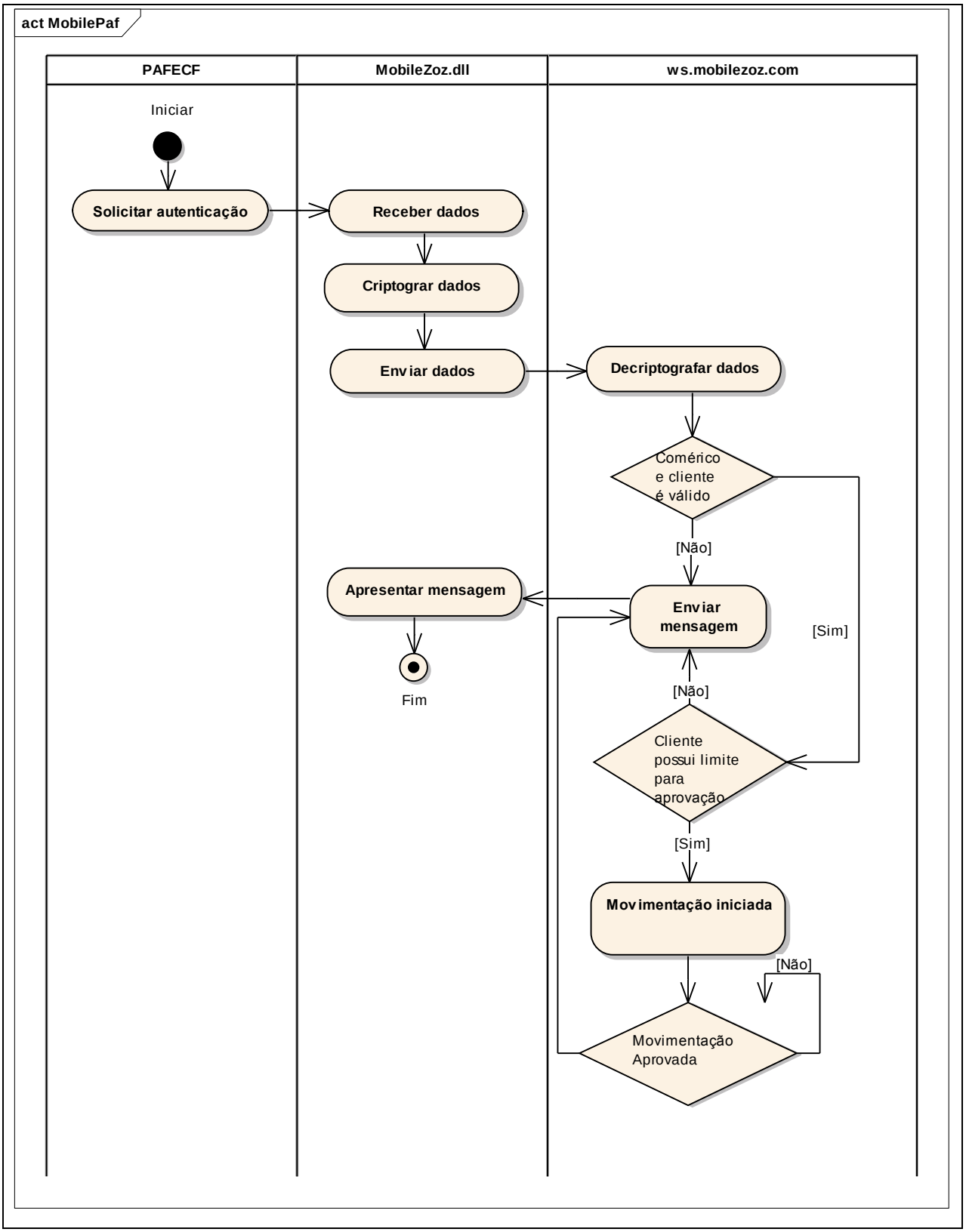

Figura 6 – Diagrama de Atividades no ponto de vista do comerciante

Na Figura 7 se apresenta o diagrama de atividades, que traz o fluxo do principal no processo executado no dispositivo móvel.

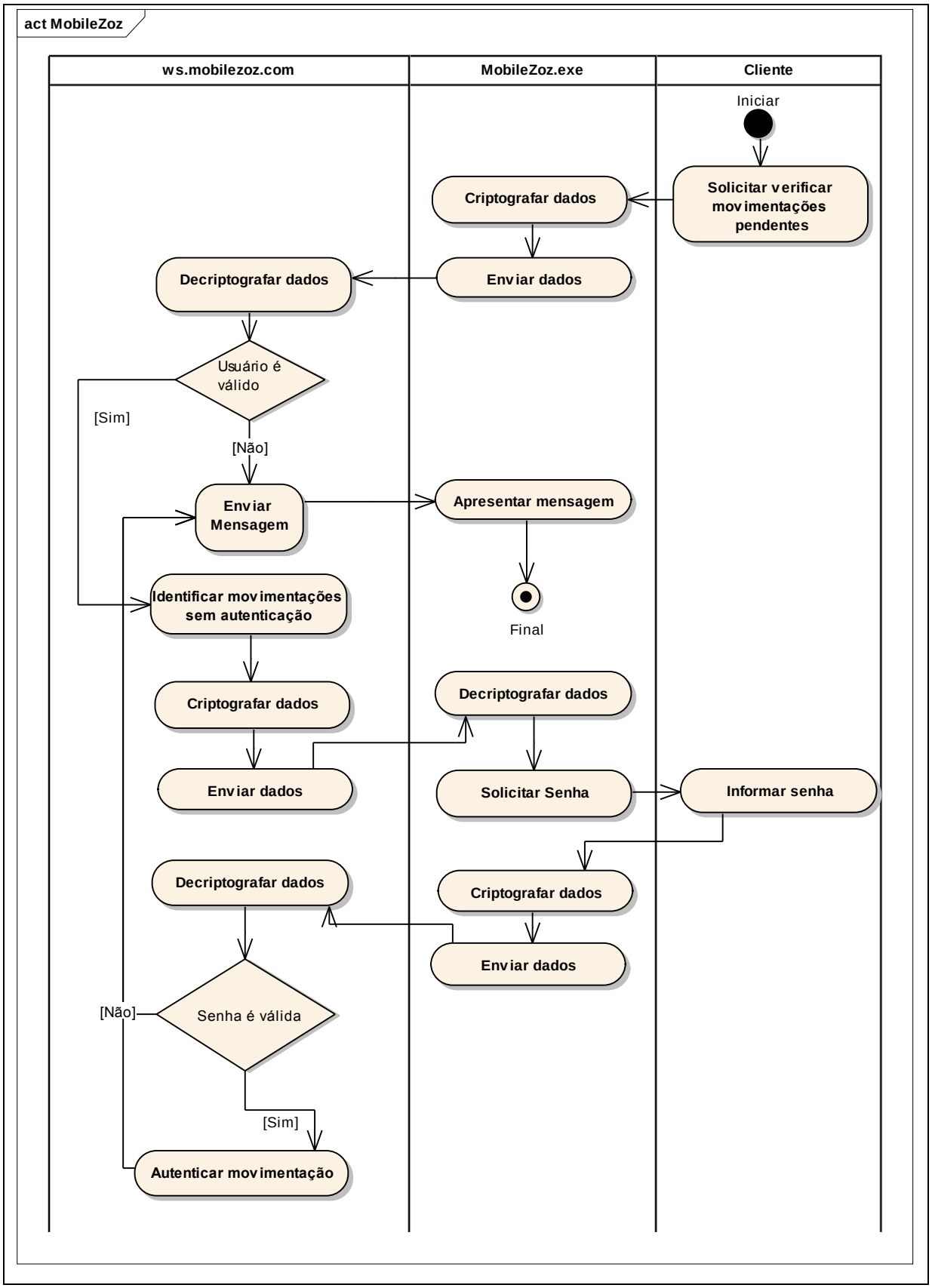

Figura 7 – Diagrama de Atividades no ponto de vista do cliente

3.6 MODELO CONCEITUAL DE DADOS

Na Figura 8 se apresenta o modelo conceitual de dados que representam as entidades que serão persistidas no banco de dados. Cada tabela de entidade é representada no banco de dados como uma tabela.

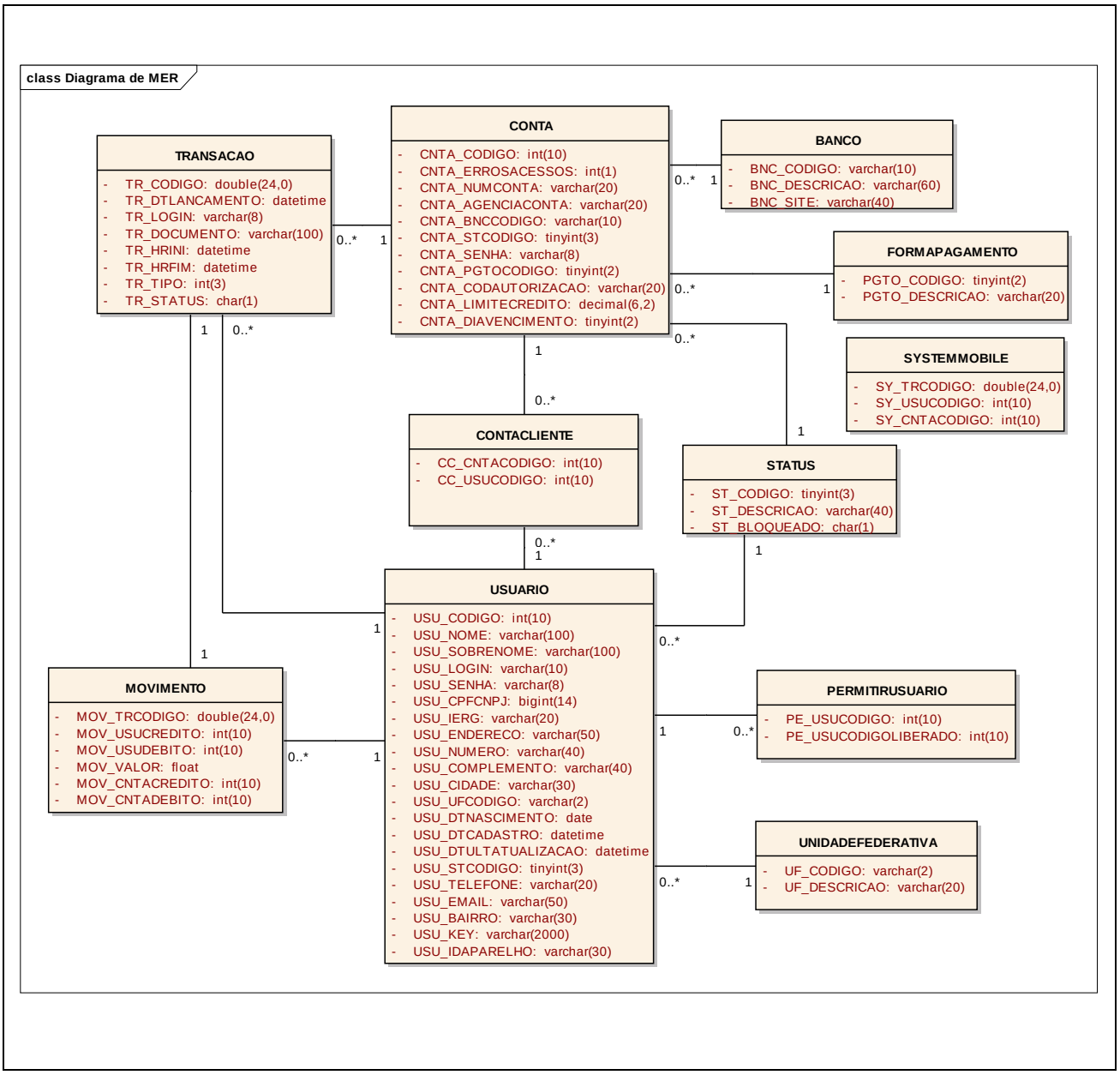

Figura 8 – Diagrama de MER

A descrição de cada tabela está a seguir:

a) tabela banco - tabela possui atributos referente a instituição financeira relacionada a conta;
b) tabela bloqueado - tabela possui atributos referente a comerciantes bloqueados por usuário;
c) tabela conta - tabela possui atributos referente a conta bancária do usuário;
d) tabela contacliente - tabela possui o atributos referente aos usuários e seu relacionando com as contas bancarias, mantêm também o identificador de cada usuário;
e) tabela formapagamento - tabela possui atributos referente as formas de pagamento oferecidas pela MobileZoz;
f) tabela movimento – tabela possui atributos referente a movimentação financeira;
g) tabela status - tabela possui atributos referente a status de cada conta ou usuário;
h) tabela systemmobile - tabela possui atributos referente controle do numero seqüencial na geração de chave usuários, contas e transações;
i) tabela transacao - tabela possui atributos referente a todas as principais operações realizadas no servidor, todas as movimentações e alguns eventos ficam armazenadas nesta tabela, mantendo um histórico de cada acesso;
j) tabela unidadefederativa - tabela possui atributos referente aos estados e suas siglas;
k) tabela usuario - tabela possui atributos referente a usuário vinculado a MobileZoz.

3.7 IMPLEMENTAÇÃO

Nesta seção estão apresentadas informações sobre as ferramentas utilizadas no trabalho.

3.8 COMPONENTE E FERRAMENTAS UTILIZADAS

Para a implementação do sistema utilizamos várias ferramentas dentre as principais:

a) Visual Studio 2008, versão: 9.0.21.22.8 RMT;
b) Windows Mobile Device Center, versão: 6.1.6965;
c) Microsoft Device Emulador, versão: V3 9.0.21022.8;
d) Connector MYSQL, versão: 6.2.2;
e) MYSQL, versão: 5.1;
f) HeidiSQL, versão: 5.0.0.3272;
g) Enterprise Architect, versão: 7.5.845.

3.9 APLICATIVOS DESENVOLVIDOS

O projeto está dividido em 4 (quatro) aplicativos, sendo eles, servidor w*ebservice*, o *website*, o *Dynamic-link library* (DLL) de Integração com programa aplicativo fiscal (PAF) e o aplicativo *mobile*.

Na Figura 9 tem-se o exemplo de como ocorre o fluxo das informações.

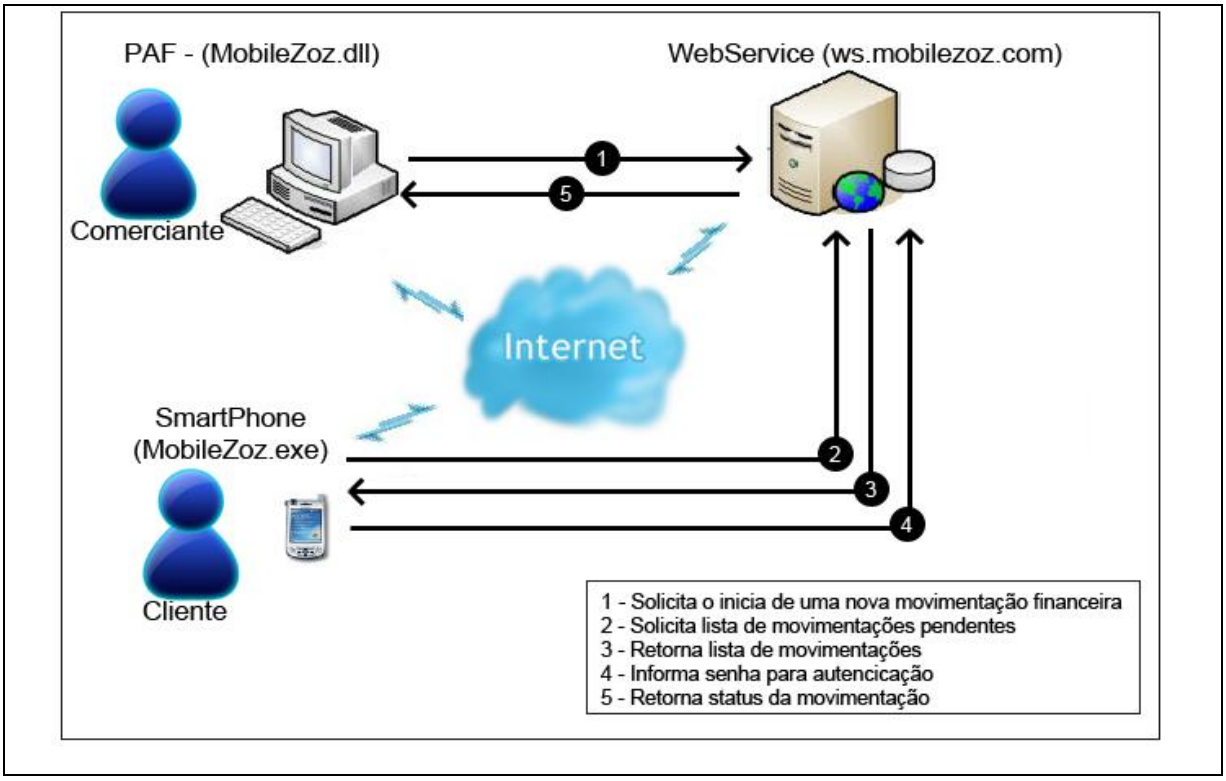

Figura 9 – Fluxo das informações

O processo desenvolvido neste projeto tem como passos básicos a iteração entre o PAF, *webservice* e MobileZoz.exe como observa-se na figura 9, que ilustra a realização de um pagamento utilizando MobileZoz, onde inicia-se quando o comerciante informa no PAF o número identificador do cliente, após, iniciar uma movimentação financeira, esta solicitação segue para o servidor aguardando aprovação. Para validar esta movimentação o cliente em seu dispositivo móvel deve acessar o *webservice* através do MobileZoz.exe onde ao receber o retorno do *webservice* o cliente informa sua senha e retorna esta informação ao *webservice* que já envia ao PAF a informação de que a movimentação foi aprovada com sucesso assim concluindo a operação.

O *website* foi desenvolvido utilizando a linguagem HTML mesclado a C# com Framework .Net, este acessa a base de dados, e o mesmo encontra-se disponibilizado em www.mobilezoz.com.

No *website* é possível acessar o cadastro de novo usuário, login de acesso às contas, gerenciamento das contas, consulta no limite de crédito e movimentações financeiras por período. Na Figura 10 observa-se a tela inicial do *website*.

Figura 10 – Tela inicial do *website*

O *webservice* foi desenvolvido utilizando a linguagem C# com Framework .Net e encontra-se publicado no endereço ws.mobilezoz.com.

No *webservice* concentram-se as principais funções de processamento, autenticação, criptografia e armazenamento de dados. Nele estão implementados os métodos utilizados nos demais aplicativos, sendo responsável por gerenciar as movimentações financeiras, validar senhas, identificar usuários, decriptografar dados e administrar a base de dados.

No desenvolvimento, aplicou-se programação Orientada a Objeto (OO) para manipulação de objetos, declarando atributos e métodos. Para manipulação de dados vindos da base *MySQL* criaram-se classes intermediárias, formando uma camada no projeto que se conectam à base e gerenciam todas as informações, realizando tratamentos e validações dos dados de forma centralizada e organizada.

No *webwevice* encontra-se os controles de chaves privadas, públicas, geração de chaves e sua distribuição entre seus usuários, no Quadro 3 pode-se observar o código que implementa a geração da chave RSA.

```
private string GerarKeyRSA()
{
    CspParameters CspParametros = new CspParameters();
    CspParametros.Flags = CspProviderFlags.UseMachineKeyStore;
    RSACryptoServiceProvider RSA = new RSACryptoServiceProvider(512, CspParametros); //Gerar nova chave
    return RSA.ToXmlString(true); //Exporta Chave
}
```

Quadro 3 – Gerar chave RSA

A chave RSA possui uma chave pública e outra privada, esta é gerada no cadastramento do usuário e gravada na base de dados. No Quadro 4 pode-se ver o par de chaves de um dos clientes.

```
<RSAKeyValue>
  <Modulus>rMbMjxXDI6dmyS35fuzGPG8UT7+NdPkQHb9axyEoyoRF6F40OsN6FISL3IOf08cJAhk6H/GEMHmZo/lxqEGWTQ==</Modulus>
  <Exponent>AQAB</Exponent>
  <P>3PBud40wAwl4160XQ2QD7bMaMByOoC+vcs6b8cF5HM0=</P>
  <Q>yDHHkZTrVc39F5DGuROGNV2qN+sFYY+5FOLXcfqyX4E=</Q>
  <DP>bteUpBfKIYvr1AUXrPboLH9DmwVRdoGjHOJGvV0fHU=</DP>
  <DQ>pOKrNrLrKd7hJ/msU19LWMTunPIqNRRYmx7ens7UwE=</DQ>
  <InverseQ>xrzAmRNnPOYTm87GQttmAFFtAWqm8Z9w4tJgo9W2FHw=</InverseQ>
  <D>qu0FQ+ywn54lxpNQB2wwdWsiuf5z8CvR8Mv0/5jjZOy0JzVn5T23nFLPSPfu0/p/NS/HpUklGbxceAR803nOAQ==</D>
</RSAKeyValue>
```

Quadro 4 – Chave RSA

Quando o usuário acessar a primeira vez o MobileZoz.exe uma instalação é iniciada, esta requisita sua chave pública ao *WebSevice*, o mesmo retorna esta informação ao usuário gravado no registro do SO que encontra-se no dispositivo móvel.

Esta chave é utilizada para decriptografar a chave TripleDES enviada pelo usuário, no Quadro 5 observa-se a principal classe que implementa um dos processo de SET, que efetua a abertura do envelope gerado no MobileZoz.exe.

```
public class Envelope
{

    public string abrirEnvelope(string envelope, string pLogin, byte[] keyDES)
    {
        TripleDESCryptoServiceProvider desCrypto = (TripleDESCryptoServiceProvider)TripleDESCryptoServiceProvider.Create();
        Serializa serializa = new Serializa();
        CriptDES criptDES = new CriptDES();
        CriptRSA criptRSA = new CriptRSA();
        Funcoes funcoes = new Funcoes();
        string keyRSA;
        //decripta string recebida
        envelope = criptDES.Decrypt(envelope, "mobilezoz14877projectTCC");
        //carregar chave do usuario gravada na base

        keyRSA = funcoes.KeyUsuarioPrivate(pLogin);
        //Criada chaveRSA
        CspParameters CspParametros = new CspParameters();
        CspParametros.Flags = CspProviderFlags.UseMachineKeyStore;
        RSACryptoServiceProvider RSA = new RSACryptoServiceProvider(512, CspParametros); //Instancia objeto

        RSA.FromXmlString(keyRSA);

        //Decripta chaveDES
        string key = criptRSA.RSADecrypt(keyDES, RSA.ExportParameters(true), false);
        //decriptografar envelope com chaveDES
        envelope = criptDES.Decrypt(envelope, key);
        return envelope;
    }
}
```

Quadro 5 – Método abrir envelope

A DLL MobileZoz.dll foi desenvolvido utilizando a linguagem C# com Framework .Net. Sua criação tem como objetivo principal criar integração com Programa Aplicativo Fiscal (PAF). A empresa parceira deve incorporar a carga da mesma, onde ao selecionar a finalizadora MobileZoz no PAF, se oferece métodos específicos para iniciar uma movimentação, enviando a solicitação para abrir movimentação financeira ao *webservice*.

A DLL programa uma tela de configuração para que o usuário possa especificar seu login, senha, url, timeOut e tempo de resposta, possui também outra tela que inicia a movimentação financeira, consulta o status da última solicitação e cancela a última movimentação.

No Figura 11 pode-se observar o formulário de configurações presente na DLL.

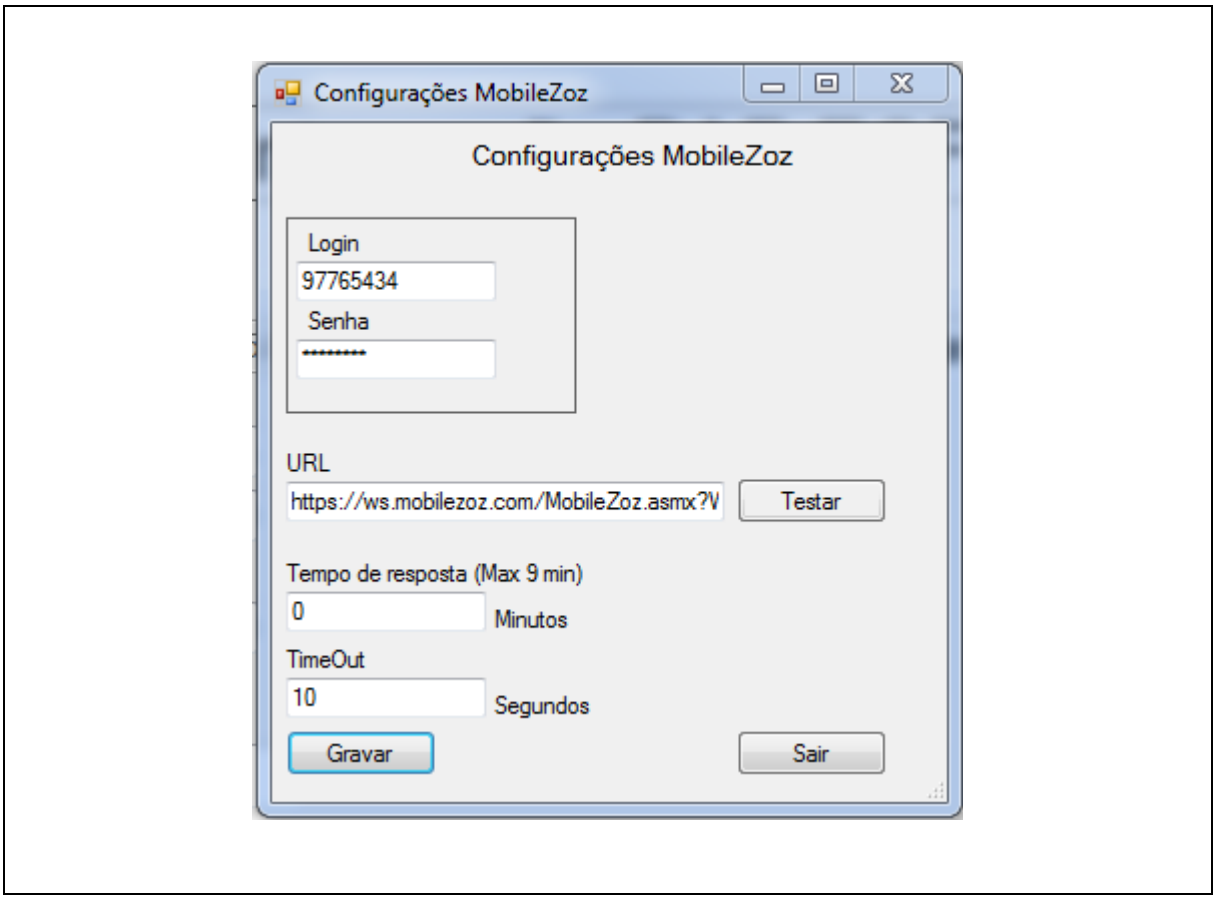

Figura 11 – Iniciar movimentação financeira

Por fim há o aplicativo MobileZoz.exe que foi desenvolvido utilizando a linguagem C# com Framework .Net. específico para celular.

Este aplicativo é responsável por várias operações, como por exemplo, rotinas que buscam no servidor uma lista de movimentações que aguardam autenticação, consulta de limite de crédito, detalhamento da movimentação financeira, digitação de senha para autenticar a movimentação, cancelar uma movimentação aberta, bloquear comerciante entre outros recursos.

Ao executar a validação, os dados devem ser envelopados onde no Quadro 6 observa-se a principal classe que programa um dos processo de SET, esta é responsável pelo fechamento do envelope para envio ao servidor, utilizando chave TripleDES e chave RSA.

```
public class envelope
{

    public string FecharEnvelope(object objeto, out byte[] key)
    {
        TripleDESCryptoServiceProvider desCrypto = (TripleDESCryptoServiceProvider)TripleDESCryptoServiceProvider.Create();
        Serializa serializa = new Serializa();
        CriptDES criptDES = new CriptDES();
        CriptRSA criptRSA = new CriptRSA();
        string KeyDES;
        string resultado = "";
        //serializar objeto
        resultado = serializa.Serializar(objeto);
        //Geração da chave DES 8bytes
        KeyDES = ASCIIEncoding.ASCII.GetString(desCrypto.Key, 0, desCrypto.Key.Length);
        //Criptografar informações serializadas
        resultado = criptDES.Encrypt(resultado, KeyDES);

        //buscar chave publica RSA
        RegistryKey rk = Registry.LocalMachine.OpenSubKey("Software", true);
        rk = rk.OpenSubKey("mobilekey");
        byte[] keyRSA = (byte[])rk.GetValue("key");
        rk.Close();
        //importar chave publica
        CspParameters CspParametros = new CspParameters();
        CspParametros.Flags = CspProviderFlags.UseMachineKeyStore;
        RSACryptoServiceProvider RSA = new RSACryptoServiceProvider(512, CspParametros); //Instancia objeto
        RSA.ImportCspBlob(keyRSA);
        key = criptRSA.RSAEncrypt(KeyDES, RSA.ExportParameters(false), false);
        resultado = criptDES.Encrypt(resultado, "mobilezoz14877projectTCC");
        return resultado;
    }
}
```

Quadro 6 – Método fechar envelope

3.10 OPERACIONALIDADE E VALIDAÇÃO

Esta sessão de testes foi criada para validar o funcionamento dos aplicativos, bem como avaliar seu desempenho e usabilidade na prática.

O processo inicial a utilização do MobileZoz quando o cliente deseja realizar um pagamento. O mesmo encaminha-se ao operador de caixa, optando por finalizar a venda utilizando MobileZoz, o comerciante solicita o número identificador do cliente, para gerar uma nova movimentação. Este número é lançado no formulário “Iniciar Movimentações Financeiras” disponível no MobileZoz.dll iniciado pelo PAF. Após este preencher estes requisitos o operador seleciona o botão “Iniciar Movimentação” conforme pode-se visualizar na Figura 12.

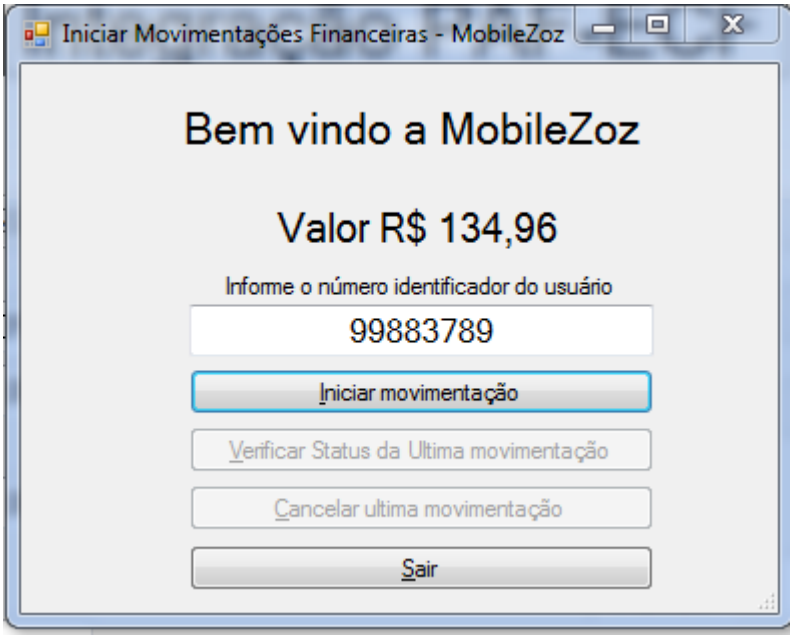

Figura 12 – Iniciar movimentação financeira

Iniciada a movimentação, o cliente pode selecionar a opção Iniciar MobileZoz, disponível no formulário principal do MobileZoz.exe instalado no *SmartPhone*, que carrega todas as movimentações em aberto do cliente. Se retornar somente uma movimentação pendente o sistema passa para o próximo formulário automaticamente, senão, lista todas as movimentações, para que o usuário possa indicar qual deseja processar, conforme Figura 13. Nesta tela o usuário tem a opção de cancelar uma movimentação financeira ou selecionar um dos valores apresentados e seleciona o botão “Próximo” seguindo o processo para autenticação.

Figura 13 – Lista de Movimentações financeiras pendentes

Identificado qual débito será finalizado, existe uma consistência que analisa se o cliente possui mais de uma conta bancária vinculada na mesma conta de usuário. Se possuir somente uma conta bancária, segue direto para o formulário de “Autenticação”, senão, o usuário deve indicar em qual conta deseja lançar o débito, na Figura 14 pode-se observar o formulário de “Contas bancárias”. Selecionada conta bancária pressiona-se o botão “Próximo” prosseguindo com o processo de autenticação.

Figura 14 – Lista de Contas bancárias vinculadas ao usuário

Identificada qual conta bancária será movimentado, o cliente pode confirmar os valores a serem processados, bem como o nome do comércio solicitante. Caso não estiver de acordo pode cancelar a movimentação ou informar a senha referente à conta selecionada, e pressionar o botão “Aprovar” como mostra o Figura 15.

Figura 15 – Formulário de autenticação das movimentações

Executado este procedimento, o cliente e o operador do caixa recebem a informação referente ao status do processo, assim finalizando a compra.

Na Figura 16 pode-se observar a informação apresentada no MobileZoz.exe.

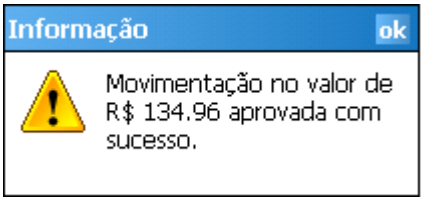

Figura 16 – Mensagem apresentada ao cliente no dispositivo móvel.

Na Figura 17 pode-se observar a informação apresentada no MobileZoz.dll.

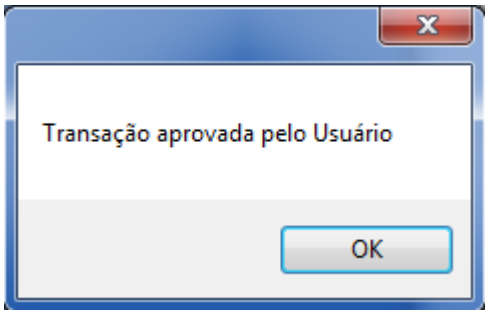

Figura 17 – Mensagem apresentada ao operador de caixa.

Com a exposição deste processo percebeu-se que a proposta de efetuar movimentações financeiras, com iteração dos clientes e comerciantes, através de um sistema rápido, seguro e estável, está bem clara, o que é fundamental para compreensão do cliente e comerciante, para que assim todos possam confiar nele utilizando-o em seu dia-dia.

4 CONCLUSÕES

As organizações, cientes da competição acirrada na atualizadade, tendem a buscar um diferencial nas diversas formas de inovar e atender com maior excelência o cliente, onde se busca invenções, criação, descobrimentos e assim ampliando o conhecimento, aperfeiçoando-o para atingir da melhor forma os objetivos. Este trabalho se propôs trazer alternativas, para melhorar questões, hoje fundamentais para o crescimento e desenvolvimento da sociedade. Elas necessitam cada vez mais de mobilidade, agilidade e segurança. Com esta visão concluiu-se um estudo sobre o que oferecer para tratar de um assunto tão complexo. Criou-se basicamente uma estrutura de mensagens entre aplicativos, utilizando uma rede aberta e, utilizando o que há de mais recente em tecnologia disponível.

Implementou-se um sistema de gerenciamento de dados capaz de proporcionar a identificação do usuário, realizando o envio de dados com segurança, garantindo principalmente integridade, autenticidade e confidencialidade das informações trocadas entre aplicativos.

Espera-se com o presente estudo, colaborar com os avanços tecnológicos nas áreas de comunicação e troca de informações, em redes abertas, onde são apresentadas práticas de gerenciamento financeiro, que atualmente é um dos recursos mais utilizados na sociedade e que pode ser mais facilmente assimilado ao leitor, auxiliando sua aceitação.

O trabalho foi concluído com sucesso, visto que todos os objetivos foram contemplados permitindo utilidade e compreensão. Sua aplicação utiliza um processo de movimentação financeira, comum no cotidiano das pessoas facilitando seu entendimento.

Desenvolveu-se um *webservice* para gerenciamento das movimentações, sendo o centro da aplicação que possui interação com outras 3 aplicações disponíveis: o dispositivo móvel utilizado pelo cliente em suas validações, a DLL quando há integração com sistemas PAF para iniciar uma movimentação financeira ao cliente e *website* quando utilizamos os mesmos objetos para acessar as informações pertinentes a cada conta de usuário e disponibilizar o cadastramento dos mesmos. Todos os itens apresentados estão interligados via rede aberta como especificado nos objetivos, sendo utilizado o protocolo SET para estabelecer segurança nas aplicações.

4.1 EXTENSÕES

Dando continuidade ao projeto e ampliando este mercado em uma próxima versão, é interessante desenvolver a versão do MobileZoz.exe para plataforma JAVA, ampliando o número de usuários que podem utilizar este recurso.

Há também a necessidade de desenvolver um módulo administrativo das contas, possibilitando que o usuário possa gerenciar os dados, emitir relatórios e gráficos, emitir boletos assim realizando o controle financeiro da MobileZoz.

Sugere-se também criar um processo para aprovação de crédito para usuários, usando a Inteligência Artificial (IA) que auxiliam e orientam as decisões.

REFERÊNCIAS BIBLIOGRÁFICAS

BANCO DO BRASIL. **Autoatendimento BB pelo celular**. [S.I.], 2009. Disponível em: <http://www.bb.com.br/portalbb/page22,101,2298,0,0,1,1.bb?codigoNoticia=2612&codigoMenu=161>. Acesso em: 29 maio 2010.

DALFOVO, Oscar, et al. **A tecnologia do futuro Wi-Fi (Wireless Fidelity)**. Blumenau, 2003. Disponível em: <http://campeche.inf.furb.br/siic/siego/docs/Artigo_Wireless_Uniplac_2003.pdf>. Acesso em: 29 maio 2010.

DARLEN, Daniel. **Introdução à Criptografia RSA**. [S.I.], 2007. Disponível em: <http://www.dicas-l.com.br/dicas-l/20070611.php>. Acesso em: 29 maio 2010.

DUPRAT, Carlos. **Comunicação para Todos**. [S.I.], 2010. Disponível em: <http://www.ericsson.com/br/solutions/3G/artigo_duprat.shtml>. Acesso em: 29 maio 2010.

Gestão. **O que é PAF ECF?**. [S.I.], 2010. Disponível em: <http://www.treinamentosparafarmacia.com/search/label/Gest%C3%A3o>. Acesso em: 09 julho 2010.

GUILHERME, Joel. **Criptografia, Chaves Públicas e Assinatura Digital**. [S.I.], 2003. Disponível em: <http://www.google.com.br/url?sa=t&source=web&ct=res&cd=3&ved=0CCgQFjAC&url=http%3A%2F%2Fwww.sbis.org.br%2FCriptografia.doc&rct=j&q=usando+hash+como+assinatura+digital&ei=wRUFTKPXHoOkuAeGhsn3DQ&usg=AFQjCNH8WJMSOE3yMK3NG1e6L6c5NnIzvQ. Acesso em: 01 junho 2009.

IDGNOW. **Empresas de busca trabalha com Intel e Sony para criar televisores que rodarão Android**. [S.I.], 2010. Disponível em: <http://idgnow.uol.com.br/computacao_pessoal/2010/03/18/vem-ai-a-google-tv/>. Acesso em: 29 maio 2010.

JAKOBSEN, Tommy. **Certificados digitais:** uma ferramenta desenvolvida com base no padrão SET. 2000. 398f. Instituto de Informática. Universidade Federal do Rio Grande do Sul, Porto Alegre.

JORNAL DE SANTA CATARINA. **Laptop estava dentro de caixa eletrônico.** 2009. Disponível em: <http://www.clicrbs.com.br/jsc/sc/impressa/4,784,2537880,12473>. Acesso em: 29 maio 2010.

LAFLOUFA, Jacqueline. **Sony planeja um novo dispositivo móvel que mistura um smartphone com um PSP**. [S.I.], [2010]. Disponível em: <http://teteraconsultoria.com.br/blog/sony-planeja-um-novo-dispositivo-movel-que-mistura-um-smartphone-com-um-psp/>. Acesso em: 29 maio 2010.

MARTIN, Henrique. **Conheça quatro navegadores para celulares e smartphones.** [S.I.], [2008]. Disponível em: <http://pcworld.uol.com.br/reviews/2008/11/21/conheca-quatro-navegadores-para-celular-e-smartphones/>. Acesso em: 29 maio 2010.

MOBILECARD. **Empresa**. Uberlândia, 2009. Disponível em: <http://www.mobilecard.com.br/empresa.shtml >. Acesso em: 29 maio 2010.

MUNIZ, Marcos. **Data Encryption Standart**. [S.I.], 1999. Disponível em: < http://www.gta.ufrj.br/grad/99_2/marcos/des.htm >. Acesso em: 29 maio 2010.

PETRY, Helô. **Protocolo SET: uma Solução para Segurança em Comércio Eletrônico**. Florianópolis, 2010. Disponível em: <http://inf.unisul.br/~ines/workcomp/cd/pdfs/2285.pdf>. Acesso em: 17 março 2010.

RAMOS, Robson. **Protótipo de software para envio de mensagens criptografadas para um dispositivo móvel utilizando a plataforma .Net**. 2004. 31 F. Trabalho de Conclusão de Curso (Bacharelado em Ciências da Computação) - Centro de Ciências Exatas e Naturais, Universidade Regional de Blumenau, Blumenau.

RIGUES, Rafael. **A Hora dos smartphones**. [S.I.], 2009. Disponível em: <http://ultimosegundo.ig.com.br/perspectivas2010/2009/12/21/a+hora+dos+smartphones+9251397.html>. Acesso em: 29 maio 2010.

SPOT. Jack. **DES - A inspiração do Fortaleza Digital**. [S.I.], 2008. Disponível em: <http://jackflashspot.spaces.live.com/blog/cns!9E91F10BF31AE52B!160.entry>. Acesso em: 09 julho 2010.

Sociedade dos usuários de Informática e Telecomunicações. **Proteção contratual**. Porto Alegre, 2009. Disponível em: <http://www.rs.sucesu.org.br/legislacao/orientacoes_basicas/glossario>. Acesso em 29 maio 2010.

WOLRATH, Carl Eric. **Secure Electronic Transaction:** a market survey and a test implementation of SET technology. [S.I.],1998. Disponível em: <http://www.wolrath.com/set.html>. Acesso em: 01 maio 2010.

APÊNDICE A – Detalhamento dos Casos de Uso desenvolvidos no projeto

Esta seção apresenta descrição detalhada dos casos de uso previstos no diagrama no item 3.4.1.

No Quadro 7 apresenta-se o caso de uso "`Cadastrar usuário`".

Nome do Caso de Uso	Cadastrar usuário
Descrição	Realiza seu cadastro para utilização dos recursos MobileZoz.
Ator	Cliente ou Comerciante
Pré-condição	*website* deve estar publicado em um servidor na Internet. Usuário com acesso a internet. Usuário acessar www.mobilezoz.com.
Fluxo principal	1. usuário seleciona opção “Cadastre-se aqui”; 2. usuário informa todos os dados obrigatórios; 3. sistema valida informações cadastrais; 4. sistema armazena os dados.
Fluxo alternativo (a)	• dados do cadastro nulo ou inválido; • mensagem “Verifique os campos obrigatórios” é apresentada; • campos inválidos ou em branco destacados.
Pós-condição	Usuário cadastrado aguardando aprovação

Quadro 7 – Descrição do caso de uso cadastrar usuário (UC01).

No Quadro 8 apresenta-se o caso de uso "`Cadastrar conta bancária`".

Nome do Caso de Uso	Cadastrar conta bancária
Descrição	Cadastrar conta para vincular suas movimentações.
Ator	Cliente ou Comerciante
Pré-condição	*website* deve estar publicado em um servidor na Internet. Usuário com acesso a internet. Usuário acessar www.mobilezoz.com. Usuário deve estar na tela de cadastro.
Fluxo principal	1. usuário seleciona opção “Adicionar Conta bancária”; 2. usuário informa todos os dados obrigatórios; 3. sistema valida informações cadastrais; 4. sistema armazena os dados.
Fluxo alternativo (a)	• dados do cadastro nulo ou inválido; • mensagem “Verifique os campos obrigatórios” é apresentada; • campos inválidos ou em branco destacados.
Pós-condição	Contas cadastradas aguardando aprovação

Quadro 8 – Descrição do caso de uso cadastrar conta bancária (UC02).

No Quadro 9 apresenta-se o caso de uso "`Efetuar Login`".

Nome do Caso de Uso	Efetuar login
Descrição	Usuário acessa aplicação via navegador FireFox 3.0 ou superior e informa dados de login e senha armazenados no cadastro de usuários.
Ator	Cliente ou Comerciante
Pré-condição	*website* deve estar publicado em um servidor na Internet. Usuário deve estar cadastrado no banco de dados. Usuário com acesso a internet. Usuário acessar www.mobilezoz.com.
Fluxo principal	1. usuário preenche seu login e sua senha; 2. sistema valida os dados de login e senha do usuário; 3. sistema verifica se usuário não está bloqueado; 4. sistema direciona o Usuário para a página de menu.
Fluxo alternativo (a)	• nome de usuário e/ou senha inválido(s); • mensagem “usuário ou senha inválida” é apresentada.
Fluxo alternativo (b)	• usuário não foi analisado para aprovação • mensagem “Seu cadastro encontra-se em aprovação” é apresentada.
Fluxo alternativo (c)	• usuário não aprovado • mensagem “Seu cadastro não foi aprovado” é apresentada.
Pós-condição	Usuário tem acesso ao gerenciamento de sua(s) conta(s).

Quadro 9 – Descrição do caso de uso efetuar *login* (UC03).

No Quadro 10 apresenta-se o caso de uso "`Iniciar movimentação`".

Nome do Caso de Uso	Iniciar movimentação
Descrição	Comerciante inicia uma movimentação financeira para um cliente
Ator	Comerciante
Pré-condição	Usuário cadastrado e aprovado. Comerciante cadastrado e aprovado. Comerciante utilizar PAF integrado com MobileZoz.dll. Cliente e Comerciante com acesso a internet. *webservice* deve estar publicado em um servidor na Internet.
Fluxo principal	1. comerciante solicita numero identificado do usuário; 2. cliente informa seu numero Identificador MobileZoz; 3. sistema envia solicitação.
Fluxo alternativo (a)	• cliente inválido; • emite mensagem para o comerciante informando "Operação cancelada, cliente ou conta não existem ou bloqueada".
Fluxo alternativo (b)	• usuário com limite de crédito insuficiente; • emite mensagem para o comerciante informando "Limite insuficiente".
Fluxo alternativo (c)	• usuário cancela operação; • emite mensagem para o comerciante informando "Transação cancelada pelo cliente.".
Fluxo alternativo (d)	• usuário bloqueou comercio; • emite mensagem para o comerciante informando "Você foi bloqueado pelo cliente.".
Pós-condição	Comerciante aguarda retorno de aprovação

Quadro 10 – Descrição do caso de uso solicitar autenticação (UC04).

No Quadro 11 apresenta-se o caso de uso "`Escolher conta de lançamento`".

Nome do Caso de Uso	Realizar a escolha de qual conta será o lançamento
Descrição	Cliente indica qual conta será lançado o débito
Ator	Cliente
Pré-condição	*webservice* deve estar publicado em um servidor na Internet. Cliente deve estar cadastrado no banco de dados. Cliente possuir mais de uma conta vinculada em seu usuário. Cliente e Comerciante com acesso a internet. Comerciante iniciou movimentação financeira. Contas com limite disponível.
Fluxo principal	1. cliente seleciona conta; 2. cliente solicita processamento da operação.
Pós-condição	Cliente identificou a conta para lançamento do novo débito.

Quadro 11 – Descrição do caso de uso escolher conta de lançamento (UC05).

No Quadro 12 apresenta-se o caso de uso "`realizar a digitação de senha no dispositivo móvel`".

Nome do Caso de Uso	Realizar a digitação de senha no dispositivo móvel
Descrição	Cliente informa a senha da conta
Ator	Cliente
Pré-condição	Usuário cadastrado e aprovado. Comerciante cadastrado e aprovado. Comerciante utilizar PAF integrado com MobileZoz.dll. *webservice* deve estar publicado em um servidor na Internet. Cliente e Comerciante com acesso a internet. Comerciante iniciou uma movimentação financeira.
Fluxo principal	1. cliente solicita lista de movimentações; 2. cliente valida valores e dados da empresa; 3. cliente informar sua senha; 4. sistema válida senha; 5. sistema envia mensagem "Processo finalizado com sucesso.".
Fluxo alternativo (a)	• sistema não validou a senha; • sistema envia mensagem "Senha inválida".
Fluxo alternativo (b)	• usuário cancelou a movimentação;
Fluxo alternativo (c)	• senha inválida mais de 3 vezes; • usuário bloqueado. • sistema envia mensagem "Você digitou a senha errada por 3 vezes. Sua conta foi bloqueada, entre em contato para desbloquear sua conta e cadastrar uma nova senha";
Pós-condição	Venda finalizada

Quadro 12 – Descrição do caso de uso digitação de senha no dispositivo móvel (UC06).

No Quadro 13 apresenta-se o caso de uso "`permitir o cancelamento de uma solicitação`".

Nome do Caso de Uso	Permitir o cancelamento de uma solicitação
Descrição	Cancelar uma solicitação
Ator	Cliente
Pré-condição	Usuário cadastrado e aprovado. Comerciante cadastrado e aprovado. Comerciante utilizar PAF integrado com MobileZoz.dll. *webservice* deve estar publicado em um servidor na Internet. Cliente e Comerciante com acesso a internet. Comerciante iniciou uma movimentação financeira.
Fluxo principal	1. Cliente solicita lista de movimentações; 2. Cliente desiste da transação; 3. Cliente cancela operação; 4. Sistema apresenta mensagem para o comerciante "Transação cancelada pelo cliente".
Pós-condição	Venda finalizada por cancelamento

Quadro 13 – Descrição do caso de uso permitir cancelamento de uma movimentação(UC07).

No Quadro 14 apresenta-se o caso de uso "`permitir o bloqueio de comerciantes`".

Nome do Caso de Uso	Permitir o bloqueio de comerciantes
Descrição	Bloquear um comerciante
Ator	Cliente
Pré-condição	Usuário cadastrado e aprovado. Comerciante cadastrado e aprovado. Comerciante utilizar PAF integrado com MobileZoz.dll. *webservice* deve estar publicado em um servidor na Internet. Cliente e Comerciante com acesso a internet. Comerciante iniciou uma movimentação financeira.
Fluxo principal	1. cliente solicita lista de movimentações; 2. cliente bloqueia comerciante.
Pós-condição	Comerciante bloqueado sem possibilidades e efetuar novas movimentação para o cliente que o bloqueou

Quadro 14 – Descrição do caso de uso permitir bloqueio de comerciantes (UC08).

No Quadro 15 apresenta-se o caso de uso "permitir o estorno de um lançamento".

Nome do Caso de Uso	Permitir o estorno de um lançamento
Descrição	Cancelar uma transação devido a um lançamento errado.
Ator	Comerciante
Pré-condição	Usuário cadastrado e aprovado. Comerciante cadastrado e aprovado. Comerciante utilizar PAF integrado com MobileZoz.dll. *webservice* deve estar publicado em um servidor na Internet. Comerciante com acesso a internet. Venda finalizada.
Fluxo principal	1. comerciante seleciona opção de estorno e informa identificador do cliente; 2. sistema lista ultimas movimentações do cliente para aquele comercio; 3. comerciante seleciona a movimentação que será cancelada.
Pós-condição	Sistema anula movimentação selecionada

Quadro 15 – Descrição do caso de uso permitir o estornar de um lançamento (UC09).

No Quadro 16 apresenta-se o caso de uso "Consultar limite de crédito disponível".

Nome do Caso de Uso	Consultar limite de crédito disponível
Descrição	Consultar quanto ainda há disponível no limite de um cliente
Ator	Cliente
Pré-condição	Cliente cadastrado e aprovado. *webservice* deve estar publicado em um servidor na Internet. Cliente com acesso a internet.
Fluxo principal	1. cliente acessa aplicativo MobileZoz.exe; 2. cliente acessa menu/limite.
Pós-condição	Sistema apresenta e seus limite disponível.

Quadro 16 – Descrição do caso de uso consultar limite de crédito (UC10).

No Quadro 17 apresenta-se o caso de uso "`Consultar extrato`".

Nome do Caso de Uso	Consultar movimentações financeiras
Descrição	Consultar relação das movimentações financeira.
Ator	Cliente e Comerciante
Pré-condição	Usuário cadastrado e aprovado. *website* deve estar publicado em um servidor na Internet. Comerciante e Cliente com acesso a internet. Usuário efetuar Login.
Fluxo principal	1. usuário seleciona opção extrato; 2. usuário define período e a conta que deseja emitir.
Pós-condição	Sistema lista todas as movimentações

Quadro 17 – Descrição do caso de uso consultar extrato (UC11).