UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
INSTITUTO DE INFORMÁTICA
CURSO DE CIÊNCIA DA COMPUTAÇÃO

RAFAEL VON HOONHOLTZ MAGRIN

Proposta de uma Arquitetura para Sistemas de Pagamento Móvel

Trabalho de Graduação.

Prof. Henrique J. Brodbeck
Orientador

Porto Alegre, junho de 2010.

SUMÁRIO

LISTA DE ABREVIATURAS E SIGLAS

API	*Application Program Interface*
ANATEL	Agência Nacional de Telecomunicações
HTTP	*Hyper Text Transfer Protocol*
HTTPS	*Hyper Text Transfer Protocol Secure*
IMEI	*International Mobile Equipment Identity*
IMSI	*International Mobile Subscriber Identity*
IND	Informação não disponível
J2ME	*Java 2 Micro Edition*
NFC	*Near Field Communication*
P2P	*Peer-to-Peer*
PDA	*Personal Digital Assistant*
PNG	*Portable Network Graphics*
POS	*Point of Sale*
REST	*Representational State Transfer*
RPC	*Remote Procedure Call*
SIM	*Subscriber Identity Module*
SOAP	*Simple Object Access Protocol*
SMS	*Short Messsage Service*
SSL	*Secure Socket Layer*
TLS	*Transport Layer Security*
URL	*Uniform Resource Locator*
USSD	*Unstructured Supplementary Service Data*
XML	*Extensible Markup Language*

LISTA DE FIGURAS

LISTA DE TABELAS

RESUMO

À medida que a tecnologia dos telefones celulares avança novas aplicações são criadas para eles. No início da década de 2000, o pagamento móvel surgiu como uma promessa que tornaria o cartão de crédito obsoleto, mas ainda estamos muito longe deste momento.

Este trabalho apresenta uma visão geral dos sistemas de pagamento móvel, suas características, as tecnologias utilizadas para implementação, os aspectos que tornam atrativo o uso, as barreiras de adoção e alguns exemplos de sistemas de pagamento móvel.

O objetivo deste trabalho é avaliar o estado atual do pagamento móvel e entender de que forma a tecnologia pode ser utilizada para facilitar sua adoção. Sendo assim, é apresentada uma proposta de arquitetura de sistemas de pagamento móvel, com foco na comunicação entre a aplicação cliente e o servidor, baseada na arquitetura de Transferência de Estado Representacional (REST).

Tendo em vista que as formas de pagamento móveis existentes são limitadas para grupos específicos que dispõem de determinado dispositivo móvel, e que esta condição dificulta a expansão deste sistema, esta arquitetura propõe uma independência entre o servidor e a aplicação cliente, permitindo uma maior flexibilidade na escolha das tecnologias utilizadas em ambas às partes.

Além disso, o fato da arquitetura proposta ser baseada em uma arquitetura REST, torna o sistema mais escalável permitindo que este se adapte à medida que a base de clientes aumente.

Palavras-Chave: telefone celular, pagamento móvel, REST

Proposal of a Mobile Payment System Architecture

ABSTRACT

As mobile phones technology advances, new applications are created for them.. In the early 2000s, the mobile payment emerged as a promise that would make the credit card obsolete, but we are still far from this moment.

This study provides an overview of mobile payment systems, its characteristics, the technologies used for implementation, the aspects that make it attractive to use, the barriers to adoption and some examples of mobile payment systems.

The purpose of this study is to analyze the current state of mobile payment and understand how the technology can be used to facilitate its adoption. Therefore, an architecture is proposed for implementing mobile payment systems, focusing on the communication between the client application and the server, based on the Representational State Transfer (REST) architecture.

Given that the existing mobile payment methods are limited to some specific groups that posses a specific mobile device, and that it hinders the expansion of the system, this architecture provides independence between the server and client application, allowing greater flexibility in the choice of technologies used by both parts.

Moreover, the fact that the proposed architecture is based on a REST architecture, makes the system more scalable allowing it to adapt as the customer base increases.

Keywords: mobile phone, mobile payment, REST

1 INTRODUÇÃO

O telefone celular tornou-se um item comum na vida das pessoas, sendo que no final de 2009 existiam aproximadamente 0,9 acessos móveis por habitante no Brasil (ANATEL, 2010). Diversos fatores influenciaram a popularização do telefone celular, entre eles o surgimento do pré-pago, como modelo de cobrança pelo serviço, que representa aproximadamente 82% dos acessos móveis, como pode ser visto na tabela 1.1 e na figura 1.1.

Tabela 1.1: População estimada e número de acessos móveis no Brasil

	População Estimada (habitantes)	Total de Acessos Móveis	Acessos Móveis Pós-Pago	Acessos Móveis Pré-Pago
2005	185.081.066	86.210.336	16.540.286	69.670.050
2006	187.665.341	99.918.612	19.632.939	80.555.682
2007	190.261.138	120.980.103	23.403.596	97.576.507
2008	192.868.399	150.646.667	27.909.410	122.737.257
2009	192.118.820	173.959.368	30.358.861	143.600.507

Fonte: ANATEL, 2010

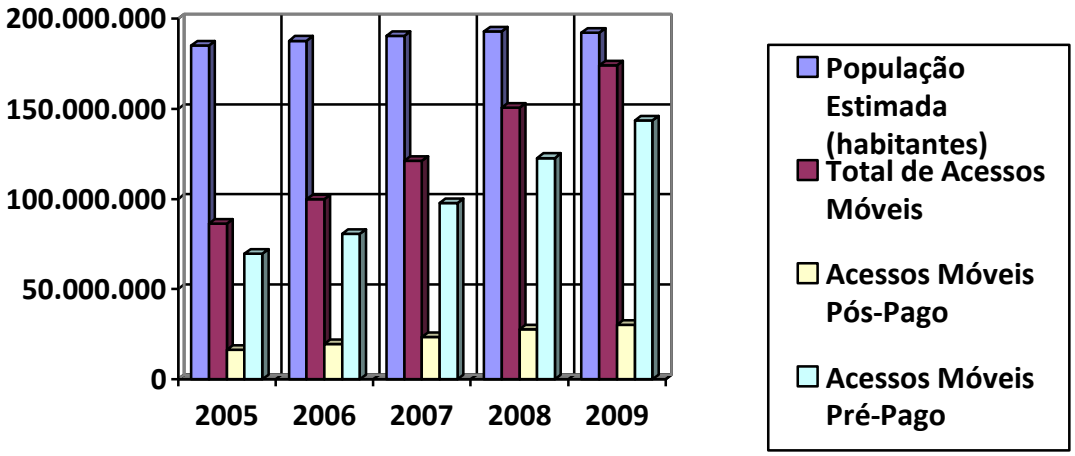

Figura 1.1: Gráfico da população estimada e número acessos móveis no Brasil

O telefone celular é utilizado não somente como um simples dispositivo para efetuar ligações telefônicas, mas como uma ferramenta com diversos recursos para nosso dia-a-dia, como, por exemplo, câmera fotográfica, agenda e acesso a internet. Com o surgimento de novos dispositivos e novas tecnologias, novas aplicações são criadas, como o uso dos telefones celulares para efetuar pagamentos.

O uso dos telefones celulares como meio de pagamento vem sendo discutido desde o início da década de 2000. Centenas de serviços de pagamento móvel foram introduzidos em todo mundo, mas muito destes esforços falharam (DAHLBERG, 2008). Apesar dos resultados negativos, muitas empresas continuaram investindo neste tipo de serviço e hoje começam a surgir alguns casos de sucesso, sendo o mais famoso o M-Pesa da Safaricom, operadora de telefonia celular queniana, com aproximadamente 9 milhões de clientes (GSMA, 2010).

No Brasil, apesar de já existirem empresas estabelecidas, este mercado ainda está engatinhando. Nos primeiros três meses de 2010, somente 5% dos usuários de telefone celular fizeram um pagamento pelo telefone celular (GUEDES, 2010).

1.1 Motivação e objetivo

Apesar de não ser algo tão novo e ter um grande potencial, o pagamento móvel ainda não é algo comum no nosso dia-a-dia. Ao mesmo tempo em que existem barreiras, também existem fatores incentivadores para que este tipo de serviço seja amplamente adotado. Isto instiga a tentar descobrir o que está impedindo que esta ampla adoção ocorra e o que pode ser feito para viabilizar a concretização deste potencial.

O trabalho tem por objetivo analisar o funcionamento dos sistemas de pagamento móvel, avaliar as atuais tecnologias disponíveis, os requisitos, os incentivadores e as barreiras de adoção, e propor uma arquitetura de sistema que tente mitigar estas barreiras.

Devido ao alto grau de complexidade de um sistema de pagamento móvel e a similaridade em alguns aspectos com outros sistemas financeiros já estabelecidos, o trabalho terá como foco o canal de comunicação entre a aplicação móvel cliente e o servidor do sistema.

Também serão apresentados alguns exemplos de sistemas de pagamento móvel em uso no Brasil.

1.2 Estrutura do trabalho

O trabalho apresenta a seguinte estrutura:

- Capítulo 2: introduz o conceito de sistemas de pagamento móvel, apresenta como são classificados os diferentes tipos de sistemas de pagamento móvel, apresenta os requisitos de segurança de um sistema de pagamento móvel e apresenta os principais incentivos e barreiras de adoção dos sistemas de pagamento móvel.
- Capítulo 3: apresenta as principais tecnologias para implementação de sistemas de pagamento móvel.
- Capítulo 4: apresenta exemplos de sistemas de pagamento móvel no Brasil.

- Capítulo 5: apresenta uma proposta de arquitetura de sistemas de pagamento móvel baseada na arquitetura REST.
- Capítulo 6: contém a conclusão e considerações finais.

2 SISTEMAS DE PAGAMENTO MÓVEL

Pagamentos móveis são pagamentos de bens, serviços e contas com um dispositivo móvel (como telefone celular, smartphone, ou assistente pessoal digital (PDA)) tirando vantagem de redes sem fio e outras tecnologias de comunicação (DAHLBERG, 2008).

Para facilitar o entendimento dos exemplos, daqui para frente vamos diferenciar os usuários de sistemas pagamentos móveis denominando-os vendedores e consumidores, sendo o primeiro grupo os usuários que recebem um pagamento e o segundo grupo os usuários que efetuam um pagamento. Vale lembrar que, dependendo do sistema, um mesmo usuário pode atuar como vendedor e consumidor.

A figura 2.1 mostra uma visão geral de como funcionam os sistemas de pagamento móvel. Apesar de em geral este ser o funcionamento de um sistema de pagamento móvel, dependendo da tecnologia utilizada para implementação do sistema, existem outras variações. Um exemplo são sistemas de pagamento por aproximação (GUEDES, 2010).

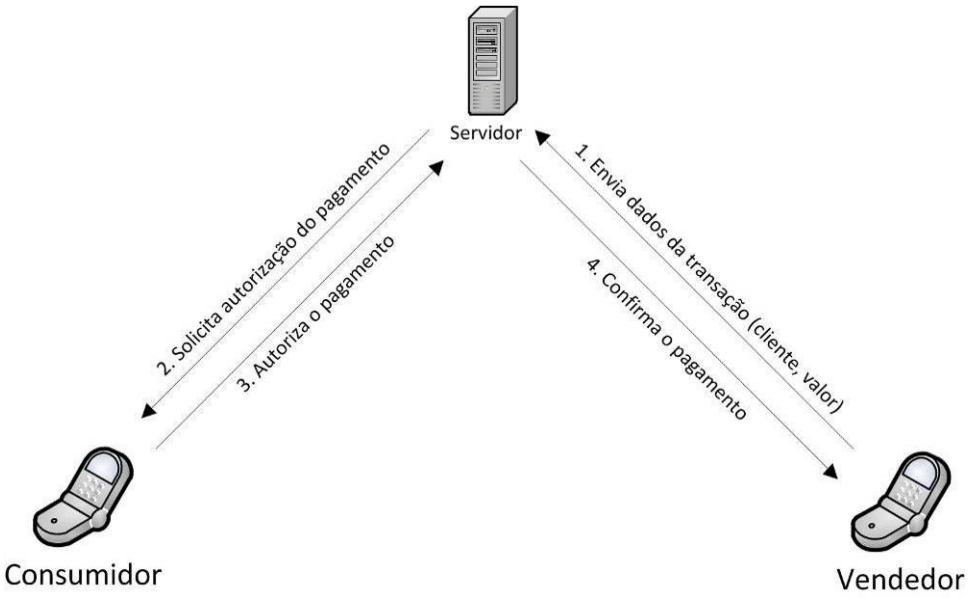

Figura 2.1: Visão geral de como funciona um sistema de pagamento móvel

2.1 Classificação de sistemas de pagamento móvel

Vários artigos foram publicados apresentando classificações de sistemas de pagamento móvel (MOHAMMADI, 2008; ZHENG, 2003; VALCOURT, 2005), mas devido ao fato de ser uma tecnologia nova, não existe um consenso entre os autores.

Abaixo apresenta-se uma classificação de sistemas de pagamento móvel fazendo uma consolidação das diversas fontes.

Os sistemas de pagamento móvel podem ser classificados de acordo com diferentes critérios, conforme segue.

2.1.1 Cenários de transações

Uma transação de pagamento móvel pode acontecer geralmente em cinco diferentes situações, distinguíveis com consideração ao ponto de venda ou serviço:

- Comércio Móvel: Compra de conteúdo ou serviços pelo telefone celular, por exemplo, vídeo/áudio streaming em telefones celulares e compra de ingressos de cinema com ticket eletrônico via SMS.
- Comércio Eletrônico: Todos os tipos de compras de bens, serviços ou conteúdo via internet, excluindo Comércio Móvel. Por exemplo, compra de bens ou conteúdo via Internet.
- Compras em lojas físicas: Transações entre uma pessoa (consumidor) e uma instituição/loja. Por exemplo, comprar roupas em um shopping center.
- Compra em máquinas automáticas: Transação entre uma pessoa e uma máquina. Por exemplo, máquinas de refrigerante e parquímetro.
- *Peer-to-peer* (P2P): Transferência de dinheiro entre indivíduos. Por exemplo, para acerto de uma transação de leilão eletrônico, pagamento de uma corrida de táxi, como mesada para as crianças, para pagamentos de débitos de baixo valor.

2.1.2 Tempo de pagamento do ponto de vista do consumidor

O pagamento do valor referente a uma transação pode ocorrer das seguintes maneiras:

- Pré-pago: o consumidor deposita antecipadamente um valor específico e utiliza esta quantia até que seu saldo esgote.
- Real-time: o consumidor tem o valor da transação debitado imediatamente de sua conta em uma instituição financeira.
- Pós-pago: o consumidor efetua, em uma data específica do mês (ou outro período estabelecido), o pagamento do valor total das transações de um determinado período.

2.1.3 Tempo de pagamento do ponto de vista do vendedor

O recebimento do valor referente a uma transação pode ocorrer das seguintes maneiras:

- Real-time: o vendedor tem o valor da transação creditado imediatamente em sua conta em uma instituição financeira.
- Pós-pago: o vendedor recebe, em uma data específica do mês (ou outro período estabelecido), o valor total das transações de um determinado período.

2.1.4 Agente financeiro

O agente financeiro é o responsável pela administração das contas envolvidas no sistema de pagamento móvel. Existem três possíveis agentes financeiros:

- Bancos: o consumidor/vendedor tem o valor da transação debitado/creditado na sua conta de cartão de crédito ou conta corrente.
- Operadoras de telefonia móvel: o consumidor/vendedor tem o valor da transação debitado/creditado na sua conta telefônica ou em conta específica para o serviço.
- Empresas de pagamento online: o consumidor/vendedor tem uma conta virtual que pode funcionar como uma conta bancária, como um cartão de crédito ou cartão pré-pago. A própria empresa responsável pelo sistema de pagamento móvel pode ser a empresa de pagamento online que administra a conta virtual.

2.1.5 Empresa responsável pelo sistema de pagamento móvel

Existem duas maneiras de classificar as empresas responsáveis pelo sistema de pagamento móvel:

- Agente financeiro: o próprio agente financeiro é o responsável pelo sistema de pagamento móvel.
- Terceiro: uma empresa é responsável pelo sistema de pagamento móvel em parceria com um ou mais agentes financeiros.

2.2 Requisitos de segurança de um sistema de pagamento móvel

A segurança é um dos principais requisitos de um sistema de pagamento móvel e, os usuários esperam que a segurança de sistemas bancários móveis tenha, no mínimo, o mesmo nível de segurança dos sistemas bancários online via PC (MMA, 2009). Sendo assim, os mesmos requisitos se aplicam a sistemas móveis, tais como:

- Transmissão segura de dados
- Controle da aplicação e do acesso a dados
- Integridade dos dados

Para satisfazer os requisitos citados acima, é necessária a implementação de serviços que fundamentam as tecnologias de segurança (NORRIS, 2001):

- Autenticação: é o processo de certificar a identidade tanto do cliente quanto do provedor do serviço;
- Privacidade: é a garantia de que os dados que estiverem trafegando entre a origem e o destino da comunicação, não possam ser entendidos ou utilizados por terceiros;
- Integridade: é a garantia de que os dados não foram alterados durante o processo de transmissão;
- Autorização: é o processo de determinação de que uma pessoa específica tem o direito de executar uma ação em particular, em relação a um objeto em particular e em determinada situação; e,

- Não-repúdio: é o mecanismo pelo qual nenhuma das partes de uma negociação possa negar que a mesma ocorreu ou que participou dela.

Além dos requisitos de segurança anteriormente citados, existe um novo desafio que deve ser avaliado no caso de sistemas móveis. Ocorrendo a perda do dispositivo móvel, o impacto na segurança deve ser mínimo e, preferencialmente, devem existir maneiras de o usuário, mesmo que através de contato com a empresa responsável pelo sistema de pagamento móvel, bloquear remotamente a utilização deste dispositivo para acessar sua conta no sistema (MMA, 2009).

2.3 Incentivos e barreiras para a adoção de sistemas de pagamento móvel

O maior problema para um sistema de pagamento móvel é obter ampla aceitação e uso é o atingimento de uma massa critica. Isso tende a ser o problema do ovo e da galinha: por um lado, o consumidor só utilizará o sistema se existir um número significante de vendedores que o aceite, por outro lado, os vendedores só estarão dispostos a adotar o sistema se existir um número significante de usuários utilizando-o (POUSTTCHI, 2004).

Outro problema relevante é a questão da segurança, pois não somente a implementação de recursos de segurança é importante, mas também a percepção que os usuários possuem da segurança do sistema (MMA, 2009).

Nenhum desses problemas possui solução fácil, mas já foram enfrentados em outras situações como na implantação dos cartões de crédito/débito e do comércio eletrônico, de onde podem ser tiradas algumas estratégias para contornar estes problemas.

Além das barreiras citadas acima, existem alguns fatores que podem incentivar ou criar barreiras para adoção de um sistema de pagamento móvel. Estes podem ser vistos do ponto de vista do consumidor ou do vendedor (MOHAMMADI, 2008).

2.3.1 Incentivos e barreiras para o consumidor

Incentivos:

- Possibilita o uso em todos os cenários de transações citados no item 2.1.1
- Não ter custos ou ter custos muito baixos de transação para o consumidor
- Fácil de utilizar e responde rapidamente
- É aceito por um grande número de vendedores
- Compatibilidade com os sistemas financeiros atuais
- Traz alguma vantagem relativa como, por exemplo, evitar filas, ser independente de tempo e lugar, e complementar pagamentos em dinheiro
- É operado por uma instituição confiável como, por exemplo, bancos e operadoras de cartão de crédito

Barreiras:

- Nível de complexidade do sistema como, por exemplo, possuir a necessidade de lembrar códigos e formatos

- Procedimentos complexos para cadastro
- Alto custo de transação para o consumidor
- Necessita que o consumidor adquira um aparelho de telefone celular novo
- Baixa adoção por vendedores
- Incompatibilidade com sistemas de outras operadoras de telefonia
- Percepção de risco na utilização do sistema

2.3.2 Incentivos e barreiras para o vendedor

Incentivos:

- Fácil de utilizar e responde rapidamente
- É utilizado por um grande número de consumidores

Barreiras:

- Sistemas complexos e de difícil uso
- Incompatibilidade com os sistemas financeiros atuais
- Alto custo de transação para o vendedor
- Necessita que o vendedor adquira um aparelho de telefone celular novo e/ou terminal POS
- Incompatibilidade com sistemas de outras operadoras de telefonia
- Não ser operado por uma instituição confiável como, por exemplo, bancos e operadoras de cartão de crédito

2.3.3 Relação entre incentivos e barreiras para o consumidor e o vendedor

Em geral, pode-se perceber que existe uma grande semelhança entre os incentivos e barreiras para o consumidor e o vendedor, como, por exemplo, a necessidade do sistema ser de fácil utilização e não ter a necessidade de adquirir um aparelho de telefone celular novo.

Mesmo assim, em alguns casos pode-se perceber que uma característica que é um incentivador para o consumidor, no caso de não existir, torna-se uma barreira para o vendedor, como, por exemplo, ser operado por uma instituição confiável.

Na hora de elaborar um sistema de pagamento móvel todas estas características devem ser levadas em consideração, mas deve ser feito uma avaliação de custo/benefício de se implementar cada uma.

3 TECNOLOGIAS PARA IMPLEMENTAÇÃO DE SISTEMAS DE PAGAMENTO MÓVEL

Existem diversas tecnologias para implementação de sistemas de pagamento móveis, sendo SMS, internet móvel e aplicativos para telefones celulares as mais comuns. A escolha de uma tecnologia específica tem suas vantagens e desvantagens, e não existe uma ideal para todos os sistemas. Desta forma, a tecnologia tem que ser escolhida de acordo com as necessidades de cada sistema (MMA, 2009).

3.1 Short Message Service (SMS)

O SMS é a tecnologia mais comumente utilizada para sistemas de pagamento móvel pelo fato de a grande maioria dos telefones celulares possuírem esta tecnologia.

Um exemplo de funcionamento de sistema de pagamento móvel utilizando SMS seria:

1) O vendedor envia um SMS para o número de telefone celular vinculado ao sistema de pagamento móvel com o valor da transação, o tipo de transação e o código do consumidor (o código do consumidor pode ser, por exemplo, o seu número de telefone celular);
2) O consumidor recebe um SMS com o nome do vendedor e o valor da transação;
3) O consumidor responde a este SMS com sua senha, autorizando a transação;
4) Ambos, vendedor e consumidor, recebem um SMS confirmando que a transação ocorreu com sucesso.

3.1.1 Vantagens e Desvantagens

Vantagens:

- Funciona na grande maioria dos telefones celulares
- Os usuários estão acostumados a utilizar SMS
- Não necessita instalação de aplicativo no telefone celular
- Funciona com qualquer operadora
- As mensagens de confirmação podem ser acessadas posteriormente sem necessidade de conexão a uma rede

Desvantagens:

- O usuário precisa memorizar o formato e os códigos utilizados no SMS;

- É necessário possuir acordo com cada operadora para ter acesso à rede SMS, ou utilizar uma empresa agregadora de SMS que tenha acordo com as operadoras;
- O ambiente não é seguro
- Não existe garantia de quanto tempo um SMS vai demorar a ser entregue, e nem que ele será entregue (CARVALHO, 2009)

3.2 Internet móvel

A utilização da internet móvel tem emergido como uma boa opção em detrimento do uso do SMS como tecnologia para implementação de sistemas de pagamento móvel, devido a fatores como o aumento do número de telefones celular que possuem acesso a internet, o maior nível de segurança e uma base relevante de potenciais consumidores.

O funcionamento de sistemas de pagamento móvel utilizando internet móvel é similar ao funcionamento de sistemas de pagamento online, tornando sua implementação mais rápida em casos onde o sistema de pagamento online já existe. Além disso, os mesmos níveis de segurança podem ser considerados para ambos, ou seja, conforme citado no item 2.2, ambos satisfazem os requisitos mínimos de segurança.

Um exemplo de funcionamento de sistema de pagamento móvel utilizando internet móvel seria:

1) O vendedor acessa o site do sistema de pagamento móvel, efetua o login na sua conta utilizando seu usuário e senha;
2) O vendedor faz uma solicitação de cobrança para o cliente;
3) O consumidor acessa o site do sistema de pagamento móvel no seu telefone celular e efetua o login na sua conta utilizando usuário e senha;
4) O consumidor visualiza os dados e autoriza a transação;
5) O vendedor visualiza no site que a transação ocorreu com sucesso.

3.2.1 Vantagens e Desvantagens

Vantagens:

- Os usuários já estão acostumados com a experiência de navegar na internet;
- A interface proporciona uma melhor experiência de uso;
- Possibilita que o usuário utilize o mesmo sistema para pagamentos online;
- Conexões seguras podem ser estabelecidas com a maioria dos browsers.

Desvantagens:

- Existência de uma diversidade de browsers que nem sempre seguem os padrões, sendo necessária a adaptação do site para cada browser;
- Inconsistência na experiência do usuário devido à variedade de velocidades de conexão e limitações do telefone celular;
- Necessidade de o cliente ter um plano de dados, o que pode ser uma barreira para adoção;

- Impossibilidade de utilizar o sistema quando o sinal do celular for muito fraco para permitir o envio de dados.

3.3 Aplicativos com uso da rede de dados

Com o surgimento de novas plataformas para telefones celulares como iPhone OS e Android, aumentou o interesse de desenvolvedores em aplicativos para telefones celulares e fez com que houvesse uma grande evolução nos recursos disponíveis para o desenvolvimento destas aplicações.

Os sistemas de pagamento móvel que utilizam aplicativos instalados no telefone celular têm a sua disposição, em comparação com outras tecnologias, uma gama maior de recursos de segurança e melhores recursos para criação da interface com o usuário.

Os grandes problemas desta tecnologia são a existência de poucos telefones que permitem a instalação de novos aplicativos e uma grande fragmentação no mercado de plataformas para telefones celulares.

Um exemplo de funcionamento de sistema de pagamento móvel utilizando aplicativo instalado no telefone celular seria:

1) O vendedor acessa o aplicativo no seu celular, efetua o login na sua conta utilizando usuário e senha;
2) O vendedor faz uma solicitação de cobrança para o consumidor através do aplicativo;
3) O consumidor acessa o aplicativo no seu celular e efetua o login na sua conta utilizando usuário e senha;
4) O consumidor visualiza os dados e autoriza a transação através do aplicativo;
5) O vendedor visualiza que a transação ocorreu com sucesso através do aplicativo.

3.3.1 Vantagens e Desvantagens

Vantagens:

- Interface com o usuário mais rica;
- Possibilidade de armazenar dados no celular, como comprovantes de transações, para visualização mesmo quando não existe conexão a rede;
- Maior número de recursos de segurança;
- Possibilidade de apagar os dados armazenados no telefone celular remotamente em caso de perda ou roubo.

Desvantagens:

- Devido à grande diversidade de plataformas e dispositivos, é praticamente inviável suportar todos;
- Inconsistência na experiência do usuário devido à diferença de recursos disponíveis e desempenho dos telefones celulares;
- Possibilidade de aumento no número de requisições para equipe de suporte técnico;

- Dificuldade de instalação das aplicações nos telefones celulares;
- Necessidade de o cliente ter um plano de dados, o que pode ser uma barreira para adoção;
- Baixa base de potenciais clientes.

3.4 Outras tecnologias

Além das tecnologias já descritas, existem outras não tão utilizadas ou que são um híbrido de uma ou mais tecnologias. Alguns exemplos são:

- **SMS Seguro (ou aplicativos com uso de SMS para comunicação) -** Possui funcionamento similar a aplicativos com uso da rede de dados, mas normalmente por razões de custos fazem a comunicação com o servidor através de SMS (MMA, 2009).
- **Canal de voz** – Utiliza-se do canal de voz para transmissão de dados criptografados (LEE, 2004).
- **USSD** – Tecnologia disponível somente em redes GSM, mas não implementada em todas. Tem funcionamento similar ao SMS, com algumas vantagens e desvantagens em relação a este (VAN, 2009).
- **NFC** – Faz uso de um microchip com capacidade para comunicação em curta distância para efetuar a transmissão de dados. Na maioria do sistemas que utiliza NFC o vendedor necessita ter um terminal POS, similar a de cartões de crédito, que se comunica com o celular do consumidor via NFC e tem conexão com servidor do sistema (VALCOURT, 2005).

4 EXEMPLOS DE SISTEMAS DE PAGAMENTO MÓVEL NO BRASIL

A seguir são apresentados alguns exemplos de sistemas de pagamento móvel no Brasil, mas devido à falta de informações disponíveis, não será possível apresentar muitos detalhes técnicos.

Tabela 4.1: Exemplos de sistemas de pagamento móvel no Brasil

Nome	Número de usuários	Número de estabeleci-mentos cre-denciados	Tecnologia	Disponibi-lidade	Cenários de Transação Possíveis
Oi Paggo	250 mil	75 mil	SMS	21 cidades / somente para cliente Oi	Comércio eletrônico e compra em loja física.
Novo e-Pay	26 mil	1,8 mil	N-token e SMS	IND	Comércio eletrônico e compra em loja física.
BB Visa Mobile Pay	IND	11 redes	SMS e internet móvel	Somente para clientes BB	Comércio eletrônico e compra em loja física.
Wappa	50 mil	11 mil	IND	IND	IND

4.1 Oi Paggo

O Oi Paggo surgiu em 2007 através de uma parceria entre a operadora de telefonia Oi e a Paggo Administradora de Crédito, sendo a segunda, adquirida pela Oi no final de 2007 (WIKIPEDIA, 2010). Atualmente ela está presente em 21 cidades no Brasil (ONDE, 2010), tem uma carteira de 250 mil usuários e 75 mil estabelecimentos credenciados (CARDS, 2010).

O sistema opera de maneira similar a empresas de cartão de crédito, ou seja, o consumidor recebe uma fatura mensal referente às compras efetuadas e o vendedor é pago 30 dias após a transação. Para utilizar o sistema é necessário fazer um cadastro, que é sujeito a aprovação de crédito, junto à operadora (PERGUNTAS, 2010).

O sistema funciona através de SMS e a aprovação da transação é feita pelo cliente com o uso de uma senha pessoal. Não está claro no site da empresa se o sistema utiliza algum aplicativo instalado no telefone celular do vendedor, mas pelas animações demonstrativas do sistema, é muito provável que isto aconteça (COMO, 2010).

Em relação à segurança, o site da empresa somente informa que as transações são seguras, pois utilizam a tecnologia GSM e o cliente precisa digitar uma senha secreta para efetuar a transação, mas não apresenta mais detalhes sobre isso (PERGUNTAS, 2010).

Em relação aos cenários de transação apresentados no item 2.1.1, o Oi Paggo pode ser utilizado nos cenários de comércio eletrônico, compra em loja física e, se a pessoa que vai receber o pagamento tiver uma conta de vendedor, peer-to-peer (COMO, 2010).

As principais vantagens do sistema são funcionar em um grande número de aparelhos de telefone celular, o usuário poder utilizar qualquer chip da Oi e as SMS utilizadas para efetuar a transação não terem custo para o cliente ou vendedor (PERGUNTAS, 2010).

As principais desvantagens do sistema são somente estar disponível para clientes da operadora Oi e o vendedor ser obrigado a comprar um chip específico para o Oi Paggo (PERGUNTAS, 2010).

4.2 Novo e-pay

O Novo e-pay foi lançado em 2008, conta com uma carteira de 26 mil clientes e cerca 1,8 mil estabelecimentos cadastrados. Em 2009 a empresa movimentou 2,82 milhões de reais em seu sistema (SERRANO, 2010).

O Novo e-pay opera de maneira similar a cartões de crédito e o cliente recebe mensalmente a fatura para pagamento (VATAGENS, 2010).

O Novo e-pay utiliza a tecnologia N-token, similar aos tokens utilizados para acesso a sites de internet banking, e uma vez que a aplicação é instalada no celular, o sistema funciona sem necessidade de conexão de rede ou envio de SMS, funcionando até em situações onde o aparelho de celular não tem sinal (COMO, 2010).

Em relação à segurança, o site da empresa relata que o sistema possui recursos de autenticação, autorização, integridade, não repúdio e confidencialidade, mas não deixa claro como isto é implementado (SEGURANÇA, 2010).

Em relação aos cenários de transação apresentados no item 2.1.1, o Novo e-pay pode ser utilizado nos cenários de comércio eletrônico, compra em loja física e, se a pessoa que vai receber o pagamento tiver uma conta de vendedor, peer-to-peer (COMO, 2010).

A principal vantagem do sistema é funcionar mesmo que o aparelho de celular não tenha sinal, desde que o vendedor tenha acesso ao sistema pela internet.

As principais desvantagens do sistema são somente estar disponível para clientes da operadora TIM e Oi (INSTALAÇÂO, 2010), e o pequeno número de estabelecimentos cadastrados.

4.3 BB Visa Mobile Pay

O Banco do Brasil em parceria com a Visa criou o sistema BB Visa Mobile Pay que permite clientes Ourocard efetuar pagamentos utilizando telefone celular. Atualmente contam com 11 redes de estabelecimentos parceiros (BB, 2010).

O sistema opera vinculado aos cartões de crédito e débito Ourocard. Para utilização do sistema o cliente deve cadastrar seu celular para transações financeiras na rede de atendimento do Banco do Brasil (BB, 2010)

Ao fazer uma compra em um estabelecimento credenciado, o cliente deve informar o número de seu telefone celular e se a operação é de débito ou crédito. Para compras até 100 reais diários o usuário recebe um SMS para confirmar a compra e para valores maiores deve autorizar a transação no auto-atendimento do Banco do Brasil pelo celular ou no auto-atendimento pela Internet (BB, 2010).

Em relação aos cenários de transação apresentados no item 2.1.1, o BB Visa Mobile Pay pode ser utilizado nos cenários de comércio eletrônico e compra em loja física.

A principal vantagem deste sistema é a integração com os sistemas do Banco do Brasil, sem a necessidade do usuário criar uma nova conta.

As principais desvantagens do sistema são somente estar disponível para clientes do Banco do Brasil que tem cartões Ourocard e a complexidade na hora de autorizar o pagamento, já que existem dois processos diferentes.

4.4 Wappa

A Wappa é uma empresa focada no mercado de despesas corporativas como Táxi, Refeição, Combustível e Alimentação, utilizando SMS (SOBRE, 2010), e conta com 11 mil taxistas cadastrados e 50 mil usuários (SERRANO, 2010).

4.5 Mobility Pass - Sodexo

A Sodexo lançou em 2009 o Mobility Pass, um sistema de pagamento móvel focado no mercado de despesas corporativas com Táxi, concorrendo com a Wappa (MIWA, 2009).

4.6 M-Ca$h

A M-Ca$h foi criada em 2004 e ao contrário dos exemplos anteriores não possui um sistema de pagamento móvel próprio, mas desenvolve soluções de pagamento móvel para outras empresas como, por exemplo, para Sodexo citada acima. No site da empresa é citado que eles trabalham com soluções compatíveis com qualquer tecnologia de telefonia celular, mas sem apresentar mais detalhes (EMPRESA, 2010).

4.7 Banrisul

O Banrisul foi um dos pioneiros no Brasil em sistemas de pagamento móvel, lançando em 2007 um projeto piloto chamado Banrisul Celular que permitia fazer pagamentos em estabelecimentos credenciados à rede Banricompras no litoral norte do estado do Rio Grande do Sul (BANRISUL, 2007).

O projeto foi feito em parceria com a operadora de telefonia celular Claro e utilizava um aplicativo instalado no celular do usuário, desenvolvido com a tecnologia J2ME (BANRISUL, 2007).

A principal vantagem deste sistema era a integração com os sistemas do Banrisul, sem haver a necessidade de o usuário criar uma nova conta.

As desvantagens deste sistema eram somente estar disponível para clientes do Banrisul que também fossem clientes da Claro, o restrito número de aparelhos compatíveis com o sistema e o restrito número de estabelecimentos habilitados.

As últimas informações sobre este projeto são de 2007 e desde então não existem mais informações disponíveis. Atualmente o sistema não existe mais e o Banrisul tem um sistema de mobile banking chamado M-Banking Banrisul, mas somente é possível efetuar operações similares a sistemas de internet banking (M-BANKING, 2010).

4.8 Outros exemplos

Um grupo formado pelas empresas Mastercard, Redecard, Itaú Unibanco e Vivo, e outro grupo formado pelas empresas Banco do Brasil, Bradesco, Claro, Visa e Cielo, estão desenvolvendo soluções de pagamento móvel que devem estar disponíveis no segundo semestre de 2010 (GUEDES, 2010).

5 PROPOSTA DE ARQUITETURA DE SISTEMA DE PAGAMENTOS MÓVEL

Neste capítulo será apresentada uma proposta de arquitetura para implementação de sistemas de pagamento móvel baseado nas informações apresentadas nos capítulos anteriores deste trabalho.

O objetivo de propor uma arquitetura de sistema e não um sistema completo ou uma implementação de um sistema, é permitir apresentar uma solução altamente adaptável e que possa ser utilizada independentemente da tecnologia ou linguagem utilizada para implementação devido a constante e rápida evolução nas tecnologias de telefonia móvel.

Além disso, o sistema a ser apresentado não abordará por completo a complexidade de um sistema de pagamentos móvel, e sim focará no aspecto da comunicação entre a aplicação cliente e o servidor, e na arquitetura do servidor. Esta decisão deve-se ao fato de que os aspectos de segurança e manipulação das transações financeiras pelo agente financeiro são complexos e não diferem de outros sistemas bancários. Sendo o conhecimento nesta área já amplamente difundido e regido por regulamentações do setor financeiro, foge do escopo deste trabalho apresentar novas idéias nesta área.

5.1 Modelagem do sistema

Inicialmente será feita uma análise dos requisitos do sistema e, baseada nesta, serão apresentados as principais funcionalidades do sistema.

5.1.1 Análise de requisitos

Antes de definirmos os detalhes da arquitetura do sistema é necessário fazer uma análise dos requisitos funcionais e não-funcionais do sistema. Está análise será feita com base no estudo apresentado no capítulo 2.

5.1.1.1 Requisitos funcionais

O objetivo principal do sistema é permitir a transferência de valores de um consumidor para um vendedor de forma a efetuar o pagamento da compra de produtos e/ou serviços. Desta forma ele deve ter no mínimo as seguintes funcionalidades:

- Permitir o vendedor solicitar uma cobrança de um consumidor em específico;
- Permitir o consumidor autorizar ou proibir o pagamento de uma cobrança pendente;

- Permitir um usuário obter detalhes de uma transação para que seja possível verificar se esta ocorreu com sucesso.

Algumas outras funcionalidades também são necessárias para permitir que os usuários tenham um maior controle sobre suas contas e sobre as transações:

- Permitir o vendedor cancelar uma cobrança caso alguma informação esteja incorreta;
- Permitir um usuário obter uma lista das suas transações;
- Permitir um usuário verificar o saldo de sua conta.

5.1.1.2 Requisitos não-funcionais

Para que o sistema esteja completo é necessário fazer um levantamento dos requisitos não funcionais deste sistema:

- As transações devem ser possíveis em todos os cenários do item 2.1.1.
- Deve satisfazer os requisitos de segurança apresentados no item 2.2;
- Cada usuário pode ter mais de uma conta no sistema, mas cada conta está associada a somente um número de telefone celular. No caso de vendedores, a conta não precisa necessariamente estar associada a um número de telefone celular;
- Cada conta deve ter um código e uma senha associada;
- Deve suportar o maior número possível de dispositivos móveis;
- Deve ser fácil de utilizar;
- A operação de pagamento deve ser rápida;
- Deve ser escalável para acompanhar o crescimento no volume de transações.

5.1.2 Funcionalidades do sistema

A figura 5.1 apresenta o diagrama de casos de uso para as principais funcionalidades do sistema.

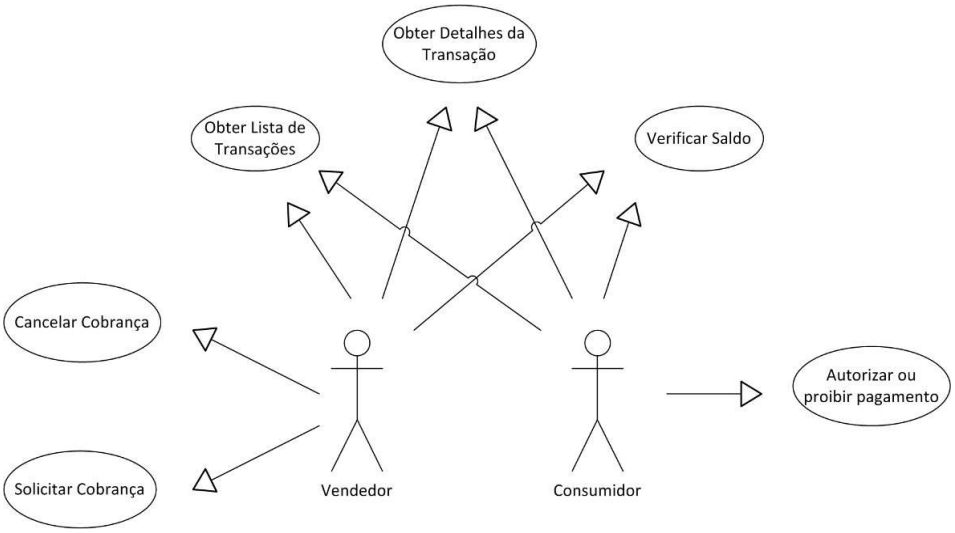

Figura 5.1: Diagrama de casos de uso

5.1.2.1 Solicitar cobrança

Está funcionalidade é utilizada quando o vendedor deseja solicitar a cobrança de um pagamento relativo a uma despesa efetuada pelo consumidor.

A figura 5.2 mostra em alto nível o diagrama de seqüência de uma operação de solicitação de cobrança. Esta operação é composta pelas seguintes etapas:

1. A aplicação cliente utilizada pelo vendedor solicita a criação de uma nova transação ao serviço web. Para isso são enviados os dados do vendedor para autenticação, o código do comprador e o valor da transação;
2. O serviço web solicita os dados do vendedor ao banco de dados para autenticá-lo;
3. O banco de dados retorna os dados do vendedor para o serviço web;
4. O serviço web autentica o vendedor;
5. O serviço web solicita a criação de uma nova transação ao servidor do agente financeiro;
6. O servidor do agente financeiro retorna o código da transação para o serviço web;
7. O serviço web repassa o código da transação para a aplicação cliente.

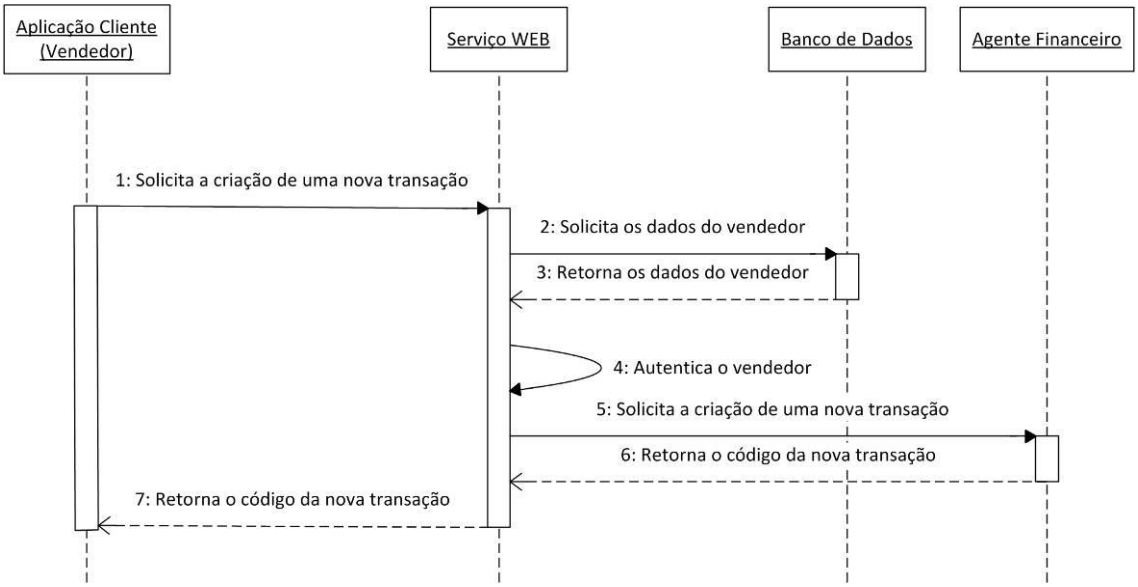

Figura 5.2: Diagrama de seqüência – Solicitar cobrança

5.1.2.2 Cancelar cobrança

Está funcionalidade é utilizada pelo vendedor para cancelar uma cobrança pendente caso alguma dado desta esteja incorreto ou o comprador desista da transação.

A figura 5.3 mostra o diagrama de seqüência de uma operação de cancelamento de cobrança. Esta operação é composta pelas seguintes etapas:

1. A aplicação cliente utilizada pelo vendedor solicita o cancelamento de uma transação ao serviço web. Para isso são enviados os dados do vendedor para autenticação e o código da transação;

2. O serviço web solicita os dados do vendedor ao banco de dados para autenticá-lo;
3. O banco de dados retorna os dados do vendedor para o serviço web;
4. O serviço web autentica o vendedor;
5. O serviço web solicita o cancelamento de uma transação ao servidor do agente financeiro;
6. O servidor do agente financeiro retorna os dados da transação para o serviço web;
7. O serviço web repassa os dados da transação para a aplicação cliente.

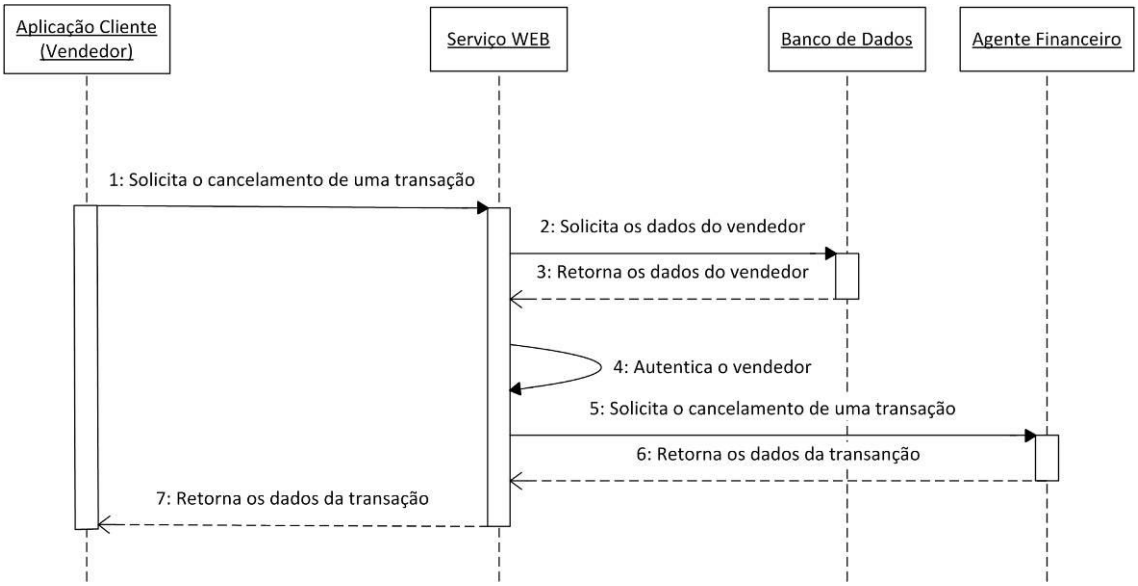

Figura 5.3: Diagrama de seqüência – Cancelar cobrança

5.1.2.3 Autorizar ou proibir o pagamento

Está funcionalidade é utilizada pelo consumidor para autorizar ou proibir o pagamento de uma cobrança.

A figura 5.4 mostra o diagrama de seqüência de uma operação de autorização de pagamento de uma cobrança. Esta operação é composta pelas seguintes etapas:

1. A aplicação cliente utilizada pelo consumidor autoriza o pagamento de uma transação ao serviço web. Para isso são enviados os dados do consumidor para autenticação e o código da transação;
2. O serviço web solicita os dados do consumidor ao banco de dados para autenticá-lo;
3. O banco de dados retorna os dados do consumidor para o serviço web;
4. O serviço web autentica o consumidor;
5. O serviço web autoriza o pagamento de uma transação ao servidor do agente financeiro;
6. O servidor do agente financeiro retorna os dados da transação para o serviço web;

7. O serviço web repassa os dados da transação para a aplicação cliente.

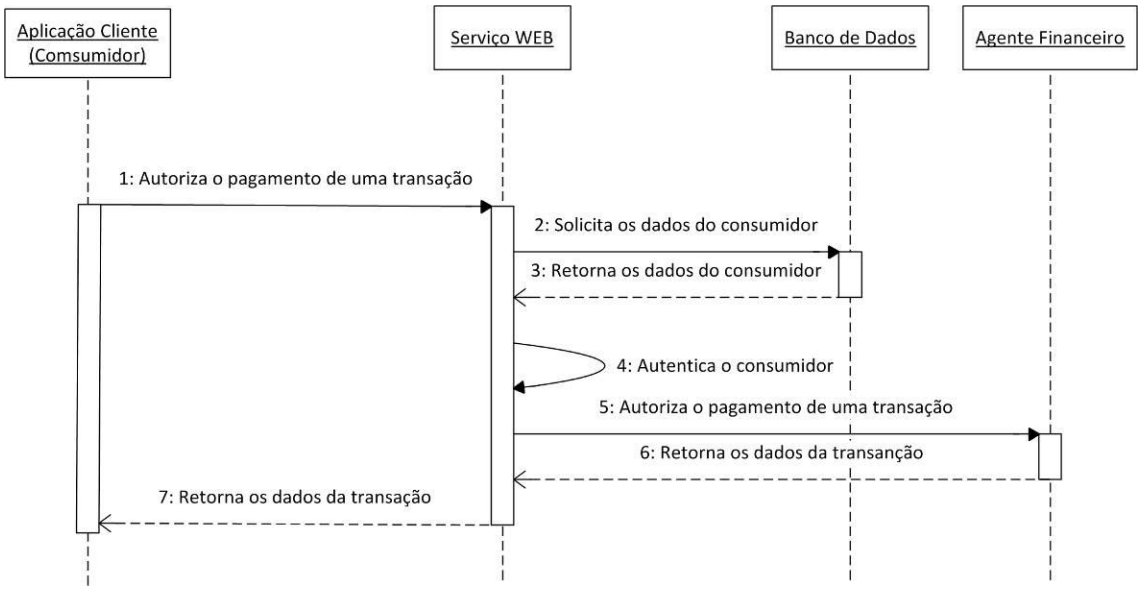

Figura 5.4: Diagrama de seqüência – Autorizar pagamento

5.1.2.4 Obter detalhes da transação

Está funcionalidade é utilizada pelo usuário para obter de detalhes de uma transação. Pode, por exemplo, ser utilizada pelo vendedor para verificar se o pagamento da transação foi efetuado com sucesso.

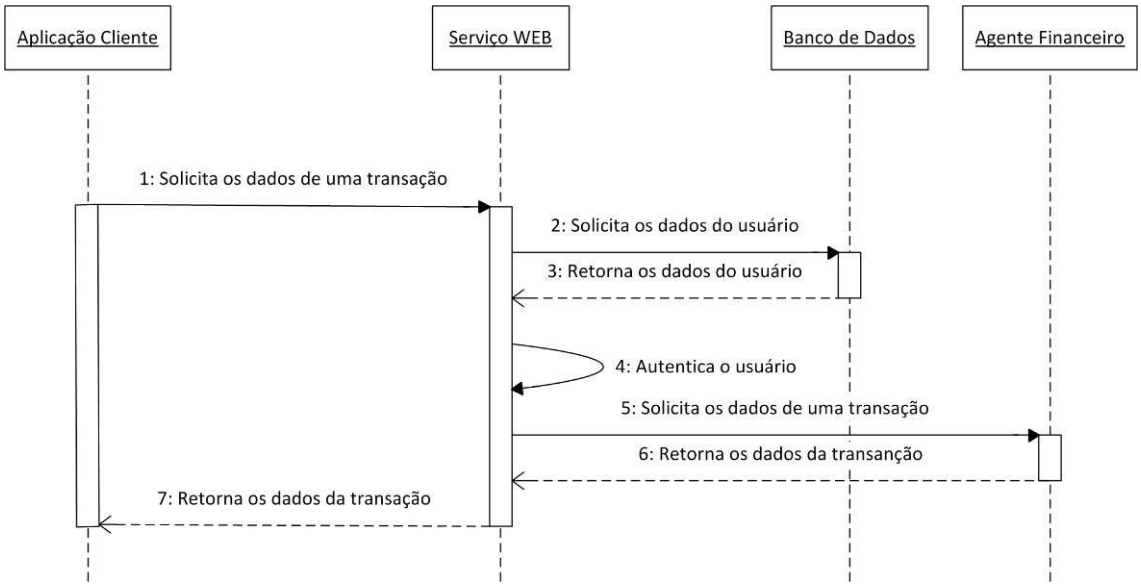

Figura 5.5: Diagrama de seqüência – Obter detalhes da transação

A figura 5.5 mostra o diagrama de seqüência de uma operação para obter detalhes de uma transação. Esta operação é composta pelas seguintes etapas:

1. A aplicação cliente solicita os dados de uma transação ao serviço web. Para isso são enviados os dados do usuário para autenticação e o código da transação;

2. O serviço web solicita os dados do usuário ao banco de dados para autenticá-lo;
3. O banco de dados retorna os dados do usuário para o serviço web;
4. O serviço web autentica o usuário;
5. O serviço web solicita os dados de uma transação ao servidor do agente financeiro;
6. O servidor do agente financeiro retorna os dados da transação para o serviço web;
7. O serviço web repassa os dados da transação para a aplicação cliente.

5.1.2.5 Obter lista de transações

Está funcionalidade é utilizada pelo usuário para obter uma lista de suas transações.

A figura 5.6 mostra o diagrama de seqüência de uma operação para obter uma lista de transações. Esta operação é composta pelas seguintes etapas:

1. A aplicação cliente solicita uma lista das transações do usuário ao serviço web. Para isso são enviados os dados do usuário para autenticação e parâmetros para filtrar a lista, por exemplo, período em que ocorreram as transações;
2. O serviço web solicita os dados do usuário ao banco de dados para autenticá-lo;
3. O banco de dados retorna os dados do usuário para o serviço web;
4. O serviço web autentica o usuário;
5. O serviço web solicita a lista das transações ao servidor do agente financeiro;
6. O servidor do agente financeiro retorna a lista com as transações para o serviço web;
7. O serviço web repassa a lista com as transações para a aplicação cliente.

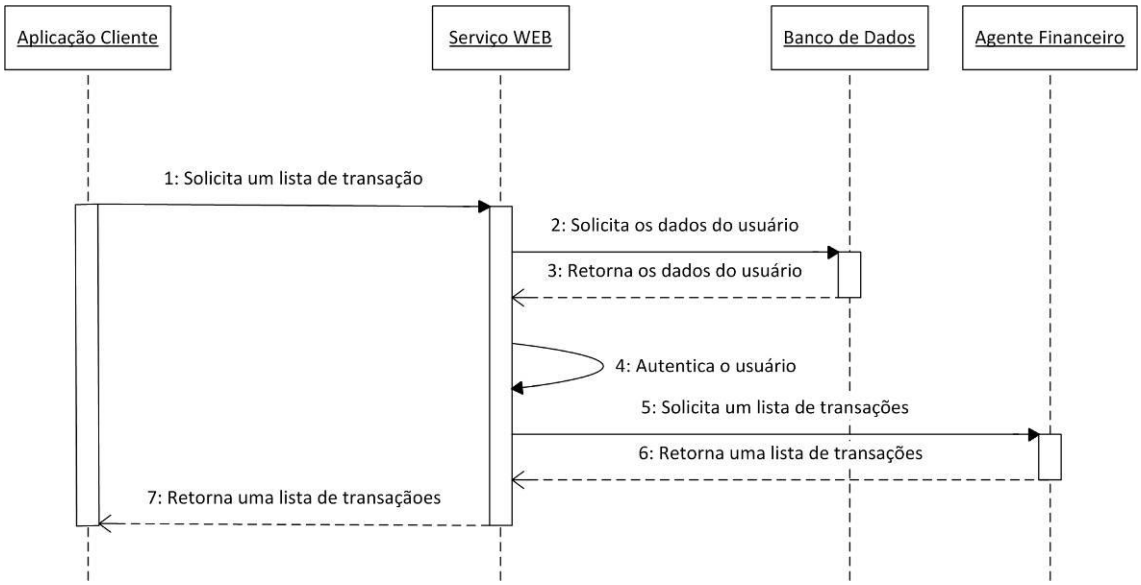

Figura 5.6: Diagrama de seqüência – Obter lista de transações

5.1.2.6 Verificar saldo

Está funcionalidade é utilizada pelo usuário verificar o saldo de sua conta.

A figura 5.7 mostra o diagrama de seqüência de uma operação de verificação de saldo. Esta operação é composta pelas seguintes etapas:

1. A aplicação cliente solicita o saldo da conta do usuário ao serviço web. Para isso são enviados os dados do usuário para autenticação;
2. O serviço web solicita os dados do usuário ao banco de dados para autenticá-lo;
3. O banco de dados retorna os dados do usuário para o serviço web;
4. O serviço web autentica o usuário;
5. O serviço web solicita o saldo da conta ao servidor do agente financeiro;
6. O servidor do agente financeiro retorna o saldo da conta para o serviço web;
7. O serviço web repassa o saldo da conta para a aplicação cliente.

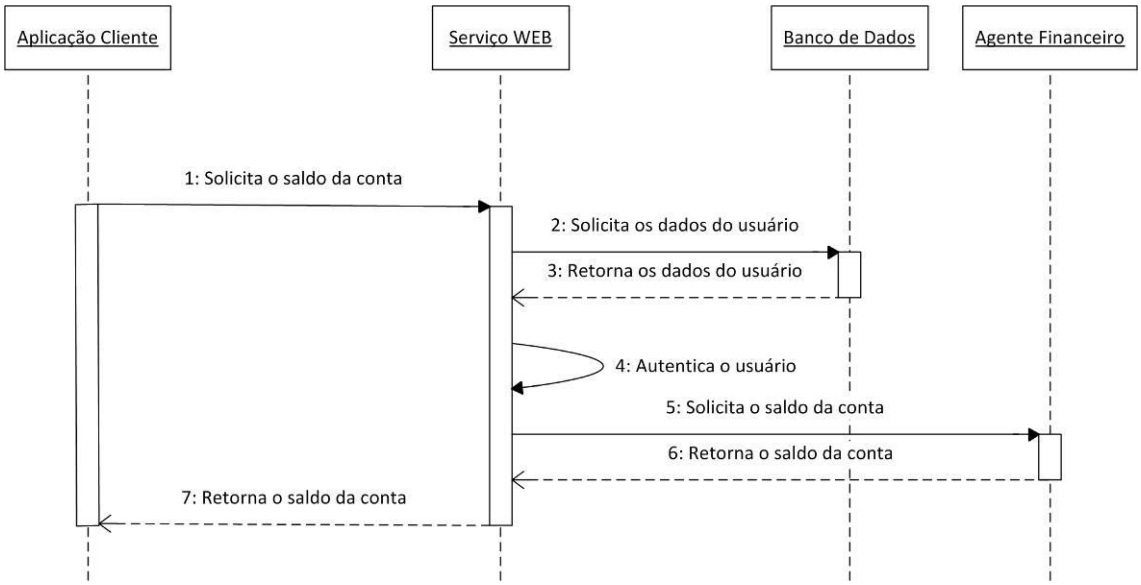

Figura 5.7: Diagrama de seqüência – Verificar saldo

5.2 Visão geral da arquitetura do sistema

A arquitetura de sistema proposta, como pode ser visto na figura 5.8, faz o uso de um servidor intermediário entre as aplicações clientes do vendedor e consumidor, na figura denominadas clientes e sem distinção entre as entidades, e o servidor do agente financeiro, mantendo o controle das transações.

Não há em nenhum momento comunicação direta entre as aplicações clientes do vendedor e do consumidor, e estas não precisam armazenar nenhuma informação relativa às transações, a não ser caso o usuário tenha interesse de mantê-la armazenadas para conferência sem a necessidade de conexão com o servidor.

Analisando em mais detalhes a figura 5.8, podemos separar o sistema nos seguintes componentes:

- Aplicações clientes: são utilizadas pelos usuários do sistema para efetuar as transações. Podem ser utilizadas diversas tecnologias para sua implementação.
- Servidor: é composto por dois ou mais sub-componentes, sendo o principal o serviço web que recebe as requisições das aplicações clientes, autentica os usuários, controla as transações e faz a intermediação da comunicação com os servidores do agente financeiro. Além do serviço web, o servidor tem um banco de dados para armazenamento das informações dos clientes e das transações, e pode ter outros componentes que servem de adaptadores para permitir a comunicação do serviço web com aplicação cliente que não tem recursos para isso.
- Servidores do agente financeiro: é o responsável pelo armazenamento das informações financeiras dos usuários e concretização das transações.

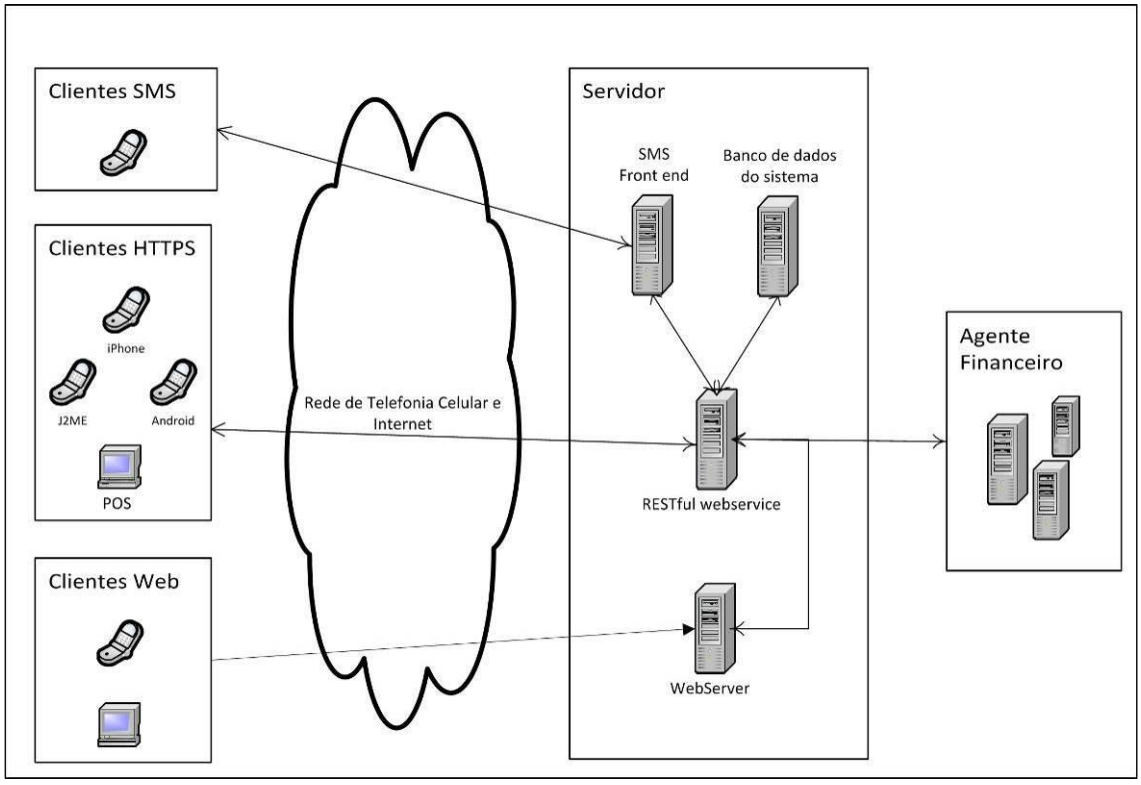

Figura 5.8: Visão geral da arquitetura do sistema

5.2.1 Serviço Web

Como o servidor do sistema faz a intermediação da comunicação entre os diversos componentes do sistema, sendo que estes podem ser desenvolvidos em diferentes plataformas, foi feita uma análise de possíveis metodologias para sua implementação.

Após esta análise, que pode ser vista em maiores detalhes abaixo, optou-se por utilizar um serviço web baseado no estilo de arquitetura de software Transferência de Estado Representacional (REST), sendo os principais fatores que levaram a esta decisão:

- Independência de tecnologia/linguagem de programação;
- Uso de padrões da web disponíveis em diversas plataformas;

- Alto grau de desacoplamento entre aplicação cliente e servidor;

5.2.1.1 Análise de técnicas de comunicação entre aplicações através de redes de computadores

As técnicas para comunicação entre aplicações através de redes de computadores podem ser dividas em duas categorias: mecanismos de comunicação entre processos e arquiteturas baseadas em serviços web. Alguns exemplos de mecanismos de comunicação entre processo são internet sockets e .NET Remoting, e de serviços web são Simple Object Access Protocol (SOAP) e REST.

Como mecanismos de comunicação entre processos são muito ligados a tecnologia/linguagem de programação utilizada, não é boa opção para sistemas onde as aplicações clientes precisam ser desenvolvidas utilizando tecnologias variadas, como é o caso de sistemas que tem como plataformas cliente dispositivos móveis.

Desta forma, optou-se pelo uso de uma arquitetura baseada em serviços web que, em geral, permitem a comunicação entre aplicações desenvolvidas com diferentes tecnologias/linguagens de programação sem grandes dificuldades.

5.2.1.2 Análise de serviços web

Serviços web são tipicamente interfaces de programação de aplicativos (API) acessadas através de protocolo de transferência de hipertexto (HTTP) e executadas no sistema remoto que hospeda o serviço. Eles podem ser implementados utilizando diversas tecnologias e podem ter diferentes funcionalidades. Os três estilos mais comuns de serviços web são: chamada de procedimento remoto (RPC), SOAP e REST.

O RPC, dependendo do seu uso, também pode ser classificado com um mecanismo de comunicação entre processos e, da mesma forma que outros exemplos destes, está bastante ligado à tecnologia usada na implementação das aplicações.

O SOAP é uma especificação de protocolo muito utilizada atualmente para implementação de serviços web e, diferente de mecanismos de comunicação entre processos, permite a comunicação entre aplicações desenvolvidas para diferentes plataformas. Devido a sua complexidade, o que muitas vezes cria acoplamento entre a aplicação cliente e o servidor, tem perdido espaço para serviços web baseados no REST.

O REST é um estilo de arquitetura de software para sistemas de hipermídia distribuídos definido na dissertação de doutorado de Fielding (2000), tendo como maior exemplo a World Wide Web.

O estilo de arquitetura REST consiste de clientes e servidores. Clientes iniciam a requisição ao servidor; servidores processam a requisição e retornam a resposta apropriada. Requisições e respostas são construídas através da transferência de representações de recursos. Nenhuma informação de estado é armazenada no servidor, sendo está obrigação do cliente. Sendo que cada vez que o cliente enviar uma requisição ao servidor é porque está pronto para mudar de estado.

Apesar de não ser um padrão, serviços web baseados em REST fazem o uso de vários padrões da Web com HTTP, URL, XML, PNG, etc. Sendo assim, o desenvolvimento de aplicações clientes torna-se mais simples em comparação com outras tecnologias, já que muitos dos recursos necessários para desenvolvimento da aplicação cliente já estão disponíveis nas linguagens de programação.

Como existe uma separação clara entre o servidor e o cliente, as possibilidades de transição de estados são informadas pelo servidor ao cliente e todo controle de estados é feito pelo cliente, é possível desenvolver novos recursos no servidor sem afetar um cliente existente e é possível desenvolver clientes com apenas alguns funcionalidades específicas.

Também, de acordo com Tyagi (2006), REST é recomendado para uso com dispositivos com recursos limitados, como PDAs e aparelhos de telefone celular, por ter um baixo overhead na comunicação.

5.2.2 Aplicações Clientes

Não é o objetivo entrar em detalhes sobre as aplicações clientes, sendo as funcionalidades implementadas em cada uma baseada na necessidade dos usuários desta aplicação cliente em específico.

As aplicações clientes podem ser desenvolvidas em diversas plataformas, sendo as únicas restrições suporte ao protocolo HTTPS e ao formato de dados utilizado pelo serviço web. Mas mesmo nesses casos, é possível criar adaptadores que servem como intermediários entre o serviço web e a plataforma incompatível.

Podemos dividir as aplicações clientes nas seguintes categorias:

- Aplicações nativas para plataformas móveis: como aplicativos para iPhone, Android, BlackBerry e Symbian;
- Aplicações para ambiente de run-time para plataformas móveis: como aplicativos desenvolvidos utilizando a tecnologia J2ME;
- Aplicações para plataformas tradicionais: como aplicativos para Windows, Linux e Unix, permitindo que o sistema possa ser integrado a sistemas de ponto de venda já utilizados pelos vendedores;
- Adaptadores: servem como intermediários entre o serviço web e a plataforma incompatível. Dois exemplos de adaptadores são mostrados na figura 4.1, onde temos o SMS Front-end que permite que a comunicação entre o dispositivo cliente e o servidor seja feita por SMS, e o WebServer que permite que o sistema seja utilizado através de um web browser. Estas aplicações podem ter algumas limitações, por exemplo, não existe garantia de que a comunicação por SMS seja segura.

5.3 Aspectos de segurança

Como mencionado no item 2.2, existem alguns requisitos de segurança que devem ser seguidos para que um sistema de pagamento móvel seja considerado seguro, sendo eles: autenticação, privacidade, integridade, autorização e não repúdio.

5.3.1 Transmissão segura de dados

A transmissão segura de dados engloba parte dos requisitos de privacidade e integridade. Na arquitetura apresentada existem quarto pontos onde ocorre a transmissão de dados: entre uma aplicação cliente e o serviço web, entre o serviço web e o banco de dados, entre o serviço web e o servidor agente financeiro, e entre uma aplicação cliente e um adaptador.

5.3.1.1 Comunicação entre uma aplicação cliente e serviço web

Para garantir a transmissão segura de dados entre a aplicação cliente e o servidor é utilizado o protocolo HTTPS, que faz o uso de SSL ou TSL para criptografar os dados transmitidos e também pode ser usado para garantir a autenticidade das aplicações clientes e do servidor.

5.3.1.2 Comunicação entre o serviço web e o banco de dados

A garantia de transmissão segura de dados entre o serviço web e o banco de dados vai depender de como o sistema é implementado. Recomenda-se que a máquina onde é executado o banco de dados não esteja ligada diretamente a internet, ou seja, não esteja na mesma máquina do serviço web.

Uma maneira de garantir a transmissão de dados segura nesta comunicação é também utilizar o protocolo HTTPS.

5.3.1.3 Comunicação entre o serviço web e o servidor do agente financeiro

Os requisitos referentes a esta comunicação são normalmente estabelecidos pelo agente financeiro, que pode ter uma série de restrições sobre as máquinas e canais de comunicação envolvidos.

5.3.1.4 Comunicação entre uma aplicação cliente e um adaptador

A garantia da transmissão segura nesta comunicação depende do tipo de aplicação cliente e canal de comunicação utilizado.

Podemos utilizar como exemplo o uso do SMS como canal de comunicação. Nesta situação a garantia de transmissão segura de dados deve ser dada pelo responsável pela rede SMS, e qualquer dado armazenado no adaptador deve ser criptografado.

5.3.2 Controle da aplicação e do acesso a dados

O controle da aplicação e do acesso a dados engloba parte dos requisitos de autenticação, autorização e não-repúdio.

5.3.2.1 Autenticação do usuário

A RFC 2617, que trata de autenticação no protocolo HTTP, apresenta dois métodos de autenticação: básica e *digest*. Resumidamente, o método básico envia um identificador do usuário e uma senha na forma de texto puro, e o método *digest* recebe do servidor uma informação que deve ser utilizada junto com os dados do usuário para criação de um *message digest* que enviado para o servidor para autenticação.

Ambos podem ser utilizados para autenticação do usuário em conexões seguras utilizando HTTPS, mas, como não existe controle de sessão no lado do servidor em serviços web baseados em REST e o usuário deve ser autenticado a cada comunicação com o serviço web, e o método *digest* necessita o envio de duas mensagens ao servidor para cada comunicação, o método básico torna-se mais interessante em redes com alta latência como as redes de dados de telefonia celular.

5.3.2.2 Autorização

Uma vez que o usuário está autenticado no sistema, esta informação pode ser utilizada para verificar se este tem direito de acesso a um determinado recurso/dado. Como é feita está verificação fica a cargo de como o sistema é implementado.

5.3.2.3 Não-repúdio

Como o usuário somente tem acesso ao sistema através do uso de sua senha pessoal e cada usuário tem acesso limitado a recursos relacionados a ele, a única maneira de efetuar uma transação no lugar de um usuário é estando de posse de sua senha pessoal.

Desta maneira, é garantido o não repúdio através da presunção de que somente o usuário sabe sua senha pessoal. Além disso, na implementação do sistema, é recomendável criar *logs* das transações e criar assinaturas das transações utilizando a senha do usuário de forma de que transações contestadas possam ser verificadas.

Para casos onde a senha do usuário é roubada, é recomendável a implementação de sistemas de *back-end* que analisem as transações e verifiquem a ocorrência de transações suspeitas de fraude para que estas sejam detectadas o mais sedo possível.

5.3.3 Outros aspectos de segurança

Existem outros aspectos de segurança que também podem ser explorados em mais detalhes, mas como não faz parte do escopo deste trabalho analisar todos estes em detalhe somente serão mencionados alguns aspectos relativos a eles.

5.3.3.1 Aspectos de segurança dependentes da plataforma da aplicação cliente

Dependendo da plataforma da aplicação cliente existem algumas formas de identificar o usuário que poderiam dificultar que outra pessoa faça-se passar por este:

- Número do telefone celular;
- Número de identificação único do aparelho de telefonia celular, chamado de IMEI;
- Número de identificação único de cartões SIM, chamado de IMSI;
- Certificado digital instalado no dispositivo;

Outro aspecto dependente da plataforma da aplicação cliente é o armazenamento de dados de forma segura. Programas nocivos podem ser instalados no dispositivo para tentar roubar informações sigilosas ou o usuário pode perder o dispositivo, e em nenhum destes casos a segurança do sistema deve ser comprometida.

5.3.3.2 Vulnerabilidades de segurança comuns em serviços web

Uma das vantagens de utilizar um serviço web baseado em REST é que, por utilizar padrões amplamente utilizados na web, a grande maioria das vulnerabilidades de segurança já são amplamente conhecidas e existe vasto material de como combatê-las. Alguns exemplos destas vulnerabilidades são:

- Ataques de negação de serviço;
- Cross-site scripting;
- Phishing.

- Ataque do homem-do-meio;
- Ataques de repetição.

5.3.3.3 Armazenamento seguro de dados

Não somente o armazenamento seguro dos dados no dispositivo cliente, mas também no servidor é muito importante. Existem duas fontes importantes de informações de praticas que devem ser seguidas no desenvolvimento de sistemas como este:

- PCI Security Standards Concil, que é um fórum global aberto criado em 2006 por empresas de tecnologia de pagamentos para avaliar práticas segurança no setor financeiro, em especial no setor de pagamento;
- The Open Web Application Security Project (OWASP), que é uma organização sem fim lucrativos focada em melhor a segurança de aplicações web.

5.3.3.4 Privacidade do usuário

Normalmente em sistemas de pagamento móvel o número do telefone celular do usuário é utilizado como seu identificador, desta maneira os consumidores fornecer seu número de telefone celular para o vendedor, mas muitos usuários não se sentem confortáveis com isso. Uma maneira de evitar esta situação é criar um segundo identificar para cada usuário para que o consumidor possa optar qual fornecer ao vendedor.

6 CONCLUSÃO

O número de telefones celulares vem aumentando, assim como as funções que eles podem exercer. Neste cenário surgiu o pagamento móvel, uma tecnologia promissora, mas que na prática, ainda não conseguiu ganhar mercado em larga escala. Como pudemos analisar no desenvolvimento deste trabalho, alguns fatores influenciam a adoção desta tecnologia.

Existem diversas tecnologias que podem ser usadas para implementação de sistemas de pagamentos móveis, mas cada uma trás suas vantagens e desvantagens, não existindo uma tecnologia ideal para todos os cenários. Sendo assim existem dois caminhos que podem ser seguidos: implementar o sistema utilizando uma tecnologia específica focando em um nicho de mercado ou implementar uma solução flexível que possa abranger diversas tecnologias deixando a cargo do usuário escolher a que se encaixa melhor as suas necessidades e requisitos.

Nos exemplos de sistemas de pagamento móvel analisados, existe um foco em tecnologias específicas e, algumas vezes, so é disponibilizado a clientes de um determinado serviço. Desta maneira, fica limitada a quantidade de potenciais usuários do sistema.

Tendo todas estas informações em vista, foi proposta uma arquitetura de sistema mais flexível, onde existe uma independência entre o servidor e a aplicação cliente, para que várias tecnologias possam ser utilizadas, de acordo com a necessidade e interesse da empresa responsável pelo sistema, permitindo uma maior abrangência de potenciais usuários.

6.1 Trabalhos futuros

O trabalho apresenta um arquitetura para implementação de sistemas de pagamento móvel, mas para que esta possa evoluir para uma solução completa é necessário definir as características do sistema, como:

- Cenários de transações que devem ser suportados;
- Tipo de agente financeiro;
- Público alvo do sistema.

Com base nestas informações é possível definir uma plataforma móvel alvo e como vai ser feita a comunicação entre o servidor e o agente financeiro, e, a partir disto, fazer a prototipação do sistema.

Na fase de prototipação, será possível avaliar a fundo algumas limitações que são inerentes desta fase de desenvolvimento de um projeto de sistemas de software, como limitações das tecnologias e recursos de segurança.

REFERÊNCIAS

ANATEL. **Dados do Serviço Móvel Pessoal**. Disponível em: <http://www.anatel.gov.br:80/Portal/exibirPortalInternet.do?acao=linkInt&src=http://www.anatel.gov.br/Portal/exibirPortalPaginaEspecial.do?acao=%26codItemCanal=1087%26codigoVisao=5%26nomeVisao=Informa%E7%F5es%20T%E9cnicas%26nomeCanal=Telefonia%20M%F3vel%26nomeItemCanal=Dados%20do%20SMP%26nomeCanal=Anatel%20em%20dados%26codigoVisao=7%26site=1%26codigoVisao=5>. Acesso em: jun. 2010.

DAHLBERG, T. et al. Past, present and future of mobile payments research: A literature review. **Electronic Commerce Research and Applications**, Amsterdam, Holanda, v.7, n.2, p. 165-181, 2008.

GSM ASSOCIATION (GSMA). **Mobile Money for the Unbanked – Deployment Tracking**. Disponível em: <http://www.wirelessintelligence.com/mobile-money/>. Acesso em: jun. 2010.

GUEDES, J. Celular no lugar de dinheiro. **Zero Hora**, Porto Alegre, Brasil, p. 14, 5 abr. 2010. Disponível em: <http://zerohora.clicrbs.com.br/zerohora/jsp/default2.jsp?uf=1&local=1&source=a2861795.xml&template=3898.dwt&edition=14430&section=1008>. Acesso em: jun. 2010.

MOHAMMADI, S.; JAHANSHAHI, H. A study of major Mobile payment systems' functionality in Europe. **2008 11th International Conference on Computer and Information Technology**, Khulna, Bangladesh, p. 605-610, dez. 2008.

ZHENG, X.; CHEN, D. Study of Mobile Payments System. **2003 IEEE International Conference on E-Commerce Technology**, Newport Beach, Estados Unidos, p.24-27, jun. 2003.

VALCOURT, E.; ROBERT, J.-M.; BEAULIEU, F. Investigating mobile payment: supporting technologies, methods, and use. **2005 IEEE International Conference on Wireless And Mobile Computing, Networking And Communications**, Montreal, Canada, v. 4, p. 29-36, ago. 2005.

MOBILE MARKETING ASSOCIATION (MMA). **Mobile Banking Overview (NA)**, jan. 2009. Disponível em: <http://www.mmaglobal.com/mbankingoverview.pdf>. Acesso em: jun. 2010.

POUSTTCHI, K. An Analysis of the Mobile Payment Problem in Europe. **Multikonferenz Wirtschaftsinformatik**, Essen, Alemanha, p. 260-268, mar. 2004.

CARVALHO, D. Pagamento Móvel vai decolar?. **Blog SOA Simples Assim!**, set. 2009. Disponível em: <http://soasimples.com/blog/?p=698>. Acesso em: jun. 2010.

LEE, O. Sound-based mobile payment system. **Proceedings. 2004 IEEE International Conference on Web Services**, San Diego, Estados Unidos, p. 820-821, jul. 2004.

VAN, L. Use of USSD technology in Mobile Banking. **Long Van's Blog em Mobile-Financial.com**, ago. 2009. Disponível em: <http://www.mobile-financial.com/node/2473/Use-of-USSD-technology-in-Mobile-Banking>. Acesso em: jun. 2010.

WIKIPEDIA. **Paggo**. Disponível em: <http://pt.wikipedia.org/wiki/Paggo>. Acesso em: jun. 2010.

CARDS 2010 Blog. **Facilidade do Oi Paggo eleva em 30% o volume de recarga de celulares**, abr. 2010. Disponível em: <http://www.cards2010.com.br/blog/?p=195>. Acesso em: jun. 2010.

ONDE Estamos. **Oi Paggo – Tudo sobre o Oi Paggo**. Disponível em: <http://www.novaoi.com.br/portal/site/NovaOi/menuitem.e45de4d5df2322fb72871a31f26d02a0/?vgnextoid=bb02aadc63180210VgnVCM10000021d0200aRCRD>. Acesso em: jun. 2010.

PERGUNTAS Freqüentes. **Oi Paggo – Tudo sobre o Oi Paggo**. Disponível em: <http://www.novaoi.com.br/portal/site/NovaOi/menuitem.e45de4d5df2322fb72871a31f26d02a0/?vgnextoid=f3bed0c9f3b10210VgnVCM10000021d0200aRCRD>. Acesso em: jun. 2010.

COMO Funciona. **Oi Paggo – Tudo sobre o Oi Paggo**. Disponível em: <http://www.novaoi.com.br/portal/site/NovaOi/menuitem.e45de4d5df2322fb72871a31f26d02a0/?vgnextoid=e66ed0c9f3b10210VgnVCM10000021d0200aRCRD>. Acesso em: jun. 2010.

SERRANO, F.; CABRAL, R. De olho em que não tem conta nem cartão de crédito. **Estadão**, mar. 2010. Disponível em: <http://www.estadao.com.br/noticias/tecnologia+link,de-olho-em-que-nao-tem-conta-nem-cartao-de-credito,3447,0.shtm>. Acesso em: jun. 2010.

VANTAGENS ao cliente. **NOVO e-pay**. Disponível em: <http://www.novoepay.com.br/vant_cli.htm>. Acesso em: jun. 2010.

SEGURANÇA. **NOVO e-pay**. Disponível em: <http://www.novoepay.com.br/seguranca.htm>. Acesso em: jun. 2010.

COMO Funciona. **NOVO e-pay**. Disponível em: <http://www.novoepay.com.br/como_funciona_port.html>. Acesso em: jun. 2010.

INSTALAÇÂO N-Token no celular. **NOVO e-pay**. Disponível em: <http://www.novoepay.com.br/meu_novo_instal_ntoken.htm>. Acesso em: jun. 2010.

BB Visa Mobile Pay. **Banco do Brasil**. Disponível em: <http://www.bb.com.br/portalbb/page3,114,4006,6,1,1,1.bb?codigoMenu=934&codigoNoticia=11571&codigoRet=8136&bread=6>. Acesso em: jun. 2010.

SOBRE. **Wappa**. Disponível em: <http://www.wappa.com.br/site2010/Sobre.aspx>. Acesso em: jun. 2010.

MIWA, R. Uso de m-payment em táxis. **Mobilepedia**, ago. 2009. Disponível em: <http://www.mobilepedia.com.br/cases/uso-de-m-payment-em-taxis-mobile-marketing>. Acesso em: jun. 2010.

EMPRESA. **M-Ca$h**. Disponível em: <http://mcash.com.br/empresa.htm>. Acesso em: jun. 2010.

BANRISUL ingressa na terceira onda da automação bancária. **Portal do Governo do Estado do Rio Grande do Sul**, dez. 2007. Disponível em: <http://www.estado.rs.gov.br/direciona.php?key=Y2FwYT0xJmludD1ub3RpY2lhJm5vdGlkPTYzODAyJnBhZz01MCZlZGl0b3JpYT0mb3JpZz0x>. Acesso em: jun. 2010.

M-BANKING Banrisul. **Banrisul**. Disponível em: <http://www.banrisul.com.br/bob/link/bobw00hw_produto_detalhe.asp?secao_id=1624&secao_nivel_2=1624&secao_nivel_1=18&secao_principal>. Acesso em: jun. 2010.

FIELDING, R. T. **Architectural Styles and the Design of Network-based Software Architectures**. 2000. 162 f. Dissertação (Doutorado em Ciência da Computação) – University of Irvine, Irvine, Estados Unidos.

WIKIPEDIA. **Representational State Transfer**. Disponível em: <http://en.wikipedia.org/wiki/Representational_State_Transfer>. Acesso em: jun. 2010.

TYAGI, S. RESTful Web Services. **Oracle – Sun Developer Network**, ago. 2006. Disponível em: <http://java.sun.com/developer/technicalArticles/WebServices/restful/>. Acesso em: jun. 2010.