

**FELIPE ANTÔNIO DE GARCIA E MOURA**

**UM MODELO DE SERVIÇO SOB O PARADIGMA  
M-PAYMENT**

**FLORIANÓPOLIS  
2005**

**UNIVERSIDADE FEDERAL DE SANTA CATARINA**

**PROGRAMA DE PÓS-GRADUAÇÃO  
EM ENGENHARIA ELÉTRICA**

**UM MODELO DE SERVIÇO SOB O PARADIGMA  
M-PAYMENT**

Dissertação submetida à  
Universidade Federal de Santa Catarina  
como parte dos requisitos para a  
obtenção do grau de Mestre em Engenharia Elétrica.

**FELIPE ANTÔNIO DE GARCIA E MOURA**

Florianópolis, Fevereiro de 2005.

# UM MODELO DE SERVIÇO SOB O PARADIGMA M-PAYMENT

Felipe Antônio de Garcia e Moura

‘Esta Dissertação foi julgada adequada para obtenção do Título de Mestre em Engenharia Elétrica, Área de Concentração em *Automação e Sistemas*, e aprovada em sua forma final pelo Programa de Pós-Graduação em Engenharia Elétrica da Universidade Federal de Santa Catarina.’

---

Prof. Carlos Barros Montez, Dr.  
Orientador

---

Prof. Alexandre Trofino Neto, Dr  
Coordenador do Programa de Pós-Graduação em Engenharia Elétrica

Banca Examinadora:

---

Prof. Carlos Barros Montez, Dr  
Presidente

---

Prof. Mario Antonio Ribeiro Dantas, PhD

---

Prof. Frank Augusto Siqueira, PhD

---

Prof. Ricardo José Rabelo, Dr

Resumo da Dissertação apresentada à UFSC como parte dos requisitos necessários para a obtenção do grau de Mestre em Engenharia Elétrica.

# **UM MODELO DE SERVIÇO SOB O PARADIGMA M-PAYMENT**

**Felipe Antônio de Garcia e Moura**

Fevereiro / 2005

Orientador: Carlos Barros Montez, Dr. Eng.  
Área de Concentração: Automação e Sistemas  
Palavras-chave: pagamentos móveis, serviços móveis, serviços web  
Número de Páginas: X + 91.

## **RESUMO:**

Este trabalho tem como principal objetivo estudar um novo canal de comércio que é o dos pagamentos móveis, analisando os principais cenários de pagamento e a necessidade de integração dos ambientes de TI com o de telecomunicações móvel.

Esta dissertação descreve as principais tecnologias do ambiente móvel sem fio e também das tecnologias de *middleware*, em particular a tecnologia de serviços web (*web services*), e as utiliza de forma integrada para o desenvolvimento do protótipo.

Um modelo de pagamentos móveis é proposto, baseado nos principais modelos encontrados na literatura. Além disso, é desenvolvido um protótipo de um sistema, fundamentado neste modelo proposto.

Abstract of Dissertation presented to UFSC as a partial fulfillment of the requirements for the degree of Master in Electrical Engineering.

# **A SERVICE MODEL USING M-PAYMENT PARADIGM**

**Felipe Antônio de Garcia e Moura**

February / 2005

Advisor: Carlos Barros Montez, Dr. Eng.

Area of Concentration: Automation and Systems.

Keywords: m-payments, m-commerce, web services

Number of Pages: X + 91.

## **ABSTRACT:**

This dissertation has as its main purpose to study a new commerce channel called mobile payments, analyzing the most important payment scenarios and the integration requirement between IT and mobile telecommunications environments.

This dissertation describes the main technologies in the wireless environment as well as middleware technologies and uses them in an integrated way to develop the prototype.

A mobile payment model is proposed based on the main models found in the literature. Furthermore a system prototype, based on this proposed model, is developed.

# Índice

Lista de Tabelas.....	x
1. Introdução.....	1
1.1 Motivações .....	2
1.2 Objetivos do trabalho .....	3
1.3 Organização do texto.....	4
2. Pagamentos móveis .....	5
2.1 Introdução.....	5
2.2 Definições básicas .....	5
2.3 Principais características, vantagens e desvantagens .....	6
2.4 Consórcios e fóruns de pagamentos móveis.....	8
2.4.1 PayCircle .....	8
2.4.2 Projeto da Aliança da Liberdade ( <i>Liberty Alliance Project</i> ).....	9
2.4.3 Iniciativa MeT ( <i>Mobile Electronic Transaction</i> ).....	9
2.4.4 Iniciativa Radicchio.....	9
2.4.5 Fórum Mobey ( <i>Mobey Forum</i> ).....	10
2.4.6 Fórum de Pagamentos Móveis ( <i>Mobile Payments Forum</i> ).....	10
2.5 Pagamentos digitais: do <i>e-payment</i> ao <i>m-payment</i> .....	10
2.6 Arquiteturas e classificações de pagamentos móveis.....	17
2.7 Modelos apropriados para os pagamentos móveis .....	18
2.7.1 Modelo dominado por bancos .....	18
2.7.2 Modelo dominado por novos provedores de serviços de pagamentos .	20
2.7.3 O papel das operadoras de telecomunicações .....	21
2.7.4 Modelo dominado pelos Intermediários / Novos Entrantes ( <i>Start-ups</i> )	22
2.8 Considerações sobre o estado atual de <i>m-payments</i> .....	22
2.8.1 Questões a serem resolvidas.....	22
2.8.2 Segurança em pagamentos móveis.....	24
2.9 Modelos propostos em outros trabalhos.....	26
2.10 Considerações finais.....	27
3. Tecnologias Móveis e Web Services.....	28
3.1 Introdução.....	28
3.2 Tecnologias de redes de telefonia móvel.....	28

3.2.1 GSM .....	29
3.2.2 HSCSD .....	30
3.2.3 GPRS .....	30
3.2.4 EDGE .....	31
3.2.5 3G .....	31
3.3 Serviços de comunicação móvel .....	31
3.3.1 SMS ( <i>Short Messaging Service</i> ).....	31
3.3.2 WAP ( <i>Wireless Application Protocol</i> ).....	32
3.3.3 I-Mode .....	32
3.3.4 USSD ( <i>Unstructured Supplementary Services Data</i> ).....	33
3.3.5 <i>Cell Broadcast</i> .....	33
3.3.6 Toolkit de aplicação SIM ( <i>Subscriber Identity Module</i> ).....	33
3.3.7 MExE ( <i>Mobile Station Application Execution Environment</i> ).....	34
3.4 Protocolos de segurança em pagamentos móveis.....	34
3.5 Plataforma Móvel de Programação (J2ME).....	36
3.6 Os serviços web ( <i>web services</i> ).....	37
3.6.1 Principais características .....	38
3.6.2 Aspectos técnicos de serviços web.....	40
3.6.3 Casos de sucesso utilizando a tecnologia de serviços web.....	43
3.7 Considerações finais.....	43
4. Modelo proposto de <i>m-payment</i> .....	45
4.1 Introdução.....	45
4.2 Motivações para o modelo.....	46
4.3 Os atores e suas interações .....	46
4.4 Uma descrição do Sistema e seus pontos de integração.....	47
4.5 Os processos de compra de créditos.....	48
4.5.1 Pagamento efetuado somente pelo cliente.....	49
4.5.2 Pagamento efetuado com a ajuda de um comerciante.....	53
4.6 Outros trabalhos relacionados.....	55
4.6.1 A proposta de Mckitterick [53] .....	55
4.6.2 O estudo de Marques [55] .....	56
4.6.3 O estudo de Martins, Rocha e Henriques [56] .....	56

4.6.4 O trabalho de Pousttchi [60].....	56
4.7 Considerações finais.....	57
5. Implementação e avaliação do modelo.....	58
5.1 Descrição geral da implementação.....	58
5.1.1 Servidor 1 .....	59
5.1.2 Servidor 2 .....	60
5.1.3 Telefone Móvel .....	60
5.2 Servidor de Pagamentos .....	61
5.3 <i>Front End</i> de serviços web.....	62
5.4 Fluxo de mensagens entre os atores .....	63
5.5 Considerações sobre a implementação.....	68
5.6 Considerações finais.....	69
6. Conclusões.....	70
6.1 Revisão das motivações e objetivos .....	70
6.2 Visão geral do trabalho.....	71
6.3 Contribuição e escopo do trabalho .....	71
6.4 Perspectivas futuras .....	74
Referências bibliográficas .....	76
Apêndice I: Análise crítica de serviços web e CORBA.....	81
I.1 Introdução .....	81
I.2 CORBA versus serviços web.....	82
I.3 Modelos de computação distribuída em CORBA e serviços web .....	84
Modelo de Dados: .....	84
Semânticas de Requisição: .....	85
Escalabilidade e Confiança .....	85
Serialização .....	86
Controle estático e de tempo de execução.....	86
I.4 Suporte a características no CORBA e serviços web .....	87
Transparência de localização.....	87
Registro .....	88
Descoberta de serviço.....	88
Firewall.....	89

Segurança .....	89
Persistência.....	90
Facilidade de implantação e construção .....	90
Independência de plataforma.....	91
Capacidade de processamento ( <i>footprint</i> ) .....	91

# Lista de Figuras

Figura 1. As três fases básicas de uma transação comercial simples.....	6
Figura 2. Um cenário básico de pagamento digital. ....	10
Figura 3. Um modelo de pagamento direto em moeda. ....	11
Figura 4. Uma transação de pagamento baseado no Modelo SET. ....	12
Figura 5. Estrutura básica de pagamentos móveis [12]. ....	13
Figura 6. Sessão de pagamento básica [12]. ....	14
Figura 7. Principais fases de um pagamento móvel [7]. ....	15
Figura 8. Modelo dominado pelos bancos [12]. ....	19
Figura 9. Pilha de Protocolos da tecnologia de serviços web. ....	41
Figura 10. Modelo Proposto de pagamento móvel de Créditos Pré-Pagos. ....	47
Figura 11. Cenário de pagamento móvel efetuado pelo próprio cliente. ....	51
Figura 12. Cenário de pagamento móvel efetuado através de um comerciante. ....	54
Figura 13. Componentes da implementação do protótipo. ....	59
Figura 14. Servidor de Pagamentos baseado na especificação da PayCircle [17]. ....	61
Figura 15. Ponte de Serviços Web baseado na especificação da PayCircle [17] .....	63

# Lista de Tabelas

Tabela 1. As diversas dimensões de pagamentos [13].....	17
Tabela 2. Comparação entre CORBA e serviços web [68]. .....	83
Tabela 3. Pilha de tecnologias em CORBA e em serviços web [68].....	84

# 1. Introdução

O processo de compra e venda evoluiu da simples troca de papel moeda e de cheques escritos para a transferência de dados de cartões de pagamento de forma pessoal, pelo telefone e através da Internet. Esta evolução envolveu a substituição da transferência física de moeda para uma troca de informações entre as partes.

O desenvolvimento do comércio eletrônico automatizou o processo de pagamento, onde os detalhes do pagamento são transmitidos através de redes abertas, e o contato físico entre o comprador e o vendedor não é mais necessário. Esta evolução dos pagamentos físicos para os virtuais trouxe grandes benefícios a compradores e comerciantes [2][76].

O contínuo e acelerado desenvolvimento do comércio eletrônico, a rápida disseminação e utilização da infra-estrutura de telefonia móvel e a gradual integração entre esses dois ambientes está dando origem a um novo canal para transações comerciais, chamado de *m-commerce* (ou comércio eletrônico móvel) [33].

As tecnologias móveis 2.5G e 3G estão sendo adotadas como uma plataforma para efetuar serviços de comunicações, negócios e lazer e têm se tornado um mercado atrativo para provedores de serviços, provedores de conteúdo e para provedores de soluções de comércio eletrônico. Para uma maior aceitação dessas novas propostas, qualidade e desempenho desses serviços devem ser garantidos através de serviços móveis (*m-services*) básicos de suporte.

Um dos mais importantes serviços de suporte para comércio móvel é o serviço de pagamentos móveis (*m-payments*), sendo que o crescimento do *m-commerce* depende profundamente de soluções efetivas para esse serviço. Atualmente, essas soluções são oferecidas por operadoras de telecomunicações móveis, instituições financeiras e provedores independentes e muitas diferenças existem entre as diversas soluções proprietárias oferecidas. Embora existam algumas organizações que foram criadas para propor um mecanismo comum para o desenvolvimento de serviços de pagamentos móveis, atualmente ainda não existe nenhum padrão comum adotado por esses provedores de pagamentos móveis.

Esta dissertação é um estudo das diversas arquiteturas e tecnologias disponíveis que podem ser empregadas nesse cenário de serviços de pagamentos móveis. Esta investigação detalhada, bem como uma análise da realidade brasileira, fizeram-se necessárias para uma posterior formulação de um modelo de pagamentos que possa ser introduzido no mercado local sem grandes resistências por parte dos usuários, e que também seja baseado na compra de um produto já em alta demanda. O modelo proposto nessa dissertação baseou-se na recarga de créditos de telefones móveis pré-pagos, hoje executada por outros meios menos eficientes. Trata-se de uma proposta para um caso específico de pagamento móvel, trazendo uma solução preliminar a uma solução de pagamento mais genérico. Nesse modelo, portanto, procura-se empregar as tecnologias mais disseminadas para facilitar a utilização por parte dos usuários.

A tecnologia de serviços web (*web services*) foi escolhida para ser utilizada na implementação deste modelo devido a sua arquitetura distribuída e sua facilidade de integração, através dos protocolos de Internet existentes, com as infra-estruturas de pagamentos móveis. A implementação também demonstra a integração desta plataforma de serviços web com um sistema de rede móvel.

## **1.1 Motivações**

Através da utilização de novas tecnologias, especialmente tecnologias sem fio, surgem novas possibilidades de se efetuar uma transação de pagamentos. Com isso, pesquisas para desenvolvimento de novas arquiteturas para serviços de pagamentos móveis vêm sendo desenvolvidas, principalmente nos últimos cinco anos.

Alguns poucos trabalhos relacionados foram encontrados na literatura. McKitterick [53] propõe um modelo genérico de pagamentos móveis utilizando a tecnologia de serviços web e oferecendo três métodos diferentes de pagamento. O trabalho de Marques [55] faz um estudo detalhado do *status* atual dos pagamentos móveis na Europa [81], e principalmente em Portugal e descreve as principais vulnerabilidades dos sistemas utilizados atualmente. Já o trabalho de Martins, Rocha e Henriques [56] faz uma análise do ponto de vista de segurança e descreve alguns protocolos novos que estão atualmente sendo padronizados. O trabalho de Pousttchi testou com um cliente, utilizando a tecnologia de serviços web, a plataforma de

pagamento proposta pela PayCircle [17] e sugere que esta proposta de padronização é apropriada.

O objetivo maior de todos esses trabalhos é o de melhorar os sistemas de pagamentos existentes para que o processo seja mais padronizado, eficiente e seguro. Além disso, existe a possibilidade de oferecimento de novos serviços, os quais passariam a se viabilizar com a introdução de mobilidade e transações à distância.

A adoção de arquiteturas de pagamentos móveis representa uma evolução lógica no ambiente de transação de valor monetário [67]. De fato, no início, pagamentos eram feitos na maioria das vezes face a face (moeda, cheques, cartões). Com a evolução da tecnologia e com o desenvolvimento de redes de telecomunicações para transmissão de dados (cartões de crédito, *e-payments*), as transações remotas ganharam popularidade. A tendência atual é a de implementar sistemas sem fio que permitam transações tanto remotas como face a face através de um único dispositivo.

Atualmente, entretanto, esta nova abordagem de pagamento enfrenta questões tecnológicas e de negócios que retardam o seu desenvolvimento. Um grande desafio, o qual provedores de pagamentos móveis enfrentam neste momento, é o de convencer compradores e comerciantes que eles precisam de novos sistemas de pagamentos [5]. Esse objetivo só deverá ser cumprido com o desenvolvimento de arquiteturas e modelos de pagamentos móveis que sejam adequados para o modelo de negócios existentes. Ou seja, o desafio final é o de conciliar, tecnologias de redes sem fio, tecnologias de sistemas distribuídos (principalmente de *middlewares*), com arquiteturas de pagamentos móveis adequadas para o modelo de negócios abordado.

## **1.2 Objetivos do trabalho**

Este trabalho tem por motivação o estudo de pagamentos móveis e das principais tecnologias que possibilitam o seu desenvolvimento. Além do levantamento do estado da arte e das principais tecnologias habilitadoras, neste trabalho tem como objetivo principal a proposta de um modelo de pagamento móvel para o caso específico de recarga de telefones móveis pré-pagos. Um protótipo foi desenvolvido, com objetivo de avaliar a viabilidade de um sistema baseado no modelo proposto. Como objetivo subjacente, são também avaliadas ferramentas de desenvolvimento do sistema, tal como os serviços web e as tecnologias J2EE e J2ME [30].

Apesar de serem considerados importantes nesses tipos de sistemas, este trabalho não tem como objetivo estudar aspectos de segurança ou de tolerância a falhas do sistema. O seu foco é o de entender o cenário atual de abordagens e de tecnologias e aplicá-las ao ambiente brasileiro, buscando uma solução inovadora, porém de introdução mais fácil à realidade local.

### **1.3 Organização do texto**

Este trabalho é dividido em 6 partes. O Capítulo 2 faz uma introdução aos pagamentos móveis, discutindo os princípios básicos dentro de um sistema de pagamentos móveis. Descreve os atores e como estes estão relacionados e faz a análise das vantagens e desvantagens dos pagamentos móveis e suas diferenças quando comparado a métodos convencionais e eletrônicos. Também ilustra um caso genérico de pagamento móvel mostrando as etapas principais de todo o processo. Além disso, o Capítulo 2 apresenta as principais entidades que buscam por padronizações no setor, mostra os principais modelos a partir dos quais os serviços de pagamentos móveis podem ser formatados, enumera as várias questões que ainda necessitam ser resolvidas e faz uma comparação entre as diversas dimensões em que os pagamentos podem estar inseridos.

O Capítulo 3 descreve tecnologias móveis, tanto de rede, como de serviços de mais alto nível envolvendo tecnologias sem fio e de segurança. Além disso, esse capítulo faz uma descrição dos serviços web e quais as vantagens de se utilizar seus protocolos. Nesse capítulo também são descritas algumas empresas que oferecem atualmente serviços de pagamentos móveis no mercado utilizando-se destas tecnologias.

O Capítulo 4 propõe um modelo de pagamento móvel que possibilita a recarga de uma conta de celular pré-pago. Mostra quais os pontos de integração que seriam necessários para implementar esse modelo na atual estrutura das operadoras de telefonia móvel, além de detalhes de todos os passos do processo de compra desses créditos de conversação. Este capítulo também faz uma análise crítica sobre alguns trabalhos anteriores relacionados a pagamentos móveis.

Por fim, o Capítulo 5 descreve uma implementação simplificada do modelo proposto no Capítulo 4 e detalha as tecnologias utilizadas na implementação e as mensagens trocadas entre as entidades envolvidas. O Capítulo 6 apresenta as conclusões desta dissertação.

## 2. Pagamentos móveis

### 2.1 Introdução

Com a crescente prevalência do comércio eletrônico (*e-commerce*) e o uso já bastante comum de telefones móveis, um novo tipo de canal está emergindo, chamado de comércio eletrônico móvel, ou *m-commerce* [33].

O uso do *e-commerce* tornou digital e virtual o processo de pagamento, deixando de ser necessário qualquer contato físico entre comprador e vendedor. Esta conversão dos pagamentos físicos para os virtuais já trouxe grandes benefícios para compradores e vendedores [2]. Contudo, o comércio móvel irá exigir novas demandas, tais como, pagamentos com acesso sem fio, em tempo real, em qualquer local e a qualquer hora, para a compra de serviços e de mercadorias físicas ou digitais. A consequência imediata é uma competição entre provedores de serviços de pagamentos – como os bancos, empresas de cartão, operadoras de telefonia móvel e novas entrantes – para ser a primeira instituição a oferecer um modelo de sucesso para pagamentos virtuais móveis.

Diferentes modelos de pagamentos móveis (*m-payments*) têm surgido devido à necessidade de padronização requerida por parte das diversas instituições envolvidas. Essas instituições vêm se organizando na forma de consórcios, os quais vêm gerando novas definições e utilizações para essa tecnologia emergente.

Este Capítulo tem por objetivo definir e apresentar os principais modelos de pagamentos móveis. Na próxima seção são apresentadas algumas definições básicas, necessárias para um melhor entendimento desse cenário.

### 2.2 Definições básicas

Define-se pagamento como uma transação de valor monetário entre uma parte e outra (usualmente entre entidades “comprador” e “comerciante”). Isso pode ser feito através de uma ou várias entidades “intermediárias”, como um banco ou uma empresa de cartão [32].

Uma transação de comércio simples (sem intermediários) entre duas partes consiste de três fases básicas (Figura 1) [32]. Primeiro o comprador escolhe o produto

ou serviço que quer comprar. Depois, quando o comprador tiver terminado a escolha, o comerciante oferece uma fatura ao cliente. Finalmente o comprador tem que pagar o comerciante pela mercadoria.

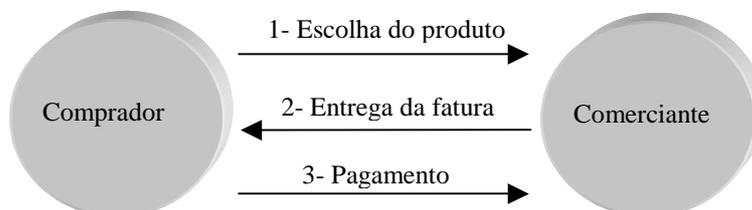


Figura 1. As três fases básicas de uma transação comercial simples.

Existe uma série de possibilidades para se estender o número de fases durante a transação de pagamento. Entretanto, um sistema de pagamento deve ser muito simples. Além disso, a transação tem que ser transparente ao máximo para o comprador, mesmo que o sistema por trás da transação seja complexo. Com um sistema complexo de transação, o comprador será desencorajado a utilizá-lo.

Tradicionalmente, os métodos mais comuns de pagamentos são através de dinheiro, cheques, cartões de débito e cartões de crédito. Com as possibilidades criadas pela Internet, uma nova geração de pagamentos surgiu: pagamentos eletrônicos ou virtuais (*e-payments*). Agora, com a crescente penetração da telefonia móvel e com o desenvolvimento do *m-commerce*, o pagamento móvel (*m-payment*) deverá se tornar um importante modo para pagar por mercadorias adquiridas.

Pagamentos móveis – definidos como pagamentos executados através de dispositivos móveis sem fio – serão provavelmente uma importante parte do setor de pagamentos no setor varejista [3]. Um estudo [4] prevê que pagamentos móveis irão representar 26 bilhões de Euros em 2005 só na Europa (87 Euros por telefone móvel por ano) o que significa apenas 0.5% dos gastos de compradores, excluindo a compra de casas e veículos.

### **2.3 Principais características, vantagens e desvantagens**

Existem diversas razões do porquê dos telefones móveis terem o potencial de se tornarem em dispositivos de pagamento em um futuro próximo. O número de usuários deste tipo de aparelho já é muito grande e pagamentos móveis podem ser realizados

através deles em todos os tipos de transações de pagamentos, tanto através de pessoas (qualquer comerciante), como de pontos de vendas automatizados (máquinas de vendas, estacionamentos, etc) e comércio eletrônico [14].

Os benefícios de utilizar dispositivos sem fio para pagamentos estão diretamente ligados à conveniência de utilizá-los através de um sistema de pagamento de fácil utilização, em tempo real, sem a necessidade de moeda, e o de se poder utilizá-los em qualquer lugar e a qualquer hora [16].

Esse cenário pode ser descrito como um comércio universal em um ambiente, em que compradores e vendedores serão literalmente capazes de conduzir comércio a qualquer hora, em qualquer lugar e da forma que desejarem [34].

Pagamentos móveis, entretanto, trazem também vários problemas a serem resolvidos. Um dos pontos mais cruciais é o preço que uma transação irá ter. Cada vez mais, compradores estão relutantes em pagar mais sem ter um serviço de valor agregado ao que eles já têm. Argumentos como conveniência e flexibilidade podem não ser suficientes para convencê-los. Além disso, consumidores já consideram caros alguns serviços de valor agregado (mensagem instantânea, por exemplo) oferecidos pelas operadoras de telefonia, e não estão dispostos a pagar além das altas taxas cobradas pelas operadoras e bancos [15].

O atual início lento do *m-commerce* pode ser atribuído ao fato que este compartilha dos mesmos problemas enfrentados pelo *e-commerce*, acrescido de alguns outros devido a peculiaridades desta tecnologia [6]. Pode-se citar, por exemplo, limitações dos aparelhos e da rede de transmissão, maturidade das soluções de pagamentos, e a falta de interesse de compradores [7]. Os fabricantes de dispositivos têm o desafio de desenvolverem equipamentos fáceis de utilizar, rápidos e confiáveis em um cenário de pagamentos. Sem um equipamento apropriado, o consumidor não será incentivado a utilizar esses novos métodos. Complementarmente, com esse objetivo, os provedores de serviços têm que achar o melhor modelo para que possam convencer usuários de telefones móveis e comerciantes a utilizar seus novos serviços de pagamentos [5].

Esta dissertação trata exatamente dessas questões: proposição de um modelo adequado para *m-payments* (para o caso particular de recarga de telefones móveis), e

estudo de linguagens de programação, *middlewares* e ferramentas adequadas para o desenvolvimento desses sistemas de pagamentos móveis.

No entanto, apesar dessas dificuldades, o potencial do *m-commerce* (e conseqüentemente, do *m-payment*) continua muito grande e isso foi decisivo para que indústrias de finanças e de telefonia móvel acelerassem o desenvolvimento, aceitação e uso do comércio móvel. A seguir são apresentadas algumas iniciativas nesse sentido.

## **2.4 Consórcios e fóruns de pagamentos móveis**

Visando o aumento da adoção de pagamentos móveis no mundo, instituições financeiras, empresas de telecomunicações e novos entrantes no mercado formaram consórcios. Os seus objetivos são o de endereçar a segurança e questões de compatibilidade através da adoção de padrões para pagamentos móveis. Uma vez que estes consórcios têm diferentes focos e algumas empresas participam ativamente de vários deles ao mesmo tempo, esses grupos não competem entre si e buscam chegar a uma convergência para a definição dos parâmetros.

### **2.4.1 PayCircle**

PayCircle é uma organização sem fins lucrativos, fundada em 2002, formada por empresas de tecnologia de telecomunicações. A PayCircle tem como foco acelerar o uso da tecnologia de pagamentos e desenvolver ou adotar bibliotecas abertas (APIs) de pagamento baseadas em XML, SOAP, Java e outras linguagens da Internet [17]. A Paycircle trabalha para que suas propostas sejam capazes de fazer interface com múltiplos dispositivos, empresas de telecomunicações e sistemas de processamento de transações [18].

Alguns dos membros da organização são Hewlett Packard, Oracle, Siemens, Sun Microsystems, Amdoc, Universidade de Augsburg e diversos outros membros e participantes. Essas instituições entendem que podem ganhar mais através da contribuição para um padrão aberto do que competindo por uma solução proprietária, permitindo um desenvolvimento mais veloz do setor.

### **2.4.2 Projeto da Aliança da Liberdade (*Liberty Alliance Project*)**

Esta Aliança foi formada em 2001 com a finalidade de desenvolver padrões abertos para o gerenciamento de identidade em redes federadas e serviços baseados em identificação. Os seus objetivos são os de garantir a interoperabilidade, o suporte a privacidade e o de promover a adoção das suas especificações, diretrizes e melhores práticas [19].

A Aliança é composta de mais de 160 membros, representando uma abrangente gama de organizações mundiais e de diversos setores (educacional, governamentais, provedores de serviços, instituições financeiras, fabricantes, provedores sem fio).

Alguns exemplos de empresas participantes são American Express, AOL, Ericsson, France Telecom, GM, HP, Nokia, Novell, NTT Do Co Mo, Sony, Sun Microsystems, Verisign, Vodafone e muitas outras.

### **2.4.3 Iniciativa MeT (*Mobile Electronic Transaction*)**

A iniciativa MeT é o maior consórcio [18] formado. Esse grupo foi criado em 2000 pela Ericsson, Motorola, Nokia, NEC, Panasonic e Siemens. O objetivo dessa iniciativa é o de criar um sistema de referência para garantir transações móveis seguras através de qualquer dispositivo ou tipo de pagamento. Esse consórcio tem como importante característica o fato de não ter bancos envolvidos.

### **2.4.4 Iniciativa Radicchio**

Fundada em 1999, a iniciativa Radicchio procura desencadear o enorme potencial dos serviços de dados sem fio, como o *e-commerce* móvel e o *e-government* móvel. Gerenciada por uma série de empresas como a EDS, Ericsson, British Telecom, Schlumberger, Vodafone, Sonera, Telefonica, VeriSign e outras, Radicchio é uma autoridade e um representante da indústria para redes confiáveis (*trusted networks*) no ambiente móvel. A Radicchio é uma parceira do Projeto da Aliança da Liberdade. O foco da Radicchio é o “*Trusted Transaction Roaming – t2r*”, que permite operadoras de telecomunicações móveis, instituições financeiras, governos e outros provedores de serviços identificar fortemente o usuário final através do seu dispositivo móvel, e portanto reduzindo o risco e custo dos serviços de comércio eletrônico.

### 2.4.5 Fórum Mobey (*Mobey Forum*)

O Fórum Mobey foi estabelecido em 2000 pelos bancos líderes mundiais. O objetivo é promover os serviços financeiros usando tecnologias móveis. Este consórcio está comprometido em acelerar a utilização de serviços financeiros móveis de tal forma a torná-los mais amigáveis aos usuários através da promoção de padrões de tecnologia abertos e não proprietários [20].

### 2.4.6 Fórum de Pagamentos Móveis (*Mobile Payments Forum*)

Este fórum foi criado por emissores de cartão de crédito em 2001. O seu objetivo é garantir que os atuais sistemas de autenticação, processamento e de cobrança possam trabalhar em conjunto com qualquer sistema e qualquer padrão de pagamento móvel que venham a emergir [18].

## 2.5 Pagamentos digitais: do *e-payment* ao *m-payment*

Para um completo entendimento da forma como as transações de pagamento digital funcionam, essa seção apresenta os principais conceitos envolvidos. A Figura 2 ilustra um cenário de uso desse tipo de pagamento [8].

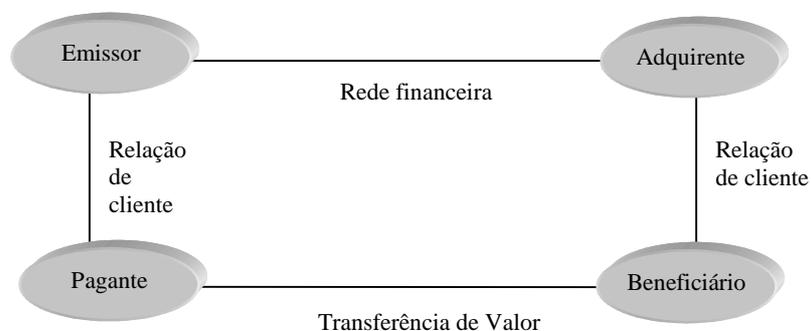


Figura 2. Um cenário básico de pagamento digital.

O pagante (comprador) faz o pagamento em troca de uma mercadoria ou serviço. O beneficiário (comerciante) é a entidade que recebe o pagamento, normalmente citado como comerciante ou vendedor. O emissor é a outra entidade (banco ou provedor de serviços) interagindo com o pagante. O adquirente representa uma outra entidade (banco ou provedor de serviços) do beneficiário. Os sistemas de pagamento digitais podem ser classificados de acordo com a necessidade de fluxo de informação entre os participantes

da transação eletrônica [9]. Alguns exemplos de modelos sugeridos [10] serão descritos a seguir.

O exemplo da Figura 3 ilustra o pagamento direto em moeda. O comprador (pagante) saca o dinheiro do banco (emissor), repassa esse dinheiro para o comerciante (beneficiário) e este deposita o dinheiro no seu banco (adquirente).

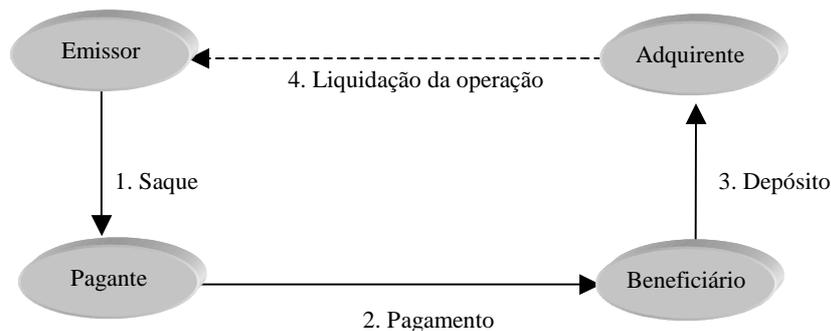


Figura 3. Um modelo de pagamento direto em moeda.

Esse sistema representado pela Figura 3 também pode funcionar com dinheiro simbólico (*token*) como é o caso de *smart cards*. Neste caso, será necessária a última fase de liquidação (*settlement*) da operação entre o emissor e adquirente que transforma esse dinheiro simbólico em dinheiro real.

Para demonstrar a flexibilidade desta representação, a Figura 4 apresenta uma descrição do sistema SET (*Secure Electronic Transaction*) [35] desenvolvido pelas empresas de cartão de crédito para facilitar as transações de pagamentos seguros de cartão através da Internet.

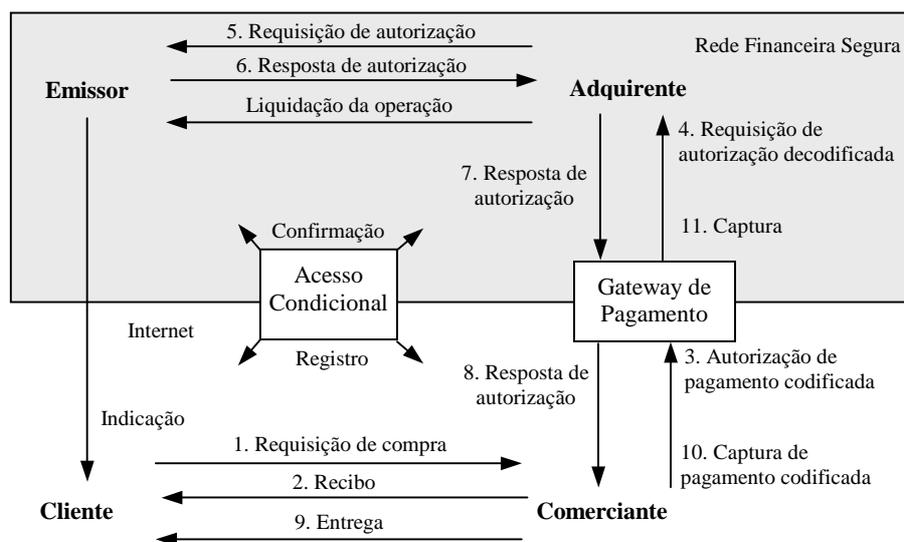


Figura 4. Uma transação de pagamento baseado no Modelo SET.

Com esse exemplo, demonstra-se notar que essa representação com Cliente, Comerciante, Adquirinte e Emissor pode ser utilizada para representar os cenários de pagamentos eletrônicos (maiores detalhes referentes à tecnologia de segurança no qual, o Modelo SET é baseado, podem ser encontrados no Capítulo 3 e detalhes sobre o seu funcionamento podem ser encontrados em [35]).

Atualmente, existem algumas poucas soluções de pagamentos eletrônicos consideradas de sucesso. Estas soluções seguem modelos com três partes envolvidas (a *American Express* processa pagamentos de cartão dentro de uma única organização) ou quatro partes envolvidas (*Visa* e *Mastercard* têm um número de bancos parceiros, que emitem os cartões, autorizam e recuperam os pagamentos para os comerciantes) [11], as quais permitem o entendimento entre comprador, comerciante e o provedor de solução de pagamento. No caso da *American Express*, onde uma única entidade faz o papel do Adquirinte e do Emissor ao mesmo tempo, sendo, portanto compartilhada pelo pagante e pelo beneficiário, essa entidade é intitulada de agente (*broker*) [8].

Baseado no modelo de pagamentos eletrônicos convencionais descritos anteriormente, os pagamentos móveis também podem ser modelados de forma análoga. Embora existam diferenças entre os vários sistemas de pagamentos móveis propostos [75], a maior parte deles é estruturada de uma forma semelhante [12]. Como pode ser visto na Figura 5, na maioria dos casos um usuário que quer efetuar um *m-payment* precisa de um intermediário no pagamento (operadora de telefonia móvel, banco, etc),

que atua como *broker*, exercendo o papel do adquirente e do beneficiário ao mesmo tempo.

O comprador contata o intermediário, o comerciante solicita ao intermediário para contatar o comprador, ou o comerciante envia o comprador para o servidor do intermediário. Uma vez que a conexão entre o comprador e o intermediário é efetuada por alguma tecnologia sem fio (SMS, WAP, etc), o comprador autoriza o pagamento (usualmente um código pessoal PIN). Depois disso o comprador e o comerciante recebem uma confirmação de pagamento.

Os comerciantes usualmente recebem os recursos provenientes da venda em suas contas no banco. Para o comprador, existem diversas maneiras de se efetuar a transferência dos recursos para o pagamento, como ilustrado na figura 5 [12]. O intermediário pode debitar a conta bancária do comprador, a conta de cartão de crédito, sua conta pré-paga, ou o intermediário agrega esse pagamento a outros pagamentos e contas e envia uma única conta para o comprador mensalmente.

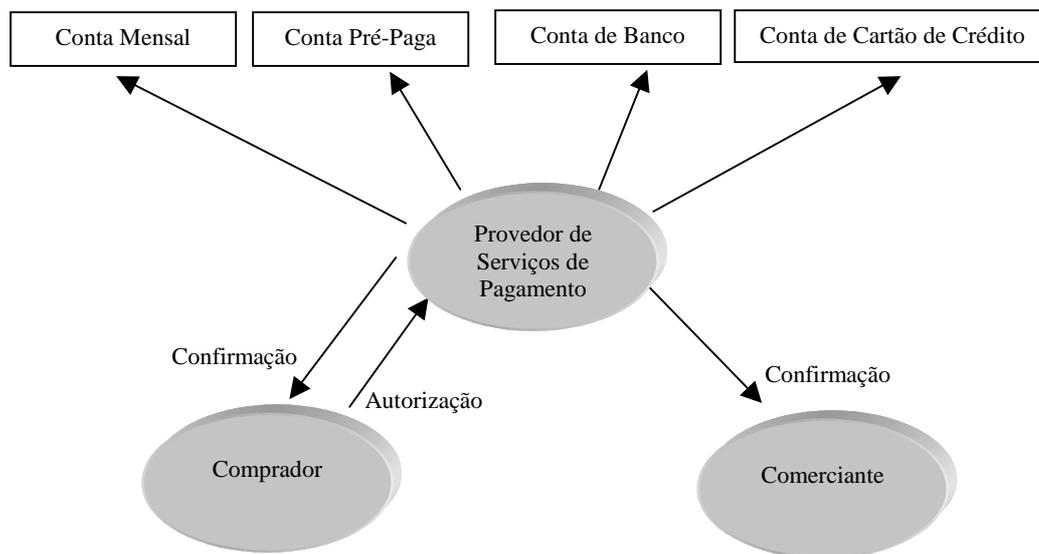


Figura 5. Estrutura básica de pagamentos móveis [12].

Um pagamento móvel deve seguir uma sessão de eventos como ilustrado no diagrama da Figura 6.

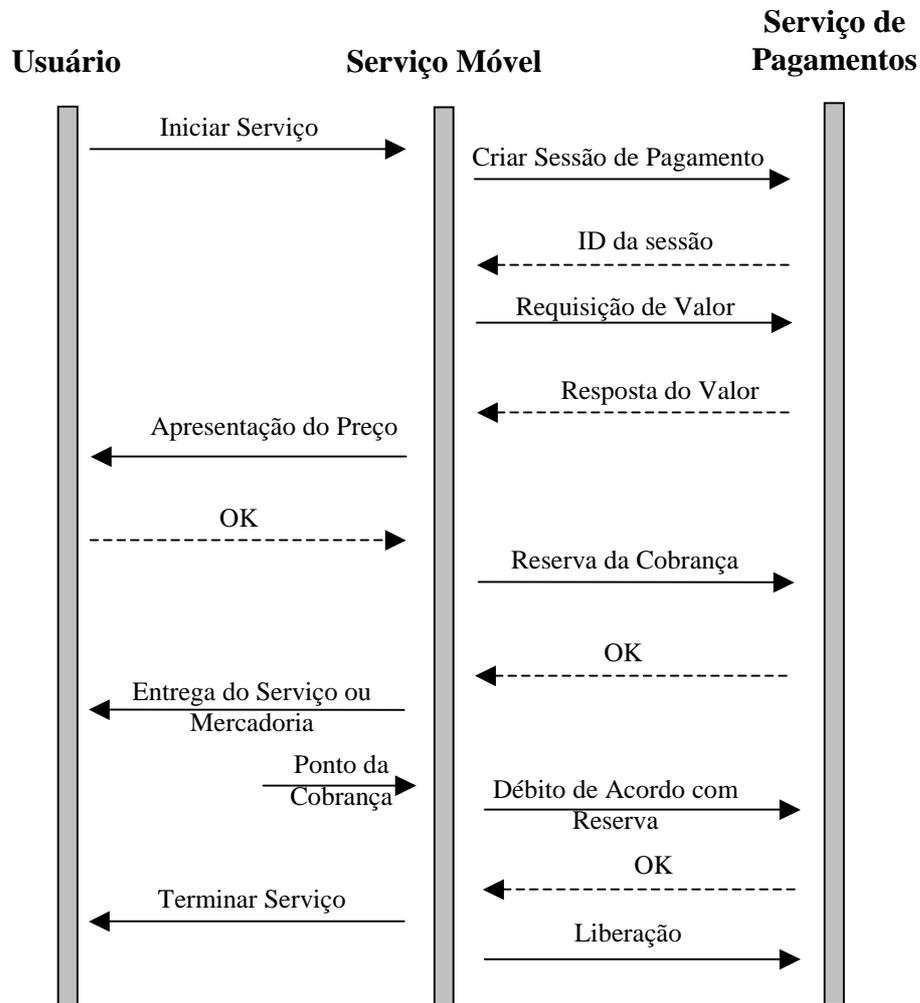


Figura 6. Sessão de pagamento básica [12].

Os principais eventos envolvidos nessa sessão são [12]:

- Criar Sessão de Cobrança: O serviço móvel estabelece uma Sessão de Cobrança. Todas as mensagens pertencentes a essa Sessão de Cobrança são processadas no mesmo contexto; este contexto contém a identidade do usuário final.
- Requisição de Valor / Apresentação do Preço: O serviço móvel procura pelo valor que o Servidor de Pagamentos irá atribuir a futura requisição de pagamentos. O preço resultante é apresentado ao usuário final para informação e aceitação.

- Reserva de Cobrança: Baseado na aceitação do preço pelo usuário final, uma quantidade acordada é reservada, e, portanto débitos podem ser efetuados durante a Sessão de Cobrança.
- Entrega do Serviço ou Produto: Depois do Serviço de Pagamentos ter confirmado o pedido de reserva, o serviço móvel entrega o serviço ou produto.
- Término do Serviço / Liberação: Em qualquer momento, o usuário final ou o serviço móvel pode decidir interromper a entrega do serviço ou produto. Como resultado, o serviço móvel irá enviar uma reserva. Então, qualquer reserva será devolvida ao usuário final, tornando-as disponíveis para futuros pagamentos.

Um exemplo de um caso real de pagamento móvel pode ser visto na Figura 7. Neste caso é ilustrado um cenário específico da aquisição de conteúdo (como, por exemplo, toques de celular, músicas mp3, jogos, etc) de um provedor de conteúdo através de um dispositivo móvel.

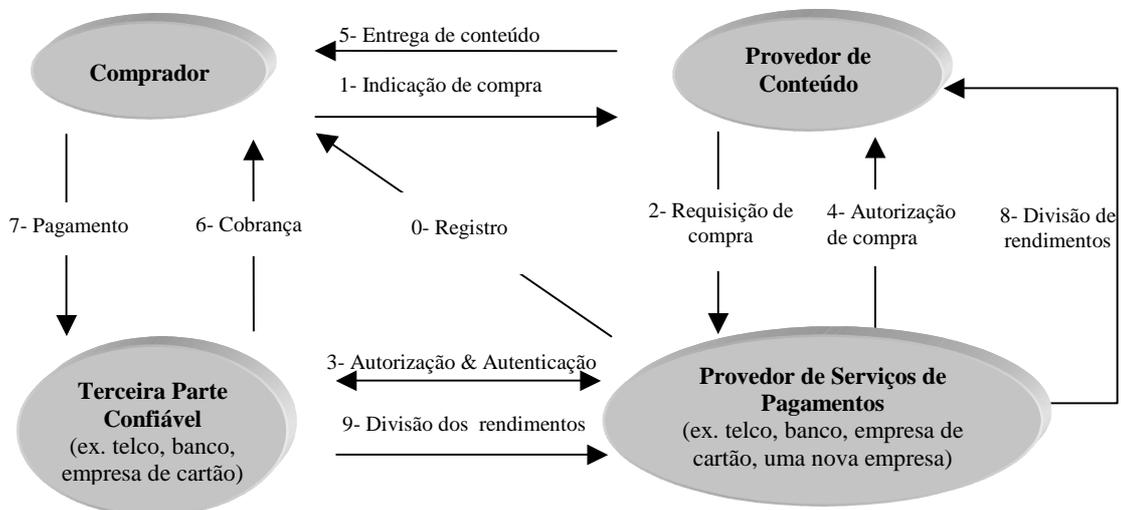


Figura 7. Principais fases de um pagamento móvel [7].

Como pode ser visto na Figura 7, existem quatro partes na transação onde o provedor de conteúdo representa o beneficiário (comerciante), o provedor de serviços de pagamentos é o adquirente e a terceira parte confiável é o emissor.

As principais etapas deste pagamento móvel estão descritas abaixo.

1. O comprador indica o seu interesse em comprar algum conteúdo. Essa indicação pode ser feita através do acionamento de um botão no telefone móvel do comprador ou através do envio de uma mensagem SMS para um número pré-determinado.
2. O provedor de conteúdo envia a requisição de compra para o Provedor de Serviços de Pagamentos.
3. O Provedor de Serviços de Pagamentos pede autorização e autenticação para a Terceira Parte Confiável.
4. O Provedor de Serviços de Pagamentos informa o sucesso do pedido de pagamento.
5. O Provedor de Conteúdo entrega o conteúdo comprado.

A Liquidação do Pagamento, ou seja, a troca de valores monetários entre as partes, pode ser feita em tempo real durante a compra ou pode ser feita de forma posterior a ela.

A Liquidação em tempo real é executada durante a etapa 4 pela Terceira Parte Confiável. Ela pode ser feita através de uma conta pré-paga se a Terceira Parte Confiável for uma empresa de telefonia móvel ou diretamente na conta corrente se for um banco.

No modo pós-pago, o Provedor de Serviços de Pagamentos envia a informação de cobrança para a Terceira Parte Confiável. Esta envia a conta para o comprador, recebe o valor do pagamento e envia para o Provedor de Serviços de Pagamento e este, então, calcula os valores a serem enviados para cada entidade e distribui os recursos apropriadamente.

Esta seção mostrou que não existem grandes diferenças no processo de um pagamento eletrônico convencional para um pagamento eletrônico móvel. Contudo, os papéis das quatro entidades básicas (Pagante, Beneficiário, Adquirente e Emissor) em todo o processo podem ser exercidos por entidades diferentes, incluindo operadoras de telecomunicações móveis (às vezes com funções mais complexas do que a simples transmissão de informações) e provedores independentes, dependendo do cenário em que o pagamento móvel está inserido. Isso será descrito em mais detalhes nas seções seguintes.

## 2.6 Arquiteturas e classificações de pagamentos móveis

Para que as chances de sucesso de uma solução de pagamento móvel sejam maiores, ela deve englobar o maior número de dimensões possíveis como apresentado na Tabela 1 [13]. Em geral, compradores são mais atraídos por soluções mais flexíveis do que as que não oferecem tantas possibilidades. Essas novas soluções de pagamentos devem apresentar uma real melhoria para compradores e vendedores para que possam ser convencidos a mudar dos processos convencionais e já disseminados. Além disso, a solução de pagamento deve sempre estar disponível uma vez que compradores querem pagar a qualquer hora e em qualquer lugar.

Tabela 1. As diversas dimensões de pagamentos [13].

Pelos meios de pagamento	Moeda (dinheiro), cheques, cartões (crédito, débito, <i>smart card</i> ), eletrônico ( <i>e/m-commerce</i> , dinheiro virtual, carteira eletrônica)
Pelo valor	Micro-pagamentos (abaixo de 10 Euros), Macro-pagamentos
Pelo local da compra	Face a face [74] ou Remoto (Internet, Compras pelo correio ou por telefone)
Pelas relações de origens do Comprador/Vendedor	B2B (raro para <i>m-payments</i> ), B2C ou P2P ( <i>Peer to Peer</i> )
Pelo tipo de compra	Mercadorias físicas, mercadorias digitais/eletrônicas, Direitos Autorais (mídias)
Pelo método de acerto	Bilateral, Multilateral (através de casas de <i>clearing</i> )
Pelo tipo de transação	Pague Para Ver ( <i>Pay Per View</i> ), Pagamento Posterior ou Pré-Pagamento
Pela geografia	Doméstico, Internacional, Apenas uma Moeda, Múltiplas Moedas
Pela localização das informações da conta do pagante	Baseado em Rede/Servidor, Dispositivo (baseado no cliente) ou Chip (baseado no cliente)

Tecnicamente, do ponto de vista dos aparelhos telefônicos a serem utilizados, as soluções de *m-payments* podem ser implementadas das seguintes formas [20]:

- Telefones móveis poderiam ser usados sem nenhum tipo de software ou hardware especial. Usa-se nesse caso somente tecnologias convencionais de transmissão (como por exemplo SMS ou WAP). Portanto, nenhum cartão de pagamento envolvido. Essa opção foi a escolhida para a proposta do modelo e da implementação deste trabalho que serão tratado posteriormente.

- Uma aplicação de pagamento poderia ser instalada em um cartão SIM. Por exemplo, dados relacionados ao pagamento, chaves de criptografia podem ser armazenados no chip SIM. Esse chip poderia se tornar o cartão de pagamento.
- O telefone móvel poderia conter 2 chips SIM. Neste caso o emissor do segundo cartão não precisaria ser necessariamente a operadora, como explicado na seção 2.7.
- O telefone móvel poderia conter um conector a mais para interfacear um cartão de pagamento (como um cartão de crédito ou débito baseado em um chip)

## **2.7 Modelos apropriados para os pagamentos móveis**

Como foi descrito na seção 2.4, existem diversos consórcios formados para padronizar sistemas de *m-payment*, cada qual com objetivos diferentes e defendendo o interesse de um tipo de indústria em específico.

O papel de cada entidade nos *m-payments* dependerá muito da estratégia adotada pelas instituições não financeiras que queiram entrar nesse mercado, especialmente as empresas de telecomunicações ou novas empresas criadas especificamente para esse propósito. Essas empresas poderiam fazer parcerias com os bancos ou estabelecer uma rede de pagamentos alternativa. Existe também a possibilidade dos telefones móveis se tornarem apenas dispositivos de acesso à conta bancária do cliente.

Esta seção faz um levantamento dos diferentes modelos que surgem a partir dessa diversidade de objetivos.

### **2.7.1 Modelo dominado por bancos**

Neste modelo, os bancos controlam toda a cadeia de valor, uma vez que operadoras de telecomunicações irão executar apenas o transporte de dados. Na prática, o dispositivo móvel se tornaria apenas uma nova forma de um cliente ter acesso às suas contas de banco.

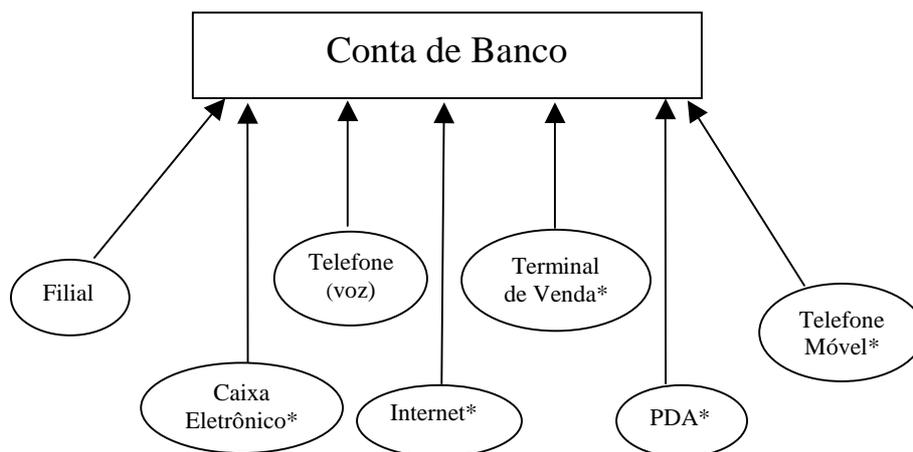


Figura 8. Modelo dominado pelos bancos [12].

Conforme indicado na Figura 8, o mercado de dispositivos (marcados com um asterisco) pode necessitar de um *smart card* para fazer pagamentos. Embora não sejam essenciais, pois podem ser usados números PIN de identificação (como no caso do atual acesso a bancos pela Internet), este cartão seria emitido pelos bancos para aumentar a segurança do armazenamento de dados e transações e permitir uma identificação forte [20]. Para o cliente, isso seria também mais conveniente, pois evitaria a necessidade de digitar os números de identificação e senha toda vez que um pagamento tenha que ser efetuado.

Com relação aos dispositivos móveis utilizados, existem várias possibilidades para implementar uma solução baseada em *smart card* do banco. O telefone poderia ter um leitor convencional de cartões de crédito ou débito como implementado pela France Telecom Mobile [36]. Uma segunda opção é a de se ter lugar para dois microprocessadores dentro do telefone, sendo um deles responsável pelo processo de pagamento. Essa foi a solução recomendada pelo Fórum Mobey [20].

Desde que esses chips sejam emitidos pelos bancos, eles têm controle completo da relação com o cliente e do processo de pagamento. Assim eles irão manter sua supremacia em prover serviços de pagamentos. Neste caso, entretanto, a competição no setor se manteria a mesma e a possibilidade de novos entrantes no mercado de pagamentos (como empresas de telecomunicações ou provedores de serviços independentes) seria muito pequena.

### **2.7.2 Modelo dominado por novos provedores de serviços de pagamentos**

O modelo dominado pelos bancos é somente uma possibilidade. Um cenário diferente seria a de empresas de telecomunicações e outras empresas que não sejam bancos possam oferecer serviços de pagamentos e usarem a Internet, o telefone móvel, ou o PDA como dispositivos de acesso, analogamente ao que fazem as empresas de cartão de crédito com seus pontos de venda (POS). Assim como ocorre com os cartões de crédito, o pagamento final é feito através de transferências bancárias. Os bancos, entretanto, não teriam mais envolvimento direto na relação consumidor-comerciante. O contato tanto do consumidor como do comerciante iria ser feito diretamente pelo intermediário. A princípio, esses intermediários podem oferecer uma ampla gama de tipos de pagamento como contas pré-pagas, cartões pré-pagos, contas pós-pagas além dos métodos tradicionais como cartões de crédito e transferências bancárias.

Este segundo cenário possibilitaria um aumento da competição no mercado de pagamentos.

Devido à necessidade de se ter uma licença para operar transações de pagamentos, ou pelo menos uma licença EMI (*Electronic Money Institute*) [37], no caso da Europa (no Brasil esse tipo de regulamentação ainda está em estágios iniciais [38]), uma saída seria a de se formar parcerias entre bancos e esses novos entrantes. Para as empresas de telecomunicações ou provedores de serviços independentes, isso seria interessante para retirar deles as preocupações com as regulamentações dos pagamentos. Além disso, iriam utilizar os nomes dos bancos como entidades já confiáveis por parte dos usuários. Para o setor bancário, seria interessante fazer essa parceria para evitar que operadoras ou novos entrantes entrem no mercado de pagamentos hoje dominados pelas instituições financeiras. Outra vantagem seria a possibilidade de conseguir novos clientes (clientes dos novos entrantes) e também uma forma de manter os custos reduzidos, tendo em vista, por exemplo, que hoje as operadoras de telefonia móvel subsidiam uma boa parte do valor do telefone móvel. Isso terá que ser feito pelos bancos, caso essa parceria não ocorra.

### 2.7.3 O papel das operadoras de telecomunicações

O papel das operadoras de telecomunicações ainda não está perfeitamente definido. Conforme descrito por Krueger [14], existem três possíveis cenários que as operadoras podem desempenhar:

- Provedores de Comunicações: Empresas de telecomunicações permanecem em seus negócios atuais, que atualmente tem tido suas margens de lucro reduzidas. Estabelecendo serviços de valor agregado, como pagamentos, parece ser o caminho natural dessas empresas para gerar receitas extras. Muito provavelmente as operadoras não ficarão fora desse mercado.
- Sistemas de Cobrança: As empresas de telecomunicações implementam sistemas de cobrança para oferecer para os comerciantes. Esses sistemas permitirão aos consumidores ter disponível uma cobrança confiável por parte das operadoras. Isso gera maior tráfego na rede e também as operadoras poderão cobrar uma comissão pela execução dos pagamentos. O problema que vem junto a essa solução é o risco de crédito. As operadoras terão que gerenciar o risco se o consumidor não puder pagar pelas mercadorias compradas antes do final do período de cobrança. As empresas de telecomunicações terão que administrar, por exemplo, limites de crédito para evitar fraudes [77]. Terão também que estabelecer acordos com outras empresas de telecomunicações caso seus clientes queiram efetuar uma compra em áreas em que não estejam presentes.
- Soluções Pré-Pagas: As empresas de telecomunicações nesse caso simplesmente debitam pagamentos para uma conta ou cartão pré-pago. Isso reduz o risco, como mencionado no caso anterior. Nesse caso, entretanto, haveria a necessidade de se ter uma licença de banco ou EMI, como estabelecido na regulamentação Européia. Como descrito anteriormente, no Brasil essa regulamentação ainda está em estágio inicial tendo em vista que nenhum serviço desse tipo foi colocado em operação ainda.

Esses são cenários em que as operadoras de telecomunicações móveis entrariam no mercado de forma independente. Outra possibilidade seria a de estabelecer uma parceria com bancos para aproveitar a sinergia entre a experiência das operadoras no lado técnico e a experiência dos bancos no lado financeiro.

#### **2.7.4 Modelo dominado pelos Intermediários / Novos Entrantes (Start-ups)**

Por causa da demora em lançar iniciativas de sucesso neste mercado por parte das operadoras e dos bancos, surgem oportunidades para novas empresas. Basicamente, essas novas empresas servirão como intermediários entre as operadoras móveis e os bancos. E esses novos entrantes irão precisar adquirir as licenças necessárias para operar nesse mercado. Assim, as operadoras não teriam que se preocupar com a regulamentação de pagamentos se elas trabalhassem com essas novas empresas. As novas entrantes também assumiriam o risco financeiro que as operadoras normalmente não estão dispostas a assumir.

Um dos casos de maior sucesso na Europa é a Paybox [39] e essa empresa é parcialmente pertencente ao Deutsche Bank, o que indica que os bancos também têm interesse em trabalhar com esses intermediários que usariam os seus serviços bancários.

### **2.8 Considerações sobre o estado atual de *m-payments***

#### **2.8.1 Questões a serem resolvidas**

Essa seção tem o objetivo de identificar algumas questões a serem resolvidas no cenário de pagamentos móveis. Conforme identificado por Taresewich [40], esses possíveis problemas são classificados nas seguintes categorias:

##### **Questões relacionadas ao hardware e software dos dispositivos móveis**

A questão é definir qual o melhor dispositivo para suportar os pagamentos móveis que podem ser um telefone móvel, um PDA, um *laptop* ou qualquer tipo de dispositivo que permita uma comunicação móvel segura que possa efetuar a transação financeira.

Essa escolha envolve principalmente a conveniência e a facilidade de utilização do dispositivo que é essencial para o incentivo da adoção dessa nova tecnologia. Os usuários procuram por dispositivos fáceis de utilizar, e se esse for muito complicado ou ficar indisponível por falta de sinal ou bateria, a maioria destes usuários ficarão relutantes em utilizar o novo serviço.

##### **Questões relacionadas à infra-estrutura das telecomunicações móveis**

O tipo da rede sem fio a ser utilizada deverá ser definido. Existe hoje uma série de tecnologias sem fio disponíveis, como será descrito no capítulo 3, e definir qual a mais

apropriada é uma tarefa difícil. Existem vantagens e desvantagens em cada uma e, portanto, a infra-estrutura escolhida deve ser definida de acordo com o tipo de pagamento. Hoje redes de comunicações de dados (como WLAN, WiFi, Bluetooth, WiMax e outras) e redes de telefonia (como GSM, GPRS, CDMA e outras) trazem uma nova dimensão a esta questão.

A cobertura da rede é um dos principais parâmetros a serem utilizados ao definir a melhor tecnologia e obviamente cada tipo de cobertura é apropriado para cada tipo de pagamento. Por exemplo, as tecnologias Bluetooth ou a de infravermelho são apropriadas para pagamentos próximos (como é o caso de máquinas de vendas) mas não para transações remotas. Então os provedores de pagamentos móveis devem escolher a tecnologia baseada no tipo de cobertura apropriado para a transação de pagamento.

### **Outras questões relacionadas à tecnologia sem fio**

A tecnologia sem fio adiciona uma dificuldade a mais, que é o fato dos dados serem vulneráveis a uma captura da informação por uma terceira parte não autorizada a receber aquela informação. Já existem métodos para reduzir o risco dos dados transmitidos pela rede sem fio sejam capturados, como é o caso da utilização da criptografia, entretanto isso exige um poder de processamento maior do dispositivo móvel sendo utilizado e também exige uma maior capacidade de transmissão de dados.

### **Questões relacionadas à aplicação dos pagamentos móveis**

A aplicação em si do pagamento móvel pode ser um problema para uma adoção em larga escala desse tipo de transação financeira. As aplicações devem estar de acordo com a expectativa dos consumidores.

A solução de pagamentos móveis deve oferecer condições para se efetuar pagamentos, independentemente do valor financeiro em questão (micro-pagamentos e macro-pagamentos). Como mencionado anteriormente, micro-pagamentos representam um nicho de mercado interessante para as operadoras e para novos entrantes uma vez que cartões de crédito não são apropriados para pagamentos de baixo valor. Entretanto, macro-pagamentos representam uma capacidade de se gerar uma maior receita devido a taxas de transações mais altas. A aplicação deve ser adaptável para micro-pagamentos, que devem ser rápidos e convenientes, e para macro-pagamentos, que devem ser extremamente seguros.

Transações financeiras também devem ser capazes de serem efetuadas tanto face a face como de forma remota. Pagamentos remotos são apropriados principalmente para *e-commerce*, enquanto pagamentos face a face serão capazes de substituir os pagamentos tradicionais entre duas partes (B2C ou P2P) que estão presentes em um mesmo lugar. A aplicação de pagamento também deve ser capaz de endereçar esse aspecto da proximidade.

### **Questões globais relacionadas aos pagamentos móveis**

Uma maneira de se efetuar pagamentos móveis é oferecer uma maneira universal para pagar. A possibilidade de pagar qualquer pessoa ou entidade, em qualquer lugar, a qualquer hora irá aumentar a chance da nova solução de pagamento ser adotada. Portanto instituições financeiras e operadoras estão buscando a formação de alianças para oferecer uma solução padrão.

A questão dos custos também é outra questão a ser analisada. A maioria dos consumidores não está disposta a pagar por uma taxa extra se o pagamento móvel não oferecer realmente valor agregado ao que já está disponível hoje. Será muito difícil convencer esses consumidores a utilizar a nova solução se essa forma for mais cara que as soluções tradicionais.

Uma outra questão a ser também estudada é a necessidade de confiança, essencial em serviços financeiros. Usuários não irão adotar o serviço se não confiarem nele. A definição de políticas de segurança e de reversão de pagamentos são essenciais para que os usuários continuem usando os serviços, mesmo após algum tipo de problema em transações.

Por último, a questão de como as novas regulamentações nesse setor, que vão ser definidas, serão importantes para seu desenvolvimento. As operadoras e os novos entrantes serão os mais afetados por essas regulamentações tendo em vista que os bancos já são extremamente regulados.

### **2.8.2 Segurança em pagamentos móveis**

Além das questões citadas acima, a questão da segurança nos pagamentos móveis é fundamental para o sucesso dos pagamentos móveis. Embora o objetivo desse trabalho não seja o de se aprofundar nessa questão, seguem abaixo algumas considerações sobre segurança.

Conforme descrito por Torvinen [45], não existe uma maneira de se garantir segurança total ao se enviar informação confidencial através de uma rede aberta como a Internet ou uma rede móvel. Existem basicamente duas iniciativas de associações de empresas de cartão: a especificação segura Visa 3-D [41] e a MasterCard SPA [42].

Existem também, conforme mencionado anteriormente, alguns consórcios e fóruns (Iniciativa MeT, Fórum Mobey, PayCircle, etc) que também estão trabalhando em especificações para pagamentos móveis. Todos eles buscam o desenvolvimento de padrões para prover transações móveis seguras. Segurança também é um aspecto essencial para permitir aos usuários confiarem nos pagamentos móveis [77].

Pagamentos móveis devem seguir cinco critérios clássicos de segurança [44]:

- Confidencialidade: Apenas o emissor e o receptor dos detalhes de pagamento devem ter acesso às informações de pagamento. Como o método de pagamento irá proteger contra o monitoramento passivo dos detalhes de pagamento (tais como os detalhes pessoais do consumidor ou a senha)?
- Autenticação: Como o método de pagamento irá garantir que o consumidor e o comerciante são quem realmente quem eles dizem ser?
- Integridade: Como o método de pagamento pode proteger os detalhes de pagamento de tal forma a garantir que eles não sejam modificados entre o momento em que são enviados e o momento em que são recebidos?
- Autorização: Como o método de pagamento irá garantir que apenas consumidores autorizados consigam efetuar o pagamento? Essa é uma questão diferente de simplesmente identificar o consumidor. Quais são os procedimentos para autorizar o consumidor?
- Não repudição: Como o método de pagamento irá garantir que o consumidor não possa falsamente alegar que ele não participou de uma transação?

Uma vez que serviços financeiros podem estar sujeitos a atividades fraudulentas, eles precisam de uma infraestrutura bem segura. Os principais riscos são o de alguém não autorizado capturar as informações durante a comunicação e a de uma terceira parte

se fazer passar pelo provedor de pagamentos. Portanto, autenticação, confidencialidade e integridade devem ser implementados na solução para prevenir esses riscos e dar maior confiança aos consumidores em utilizar a nova tecnologia. Maiores detalhes sobre segurança em pagamentos móveis podem ser obtidos em [43] e [44]. Uma descrição sucinta dos principais protocolos de segurança também pode ser encontrada no capítulo 3.

## 2.9 Modelos propostos em outros trabalhos

Alguns trabalhos foram encontrados na literatura acadêmica buscando a definição do estado da arte de pagamento móveis em geral.

Nambiar e Lu [77] descrevem o modelo de pagamentos móveis do ponto de vista de sua cadeia de valor, ciclo de vida e características. São analisadas soluções de pagamentos móveis que podem ser adotadas pela indústria e também são definidas as principais fraudes que podem ocorrer nesse contexto e possíveis soluções para que sejam prevenidas essas fraudes. O trabalho conclui que é essencial o desenvolvimento de sistemas de gerenciamento de fraude para o ambiente de pagamentos móveis que tem como principais desafios o monitoramento das atividades dos usuários e de estar alerta a natureza de mudanças das fraudes.

N. Kreyer<sup>1</sup>, K. Pousttchi, K. Turowski [80] descreveram as características dos diversos procedimentos dos pagamentos móveis buscando a padronização das mesmas para garantir que pudessem ser adotadas em maior larga escala e propiciar um maior investimento nestas garantindo seu desenvolvimento. Ao descrever esses procedimentos, os autores tiveram a preocupação de garantir que estes pudessem funcionar em diversos cenários de comércio móvel, comércio eletrônico, comerciante estacionado e de C2C (*customer to customer*). Os procedimentos de pagamento ainda foram classificados por critérios de estratégia, participação e operacional utilizando um método morfológico.

Hort, Gross e Fleisch [79] analisam os fatores críticos de sucesso dos pagamentos móveis. São analisadas a percepção dos consumidores com relação ao instrumento de pagamentos, e a aceitação do comerciante com relação ao método de pagamento uma vez que este arca, segundo o trabalho, com a maior parte dos custos associados a plataforma e, portanto, assume um maior risco que os consumidores. São analisadas as

tecnologias disponíveis e como elas podem afetar positivamente ou negativamente o sucesso das soluções de pagamento.

Fleisch, Lampe e Müller [78] definem como *u-payment* (*ubiquitous payment*) o tipo de pagamento móvel que utiliza dispositivos com tecnologias não obstrusivas (*unobtrusive technologies*) como RFID. Este trabalho busca identificar requisitos e testar tecnologias para serem utilizadas em *u-payments* em um trabalho de pesquisa conjunto com o UBS (*United Bank of Switzerland*). O trabalho baseado na arquitetura do Fórum Mobey [20] desenvolve um sistema de testes completo de pagamentos denominado BluePay, com o objetivo de ganhar experiência com pagamentos locais utilizando tecnologias como Bluetooth e RFID. Os principais resultados desse trabalho são a definição de *u-payment* pelos autores e quais as implicações de sua adoção garantindo estar sempre presente em todos os lugares (*ubiquitous*), não obstrusiva e invisível.

## **2.10 Considerações finais**

A importância da tecnologia de pagamentos móveis tem aumentado devido, principalmente, ao surgimento de novas tecnologias e à prevalência da telefonia móvel. Essa importância crescente do *m-payment* deu origem nos últimos 5 anos à formação de consórcios com objetivos de padronizar modelos e tecnologias associadas.

Este Capítulo tratou dessa questão, apresentando os principais conceitos e modelos relacionados a esse tema. No próximo capítulo algumas das principais tecnologias estudadas neste trabalho, e que serão empregadas no modelo de pagamentos móveis proposto, serão apresentadas. Serão relacionadas também as principais soluções hoje já disponíveis no mercado.

## 3. Tecnologias Móveis e Web Services

### 3.1 Introdução

O desenvolvimento e consolidação de uma série de novas tecnologias vêm permitindo a proposição de novos tipos de serviços, tais como *m-commerce*, onde o papel de *m-payment* passa a ganhar importância crescente. Essas tecnologias têm em comum o fato de estarem relacionadas com: o desenvolvimento de aplicações na web; suportes a comunicações (principalmente sem fio); ao desenvolvimento de sistemas distribuídos fortemente acoplados (ex. Java RMI) ou fracamente acoplados (ex. *web services*).

Este Capítulo trata das diversas tecnologias que hoje competem para se tornarem os padrões em pagamentos móveis virtuais ou físicos. A gradual adoção de cada tecnologia por parte dos usuários terá papel fundamental no nível de sucesso de cada uma delas. Tanto para comerciantes como para consumidores, a solução de pagamento móvel se tornará popular apenas se esta se mostrar mais simples de ser utilizada e mais econômica que os métodos convencionais.

Essas tecnologias foram estudadas no desenvolvimento deste trabalho de mestrado, e suas características, que as tornam adequadas para determinadas partes do sistema, são enfatizadas neste texto. Nesse sentido, também foi feita uma comparação extensiva entre o uso de serviços web e CORBA. Contudo, esse estudo comparativo é apresentado no Anexo I deste texto.

### 3.2 Tecnologias de redes de telefonia móvel

As tecnologias de redes móveis [46] evoluíram de sistemas analógicos para sistemas digitais e de tecnologias baseadas em circuito para tecnologias baseadas em pacotes. Essa evolução pode ser descrita por diferentes gerações de tecnologias móveis como as tecnologias da primeira geração (1G), da segunda geração (2G), da 2.5G e da terceira geração (3G). Apenas a 1G é baseada em tecnologia analógica. Alguns dos padrões de cada geração são:

- **1G:** AMPS (*Advance Mobile Phone System*), TACS (*Total Access Communication System*), NTT (*Nippon Telegraph & Telephone*), CDMAONE (*Code Division Multiple Access One*).

- **2G:** GSM (*Global System for Mobile Communication*), CDMA2000 (*Code Division Multiple Access 2000*), HSCSD (*High Speed Circuit Switched Data Technology*), TDMA (*Time Division Multiple Access*).
- **2.5G:** GPRS (*General Packet Radio System*), EDGE (*Enhanced Data Rate for GSM Evolution*).
- **3G:** UMTS (*Universal Mobile Telephone Standard*), WCDMA, CDMA 1xEV.

No Brasil, o estágio de evolução atual está na 2.5G.

### 3.2.1 GSM

A tecnologia GSM [47] é um padrão da segunda geração para comunicação móvel, desenvolvida pela ETSI (*European Telecommunications Standards Institute*) e atualmente administrada pela 3GPP (*Third Generation Partnership Project*). Operando nas bandas de frequências 900 MHz e 1800MHz, o GSM é o padrão mais utilizado atualmente na Europa e na Ásia. No Brasil, esta tecnologia foi adotada muito rapidamente nos últimos anos.

Essa tecnologia empregou métodos digitais, diferentemente dos sistemas celulares analógicos como AMPS e TACS. As técnicas utilizadas são uma combinação entre o TDMA e o FDMA (*Frequency Division Multiple Access*), que são basicamente utilizadas para transmissão de voz e controle. Uma vez que usuários compartilham o mesmo espectro de rádio e este é limitado, essas técnicas permitem dividir a largura de banda entre o máximo de usuários.

Os serviços oferecidos pela tecnologia GSM [48] são:

- Serviço de telefonia básico.
- Serviços de dados:
  - Serviços de Internet: receber e enviar dados na velocidade de 9.6Kbps.
  - SMS (*Short Message Service*): serviço bidirecional de mensagens alfanuméricas de até 160 bytes, a ser descrita em mais detalhes na seção 3.3.1.

- Facsimile: Enviar e receber mensagens de fax utilizando o telefone GSM e um computador.
- Acesso seguro a uma LAN corporativa: acesso seguro a e-mails, faxes, e transferência de arquivos através de um *link* criptografado.
- Serviços adicionais: Reenvio de chamada, bloqueio de chamada, identificação da origem da ligação, espera de chamada e conferência. Essas funções podem ser controladas através de APIs GSM, como as especificadas pelo Grupo Parlay [65].

O GSM é limitado devido a sua baixa velocidade de transmissão e além disso o acesso à Internet é baseado em tempo ao invés de quantidade de dados transmitidos como é o caso de tecnologias mais novas como o GPRS.

### **3.2.2 HSCSD**

HSCSD [49] é um protocolo baseado em circuito e na tecnologia GSM, provendo um avanço na transmissão de dados quando comparado ao GSM. Essa tecnologia possibilita a transmissão de dados em uma velocidade maior usando múltiplos canais, diferentemente de um canal único de voz como no GSM. A velocidade de transmissão pode chegar a 57.6 Kbps utilizando quatro canais de rádio simultaneamente. Essa tecnologia foi utilizada por pouco tempo até ser substituída pelo GPRS.

### **3.2.3 GPRS**

O GPRS [50] é protocolo sem fio baseado em pacotes que provê um serviço de valor agregado, mas não destinado a voz, que permite que informação seja enviada e recebida através da rede de telefonia móvel. Esta tecnologia já é considerada como sendo da geração 2.5G, pois é baseada em pacotes, diferentemente da tecnologia GSM que é baseada em circuitos. A velocidade de transmissão de dados varia entre 9,6 kbps e 171,2 kbps (teoricamente) ao se utilizar essa tecnologia. Além de velocidades maiores, o GPRS provê uma conexão permanente para o usuário e normalmente o pagamento pela utilização é baseado somente na quantidade de dados trafegada ao invés do tempo de conexão. O GPRS é uma tecnologia mais desenvolvida e um passo intermediário até a adoção das tecnologias 3G, como EDGE e UMTS. Algumas das aplicações GPRS são acesso a Internet e Intranet, e-mail, fax e mensagens.

### **3.2.4 EDGE**

O EDGE [47] é uma versão do GPRS com maior largura de banda, permitindo transmissões de até 384 kbps. Esta tecnologia também é compatível com o protocolo GSM, mas requer uma qualidade melhor dos sinais de rádio para atingir essa velocidade mais elevada de transmissão.

Ao implementarem essa tecnologia, as operadoras de redes móveis serão capazes de suportar aplicações móveis multimídia de alta velocidade. O EDGE também representa um passo intermediário entre o GPRS e o UMTS devido à necessidade de alterações na modulação da rede atual para a implementação do UMTS (ver seção 3.2.5). Muitas empresas estão considerando adotar essa tecnologia antes da UMTS, mas nenhum investimento significativo foi feito até agora e a janela de oportunidade para essa tecnologia pode ser muito pequena, a não ser que grandes atrasos do desenvolvimento da UMTS aconteçam.

### **3.2.5 3G**

A terceira geração 3G é o termo genérico para o próximo grande passo no desenvolvimento da tecnologia móvel. O padrão oficial para o 3G é o IMT-2000 (*International Mobile Telecommunications 2000*) [51]. Este padrão tem sido estabelecido por diversas comunidades de desenvolvedores como o W-CDMA (*Wideband Code Division Multiple Access*) que é defendido pela Ericsson, Nokia e fabricantes de aparelhos japoneses e o CDMA2000 que é defendido pela Qualcomm e Lucent.

UMTS (*Universal Mobile Telephone System*) [46] é planejada para prover para a 3G serviços de dados. Expectativas realísticas da tecnologia sugerem uma capacidade máxima em áreas metropolitanas de 384 Kbps, pelo menos nos anos iniciais do seu desenvolvimento. Este sistema permite a transmissão de vídeo, dados e voz em alta velocidade e baixo custo. Este sistema já está implementado no Japão.

## **3.3 Serviços de comunicação móvel**

### **3.3.1 SMS (*Short Messaging Service*)**

O SMS [52] foi criado como parte do padrão GSM para enviar e receber mensagens de texto com até 160 caracteres alfanuméricos de comprimento entre telefones móveis. O

SMS é um serviço inteligente (quando comparado, por exemplo, ao *paging*) uma vez que este pode armazenar mensagens quando o telefone móvel destinatário está desligado e envia essas mensagens armazenadas quando o telefone volta a seu uso normal. Algumas das aplicações de SMS são notificações de mensagem de voz ou fax, mensagem unificada (em que o usuário pode acessar através de uma única caixa de entrada vários tipos diferentes de informação como mensagem de voz, fax, e-mail), entrega de toques e logos para telefones, comunicação pessoal através de mensagens de texto, e qualquer serviço de informação que possa ser entregue em pequenas mensagens de voz.

### **3.3.2 WAP (*Wireless Application Protocol*)**

O WAP [53] é uma tecnologia que permite disponibilizar informações da Internet em um telefone móvel ou qualquer dispositivo sem fio. Isso é feito através da tradução das informações da Internet em um formato que possa ser mostrado considerando as limitações dos telefones móveis. O WAP é um padrão aberto, desenvolvido pelo *Forum WAP* [53], que tem mais de 500 membros. Os fundadores deste fórum são grandes fabricantes de equipamentos sem fio como a Nokia, Ericsson, Motorola e uma empresa de software americana, Phone.com. Hoje esse fórum faz parte da OMA (*Open Mobile Alliance*) [54].

Para se conseguir acesso a Internet, o telefone móvel deve ser compatível com a tecnologia WAP e a informação do sítio web deve estar no formato WML (*Wireless Markup Language*). WML é o equivalente ao HTML usado na Internet convencional. Um gateway WAP também é necessário entre o dispositivo móvel e o servidor WML, para traduzir a requisição WAP. A resposta do servidor é traduzida para uma resposta WAP pelo gateway WAP, que poderá ser exibida no dispositivo móvel.

### **3.3.3 I-Mode**

O I-Mode [55] é uma tecnologia sem fio desenvolvida pela empresa japonesa NTT DoCoMo, que também permite o uso de serviços de Internet através de telefones celulares. O I-Mode pode ser utilizado para trocar e-mails com computadores, PDAs (*Personal Digital Assistants*) e outros telefones celulares I-Mode. O I-Mode já dominou o mercado japonês e tem sido considerado um sucesso no comércio móvel.

O I-Mode é uma tecnologia simples de ser utilizada o que incentiva provedores de serviços a criarem novos serviços baseados nesta tecnologia e permite aos usuários utilizá-los sem grandes complicações. O serviço utiliza a linguagem de *mark-up* HTML compacto (cHTML), que é uma versão simplificada do HTML original. cHTML é relativamente simples e a conversão de HTML para cHTML pode ser feita sem dificuldades. A velocidade de transmissão do I-Mode é, entretanto, de apenas 9,6 kbps. A DoCoMo opera uma rede baseada em pacotes, o que significa que os usuários não pagam baseados em tempo e sim pela quantidade de pacotes transmitidos, e portanto também têm uma conexão permanente, algo análogo ao GPRS.

#### **3.3.4 USSD (*Unstructured Supplementary Services Data*)**

USSD é um mecanismo de transmissão de informação através de uma rede GSM. É uma tecnologia similar ao SMS, entretanto oferece apenas um serviço de armazenamento e envio. USSD oferece uma conexão em tempo real durante uma sessão.

A conexão de rádio continua aberta até que o usuário ou a aplicação a desconecte, o que é interessante para aplicações de tempo real. Esta tecnologia tem sido usada principalmente para serviços financeiros, compras e pagamentos.

#### **3.3.5 *Cell Broadcast***

Cell Broadcast, desenvolvida pelo fórum *Cell Broadcast* [56] é uma tecnologia projetada para entregar simultaneamente mensagens de texto para diversos usuários dentro de uma área específica ou em um determinado país. Cell Broadcast é similar ao SMS, mas é um serviço de um-para-muitos ao invés de um-para-um. É um serviço de distribuição em massa para notícias e informações genéricas.

#### **3.3.6 Toolkit de aplicação SIM (*Subscriber Identity Module*)**

O Toolkit de aplicação SIM é um padrão da ETSI (*European Telecommunications Standards Institute*) [57] para serviços de valor agregado e comércio eletrônico usando telefones GSM para executar transações. Esta tecnologia permite às operadoras de telecomunicações móveis enviar aplicações via SMS ou como uma mensagem Cell Broadcast de maneira a atualizar os cartões SIM ou adicionar novos serviços. As aplicações baseadas no Toolkit SIM são construídas em Java em um ambiente cliente

servidor. Praticamente todos os fabricantes de telefones desenvolveram aparelhos com o Toolkit SIM, mas por existirem muitas classes diferentes no protocolo, nem todos aparelhos executam todas as aplicações. Um exemplo de aplicação já bastante utilizada por essa tecnologia é o *download* de toques de celulares.

O Toolkit SIM, programado em um chip SIM, permite a este chip SIM, utilizando o aparelho GSM, uma troca interativa de informações entre a aplicação e o usuário final. O chip também tem o objetivo de controlar o acesso à rede.

Segurança é uma característica fundamental do Toolkit SIM, uma vez que confidencialidade e integridade já estão incluídas no padrão. Notam-se já algumas aplicações bancárias utilizando este tipo de tecnologia em alguns países. Serviços de e-mail e de informações também fazem uso desta tecnologia. O protocolo WAP 2.0 irá incluir o Toolkit SIM e será como a nova geração desta tecnologia.

### **3.3.7 MExE (*Mobile Station Application Execution Environment*)**

O MExE, também especificada pela 3GPP, é essencialmente a incorporação da máquina virtual Java em um telefone móvel permitindo a execução completa de aplicações. Este protocolo permite a execução de serviços de localização e uma variedade de interfaces, como o reconhecimento de voz. O MExE irá incorporar as tecnologias WAP, J2ME, CLDC e MIDP.

## **3.4 Protocolos de segurança em pagamentos móveis**

Embora um exame detalhado dos aspectos de segurança no comércio móvel esteja fora do escopo desta dissertação, segue abaixo uma visão geral das principais tecnologias que possibilitam essa segurança nos pagamentos móveis.

Criptografia pode ser utilizada para garantir a confidencialidade e é o processo em que informações representadas na forma de texto são transportadas na forma de dados não compreensíveis. Isso é conseguido através da codificação dos dados e chaves de decodificação.

Os mecanismos a seguir são baseados em sistemas de criptografia de chave pública. Estes sistemas de criptografia definem como a codificação e decodificação são efetuadas. Em um sistema de criptografia de chave pública, um par de chaves

relacionadas é utilizada: uma chave pública, que é de conhecimento de todos, e uma chave privada, que é secreta.

Assinaturas digitais podem ser utilizadas para garantir a autenticidade de uma transação entre duas partes, a integridade e a não repudição das transmissões. Uma assinatura digital é um dado que acompanha uma mensagem codificada digitalmente [50]. Uma assinatura digital é utilizada codificando o conteúdo dos dados a serem transmitidos usando uma chave privada. Isso garante que a assinatura digital não pode ser forjada e a única parte que pode ter enviado aquela informação é a detentora dessa chave privada. Funções matemáticas como as funções de *hash* podem ser utilizadas para diminuir o tamanho da assinatura digital.

Para verificar a assinatura digital, deve-se utilizar a chave pública da parte que assinou os dados. É importante garantir que a chave pública utilizada nesse processo é a correta, caso contrário, existem oportunidades para brechas de segurança. Certificados digitais permitem que as chaves públicas possam ser distribuídas de uma forma segura o que provê essa garantia.

Um certificado digital é uma coleção de informações em que a uma assinatura digital foi anexada por alguma autoridade reconhecida ou acreditada por alguma comunidade de usuários de certificados [50]. Um tipo comum de certificado digital é o certificado de chave pública, que, de forma única, liga uma pessoa particular, dispositivo ou entidade a uma chave pública. Um certificado digital contém quatro componentes principais [51]: uma chave pública, informação associando essa chave pública ao seu dono, informação sobre o emissor do certificado e a assinatura digital deste emissor. Uma Autoridade de Certificação emite certificados digitais.

Uma PKI (*Public Key Infrastructure*) é definida pelo Grupo de Trabalho PKIX como um conjunto de hardware, software, pessoas e procedimentos necessários para criar, gerenciar, armazenar, distribuir e revogar certificados baseados em criptografia de chave pública [51]. Este é o conjunto de padrões que controlam o ciclo de vida dos certificados digitais. Uma PKI pode ajudar a endereçar os aspectos de não-repudição e na autorização da segurança.

As tecnologias mencionadas acima são instrumentos para estabelecer um ambiente seguro para pagamentos no comércio móvel. Um exemplo disso é o WTLS, um protocolo seguro na arquitetura WAP que inclui criptografia e certificados digitais.

WTLS garante a segurança na comunicação entre o aparelho móvel do consumidor e o gateway WAP.

Um outro exemplo de protocolo é o SET (*Secure Electronic Transaction*) [35], que foi anteriormente ilustrado na Figura 4 do Capítulo 2. O SET é um protocolo especificado pela MasterCard e pela Visa para suportar pagamentos utilizando cartões de banco. O protocolo SET é implementado utilizando o PKI.

Métodos futuros de pagamento provavelmente irão basear-se em ambientes seguros oferecidos por uma implementação do PKI suportado pela especificação WAP, ou pelo Toolkit SIM [7]. Um modelo híbrido desses dois também parece ser possível. Até agora, ainda não há uma definição de qual desses modelos irá dominar o mercado sem fio.

Utilizando a tecnologia WAP, os consumidores serão capazes de se autenticar junto a comerciantes ou ao provedor de serviços de pagamentos utilizando WTLS e WIM (*Wireless Identity Module*), que irá armazenar referências para certificados digitais. Esses WIMs podem ser implementados utilizando *smart cards* ou chips SIM. Consumidores serão capazes de utilizar seus telefones móveis para assinar digitalmente e codificar a informação enviada por eles. Esses chips SIM nos aparelhos móveis dos consumidores servem de depósito para chaves privadas e certificados.

Tornar pagamentos móveis seguros não é apenas uma equação envolvendo tecnologia. O processo de estabelecer confiança é tão importante quanto. Uma terceira parte confiável pode ser utilizada para efetuar autenticações entre as partes envolvidas na transação. Essa terceira parte pode ser tanto a empresa de telecomunicações, como um banco, uma empresa de cartão de crédito ou uma nova entrante.

### **3.5 Plataforma Móvel de Programação (J2ME)**

J2ME (*Java 2 Micro Edition*) [30] provê um ambiente para o desenvolvimento de aplicações para dispositivos móveis. Devido ao limite de recursos de memória e de execução em um dispositivo móvel, J2ME foi projetado para limitar o uso destes recursos quando comparado a outras edições do Java 2.

J2ME define duas configurações de dispositivo, a Configuração de Dispositivo Conectado (CDC) e a Configuração de Dispositivo Conectado Limitado (CLDC). CDC

é projetado para dispositivos com maior capacidade de memória (2 a 4 Mbytes) e alta largura de banda. Já o CLDC é projetado para dispositivos de menor capacidade (como telefones móveis) com memórias limitadas (até 128 Kbytes) e baixa largura de banda.

O CLDC é estendido pelo MIDP (*Mobile Information Device Profile*). O MIDP define as características para um dispositivo móvel em uma camada acima do CLDC, provendo suporte para interface com o usuário, rede e armazenamento persistente. O MIDP oferece suporte para conexões através de *sockets* TCP/IP entre dispositivos móveis e também com aplicações de servidor. Também oferece suporte ao protocolo de segurança SSL (*Secure Socket Layer*) [71], que é essencial para sistemas de pagamentos.

### **3.6 Os serviços web (*web services*)**

O surgimento da Internet, e em particular a web, propiciou uma enorme evolução na forma como comunicações e negócios são feitos hoje. Os “internautas”, atualmente, podem comprar livros e CDs, fazer reservas e aquisição de passagens aéreas, adquirir e vender ações de empresas, participar de leilões, comunicar-se com pessoas espalhadas por todo o mundo e muitas outras atividades.

O surgimento da web também possibilitou a conexão entre diferentes negócios. Uma empresa pode comprar produtos de outra através da Internet. Contudo, por princípio, essa transação só era possível somente se alguém na primeira empresa entrasse em um computador e fizesse a compra no sítio da outra. A web não foi projetada para uma transação direta entre negócios e máquinas. Foi projetada para pessoas utilizarem.

A tecnologia de serviços web foi criada com o intuito de resolver, entre outros aspectos, este problema. Construir uma web orientada para utilização de pessoas é bem mais simples que conectar negócios através da Internet. Uma empresa que quer abrir um portal de comércio eletrônico tem somente que desenvolver uma nova interface (HTTP/HTML) para seus atuais sistemas que já estão sob completo domínio. Construir, entretanto, serviços web entre negócios, exige da empresa conectar os seus atuais sistemas a diversos outros sistemas externos (ou mesmo internos, no caso de sistemas diferentes da mesma empresa não se comunicarem e/ou entre áreas distintas da empresa

ainda não conectadas) e muitas vezes com tecnologias completamente diferentes ou antigas.

Empresas parceiras, onde a integração é importante, podem possuir sistemas baseados em Windows, outras em Linux e algumas até na antiga tecnologia de *mainframes*. Outras diferenças entre sistemas também podem ser citadas como diferentes tipos de *hardware* ou de linguagens de programação. Implementar a comunicação destes sistemas utilizando as tradicionais APIs pode ser extremamente difícil. Essas empresas precisam construir sistemas que podem se comunicar utilizando serviços independentes da tecnologia e adotar arquiteturas orientadas a serviço (SOAs - *Service-Oriented Architecture* [1]) projetados para o desafio de conectar sistemas distribuídos heterogêneos. (Esse tipo de arquitetura será descrito na seção 3.4.2 adiante.)

Os serviços web também devem ser mais tolerantes a faltas, tanto dentro da infraestrutura da Internet como em outros sistemas. Serviços web podem lidar com mudanças inesperadas em aplicações remotas, permitindo às empresas construir sistemas que são capazes de se adaptarem e responderem a eventos não planejados. Estes são os benefícios de utilizar-se acoplamento livre (*loose coupling* [1]). A definição de acoplamento livre será vista adiante.

Serviços web, portanto, utilizam interfaces padronizadas que são completamente separadas da operação interna dos componentes que constituem o sistema. As interfaces não mudam as funções individuais dos componentes, mas permitem que componentes ofereçam serviços para outros.

Esse conceito de programação usando componentes já existe há vários anos e as aplicações que se comunicam com outras utilizando APIs padrões já são comuns. Os serviços web, embora tenham herdado muitos dos conceitos destas tecnologias (como a SOA), permitem resolver vários problemas que não foram resolvidos com os sistemas baseados em componentes. Alguns dos benefícios oferecidos por serviços web são apresentados a seguir [1].

### **3.6.1 Principais características**

#### **Independência**

Serviços web permitem que aplicações se comuniquem, mesmo se forem escritas em linguagens de programação diferentes ou se forem executadas em sistemas operacionais

distintos ou em *hardware* de diversos fornecedores. Por serem tão genéricos, Serviços web reduzem de forma significativa a dependência de um fornecedor.

### **Padronização**

A vasta aceitação e adoção dos padrões dos serviços web significam que finalmente as empresas acordaram universalmente em uma tecnologia para a integração e comunicação entre aplicações. A adoção de serviços web está se tornando um padrão de comunicação, assim como ocorreu com o FAX e o email.

### **Capacidade de reutilização**

A modularidade – explicada no item anterior – permite uma melhor reutilização de serviços para outras aplicações, diferentes daquelas para as quais estes foram originalmente desenvolvidos. A habilidade de se reutilizar serviços já existentes significa uma redução do tempo de desenvolvimento das aplicações de negócios. Acrescenta-se ainda, que a reutilização em serviços web não requer software portátil ou reutilizável. É o serviço que é reutilizado e não o código fonte de um determinado objeto ou componente.

### **Custos menores**

A capacidade de reutilização e a arquitetura baseada em serviços (SOA) dos serviços web significam um melhor retorno no investimento feito pelas empresas. Uma maior padronização das interfaces dos serviços web irá permitir a integração de um novo sistema e a conexão de novos parceiros de negócios de uma maneira mais genérica e através de processos com maior facilidade de repetição dos que os utilizados atualmente.

### **Acoplamento Livre (*loose coupling*)**

Ao conectar dois sistemas, programadores são tentados a utilizar atalhos que economizam tempo e, portanto, reduzem investimentos imediatos. Por exemplo, se dois sistemas utilizam a mesma codificação para armazenar caracteres, programadores podem utilizar esta codificação para transmitir *strings* de um sistema para outro. Esta solução irá funcionar bem até que um terceiro sistema necessite ser conectado usando uma codificação diferente. Assim inicia-se uma solução complexa e de alto custo de integração.

Acoplamento livre (também chamado de acoplamento fraco) permite que dois sistemas díspares, utilizando tecnologias e processos diferentes, sejam conectados sem a necessidade de que uma das partes tenha conhecimento das tecnologias sendo utilizadas pela outra. Isso evita o problema citado acima, uma vez que sistemas de acoplamento livre podem se comunicar utilizando formatos e técnicas independentes dos sistemas.

### **Maior robustez**

Como no exemplo ilustrado no tópico acima, sistemas fortemente acoplados (*tightly coupled*), mesmo os baseados em componentes, têm maior probabilidade de falhar quando colocados para trabalhar em ambientes diferentes dos que foram projetados para funcionar. Serviços web são construídos usando uma arquitetura orientada a serviços (SOA) e de acoplamento livre, portanto os sistemas criados com eles são mais robustos e podem trabalhar em ambientes para os quais não foram projetados. São, assim, menos susceptíveis a falhar quando um serviço é alterado internamente e quando novos serviços necessitam ser conectados.

### **Escalabilidade**

A capacidade de reutilização e padronização dos serviços web permite o desenvolvimento de soluções que conectam um sistema em muitos sistemas, ao invés das mais tradicionais conexões de um sistema para outro. Uma vez que a tecnologia para conectar em vários sistemas é a mesma utilizada para conectar poucos sistemas, o custo incremental de adicionar um parceiro de negócios adicional ao sistema é praticamente nulo.

## **3.6.2 Aspectos técnicos de serviços web**

Os serviços web [1] são componentes de software baseados em XML e provêm uma arquitetura para serviços fracamente acoplados que podem ser publicados, localizados e invocados remotamente através de protocolos de Internet, por clientes escritos em uma linguagem diferente.

Os serviços web libertam sistemas distribuídos das restrições da uma única rede e permitem a integração de sistemas heterogêneos via Internet. Isso pode ser conseguido sem as dificuldades associadas com a re-configuração de *firewall* como é o caso de outras arquiteturas distribuídas como o Corba e o Java RMI. Esta arquitetura faz uso de protocolos de Internet existentes como o HTTP e o TCP/IP.

A Figura 9 ilustra a pilha dos protocolos principais que compõem a tecnologia de serviços web:

UDDI (Serviço de Diretórios)
WSDL (Descrição das Interfaces)
Mensagens SOAP
Codificação XML UTF
HTTP
TCP/IP

Figura 9. Pilha de Protocolos da tecnologia de serviços web.

## XML

O XML (*Extensible Markup Language*) [61] é o alicerce em que os serviços web são construídos através da descrição de todos os aspectos dos serviços web. XML define uma maneira padrão de se estruturar a informação para descrever, armazenar e trocar dados através de serviços web. Este padrão foi desenvolvido para aplicações que requerem uma funcionalidade a mais do que a oferecida pelo HTML.

XML permite a comunicação estruturada de dados entre componentes de serviços web. Não existe uma semântica pré-definida, portanto a definição dos dados a serem transmitidos deve ser previamente acordada entre as partes. Uma grande vantagem do XML é que pode ser utilizado para descrever qualquer tipo de documento (através da definição de *tags*), sem afetar o processo de troca de mensagens.

## SOAP

SOAP (*Simple Object Access Protocol*) [23] especifica um formato simples para transmitir mensagens codificadas em XML na arquitetura de serviços web. Mensagens SOAP são transmitidas através de protocolos padrões da Internet como HTTP, SMTP e MIME. Todas as mensagens SOAP são codificadas em XML e cada mensagem é um documento XML.

A estrutura da mensagem definida pelo SOAP consiste de três partes principais, o envelope, o cabeçalho (*header*) e o corpo (*body*). Todas as partes são obrigatórias em

uma mensagem, com exceção do cabeçalho que é opcional. O envelope é o componente XML de mais alto nível em uma mensagem SOAP. O envelope contém o cabeçalho e o corpo da mensagem, e é a unidade de comunicação. O cabeçalho é utilizado para estender o uso da mensagem SOAP com funcionalidades adicionais como segurança ou atributos de qualidade de serviço associados a mensagem. O corpo contém os dados que serão utilizados pela aplicação destino e também é descrita no formato XML.

## **WSDL**

WSDL (*Web Services Description Language*) [63] define uma maneira padrão de descrever e publicar os formatos e protocolos de um Serviço Web. Um arquivo WSDL descreve como um serviço é localizado e como acessá-lo. O WSDL é escrito em XML e cada arquivo WSDL é um documento XML.

Em uma interação de serviço web, o arquivo WSDL é produzido e publicado pelo lado do serviço e este arquivo é utilizado pelo lado do cliente para obter as informações necessárias sobre o serviço. Ambas as partes necessitam de uma cópia do arquivo WSDL para que a interação entre eles funcione de forma apropriada.

Os principais componentes definidos pelo arquivo WSDL são:

- Tipos (*Types*): um container para as definições dos tipos de dados.
- Mensagem (*Message*): uma definição dos dados sendo transmitidos.
- Operação (*Operation*): uma definição da operação para a mensagem suportada pelo serviço.
- Tipo de Porta (*Port Type*): um grupo de operações mapeadas para um ou vários pontos finais (*endpoints*).
- *Binding*: um protocolo e o formato dos dados associados a um tipo de porta específico.
- Porta: (*Port*): a definição de um ponto final definido como uma comunicação entre o *binding* e um endereço de rede.
- Serviço: uma coleção de portas relacionadas.

## UDDI

A especificação do UDDI (*Universal Description, Discovery and Integration*) [64] define a implementação de um registro para procurar por serviços web. Ele armazena arquivos WSDL que definem as interfaces dos serviços web. Este registro de serviços web se comunica através do protocolo SOAP e seu objetivo é o de funcionar como um serviço de procura de serviços. Serviços web são publicados neste diretório permitindo que potenciais clientes obtenham a localização, a descrição e a informação de *binding* do arquivo WSDL armazenado no registro.

### 3.6.3 Casos de sucesso utilizando a tecnologia de serviços web

A revolução dos serviços web ainda está em seus estágios iniciais. Uma grande quantidade de serviços já pode ser encontrada na web, contudo, sua maioria ainda é muito simples, como um serviço de cotação de valores de ações, ou um serviço de conversão de graus Célsius para Fahrenheit.

Entretanto, em antecipação ao rápido crescimento dos serviços web, algumas empresas estão desenvolvendo as partes da infraestrutura básica requerida para o desenvolvimento destes serviços, variando de tecnologias básicas com *parsers* XML [72], validadores de *Schema* XML [73], até serviços complexos como diretórios UDDI, etc. Empresas também têm construído servidores de aplicação que provêem uma plataforma unificada integrando UDDI, WSDL, e suporte a SOAP (por exemplo, IBM WebSphere [65]).

A Microsoft, em particular, tem investido muito no .NET [66], que é uma plataforma para construir serviços web distribuídos. O objetivo desta plataforma, assim como as de outros fabricantes, é que serviços padronizados mais básicos possam ser utilizados como componentes para a construção de aplicações maiores, facilitando o desenvolvimento.

## 3.7 Considerações finais

O desenvolvimento de aplicações de pagamentos móveis exige suportes que facilitem a programação de sistemas distribuídos com uma série de características (reusabilidade, transparências de distribuição, robustez, dentre outras). Apesar desses requisitos não serem novos, estes são exacerbados pelo tipo de aplicação que, conforme visto no

Capítulo 2, possuem usuários em potencial, mas que não desejam pagar mais pelo serviço, e que, além disso, precisam se assegurar que esse novo serviço possui requisitos de confiabilidade.

Este Capítulo apresentou algumas tecnologias habilitadoras dos serviços de pagamentos móveis, e descreveu algumas de suas mais importantes características. Uma análise crítica e uma comparação das duas principais tecnologias estudadas – serviços web e CORBA – é apresentada no Apêndice I.

## 4. Modelo proposto de *m-payment*

### 4.1 Introdução

Após um detalhado estudo dos diversos modelos, tecnologias e implementações existentes de pagamentos móveis notou-se que poucos estão sendo efetivamente utilizados em larga escala no mundo e muito menos no Brasil (algumas operadoras já estão vendendo conteúdo como toques de celular e outros conteúdos para serem utilizados nos aparelhos móveis no Brasil). Isso acontece por uma série de fatores e principalmente devido à mudança de cultura necessária da maior parte dos usuários de telefones móveis, uma vez que eles ainda não se sentem motivados em utilizar o pequeno teclado e visor dos aparelhos móveis para executar pagamentos, além da preocupação com a segurança.

O possível surgimento, dentro dos próximos anos, de algumas poucas soluções heterogêneas dispersas com procedimentos operacionais totalmente diferentes entre si (do ponto de vista dos usuários desses serviços), provavelmente só irá aumentar a desconfiança dos usuários. Uma forma de lidar com esse problema é a proposição de arquiteturas e modelos padronizados para lidar com pagamentos móveis, que já têm sido propostos pelos diversos fóruns, associações e alianças descritas previamente.

Tentando suavizar o impacto dessas novas possibilidades de pagamentos móveis na cultura dos usuários, principalmente os brasileiros, e com o objetivo de seduzi-los a começar a utilizá-los de forma gradual, propõe-se abaixo um modelo para um caso de pagamento móvel específico e de fácil utilização: a compra de créditos para telefones móveis pré-pagos. Este modelo pode servir de ponto de partida para introdução gradual de pagamentos móveis mais sofisticados que poderão servir para a aquisição de qualquer produto ou serviço e de qualquer valor.

Foi escolhido o pagamento móvel de créditos de telefones pré-pagos, pois esse já é um serviço de alta demanda. Atualmente esse serviço é efetuado nos diversos pontos de vendas das operadoras, principalmente através de cartões pré-pagos vendidos no comércio em geral.

## 4.2 Motivações para o modelo

Constatou-se que a solução atual de se utilizar cartões pré-pagos para adicionar créditos a telefones móveis é demasiadamente ineficiente e uma solução de pagamentos móveis representa uma significativa redução de custos para as operadoras, pois elimina a necessidade da produção, distribuição e armazenamento desses cartões pré-pagos. Os custos dessas etapas são exacerbados, considerando a necessidade de lidar com questões de segurança, pois esses cartões podem ser considerados um “novo” tipo de moeda.

Essa solução digital também acrescenta uma grande flexibilidade aos usuários como a de adicionar crédito a qualquer hora do dia e em qualquer lugar. Isso representa uma grande motivação para os usuários começarem a se interessar por esse tipo de serviço.

Uma outra grande vantagem dessa “carteira” pré-paga de créditos é a extensão da simples utilização dos créditos para conversação telefônica para a compra de outros produtos ou serviços (como pagamentos de contas, loteria, ingressos, pagamentos entre pessoas, estacionamento, etc). Portanto, a venda de créditos pré-pagos pode se estender para pagamentos móveis em geral de forma gradual e é uma maneira de incentivar o início da utilização dessa tecnologia por parte dos usuários.

## 4.3 Os atores e suas interações

A solução proposta de pagamentos móvel de créditos para telefones pré-pagos engloba a interação de quatro atores principais.

1. Usuário final (cliente ou comerciante) tipicamente buscando a aquisição ou a venda de créditos para telefones pré-pagos.
2. Provedor de serviços móveis que são as operadoras de telecomunicações buscando a substituição da solução antiga de cartões pré-pagos por uma solução totalmente digital.
3. Provedor de serviços de pagamentos gerenciando os detalhes de cada transação de pagamento. Esta tarefa pode ser exercida diretamente pela operadora de telecomunicações móveis ou terceirizada a uma empresa especializada.
4. Provedor de serviços financeiros provendo reconciliação e liquidação dos pagamentos (os bancos).

A existência desses quatro atores no modelo proposto está em conformidade com as principais arquiteturas de pagamentos móveis que foram apresentadas no Capítulo 2.

#### 4.4 Uma descrição do Sistema e seus pontos de integração

O diagrama da Figura 10 mostra como funciona a interação entre esses atores. Como pode ser visto na figura, existem três canais para se acessar a aplicação de pagamentos: através da plataforma SMS ou WAP da Operadora Móvel, através da Internet ou através de uma interface Web na Intranet do provedor de Pagamentos. Os canais SMS, WAP e Internet permitem clientes e comerciantes efetuarem recargas dos telefones móveis e o canal da Intranet permite o gerenciamento das contas dos usuários como a criação, atualização ou retirada de um cliente ou comerciante.

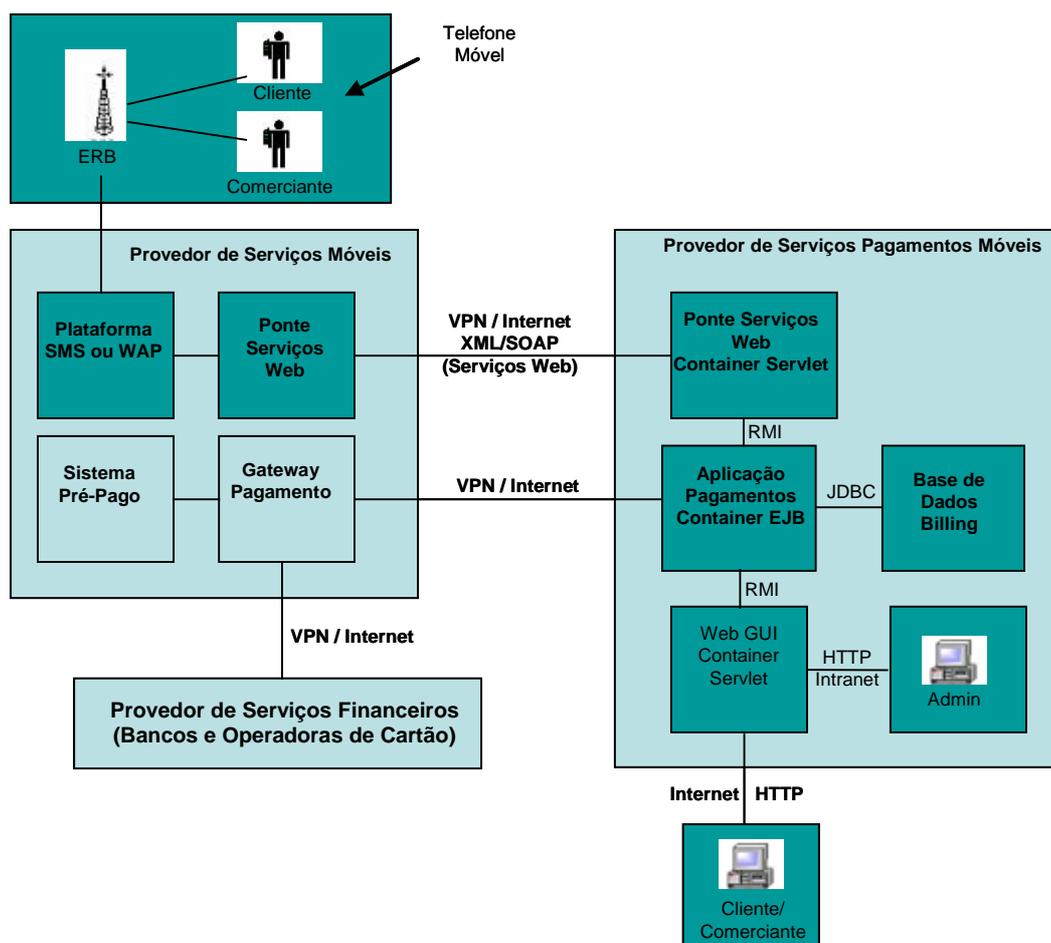


Figura 10. Modelo Proposto de pagamento móvel de Créditos Pré-Pagos.

Considerando que atualmente, a plataforma SMS e WAP, o sistema de pré-pago, a rede móvel e a conexão com bancos já estão em operação em todas as operadoras móveis brasileiras, esse novo ator, responsável pelo pagamento móvel, exige três pontos básicos de integração com esta plataforma já em utilização na operadora.

O primeiro é a integração entre plataforma SMS e/ou WAP e a Aplicação de Pagamentos, que se faz necessária para permitir que clientes e comerciantes acessem a aplicação de pagamentos através de mensagens SMS e/ou WAP.

O segundo ponto de integração é entre a plataforma de pagamentos e o *gateway* de pagamentos. Esse *gateway* já existe nas operadoras de telecomunicações atualmente e normalmente já utilizam protocolos específicos de telecomunicações. Essa integração tem dois objetivos:

1. Conectar a aplicação de pagamentos à plataforma de pré-pago para permitir que as contas dos celulares pré-pagos sejam creditadas após o pagamento; e, também,
2. a conexão com diversos bancos que já estão conectados à operadora, que permite o débito do valor dos créditos comprado na forma escolhida pelo usuário para o pagamento, como débito direto na conta do comprador, cartão de crédito ou cartão de débito.

Como pode ser visto no esquema da Figura 10, a integração entre a Aplicação de Pagamentos e a Plataforma SMS e/ou Plataforma WAP é feita utilizando serviços web com o protocolo SOAP e XML. A figura também representa algumas tecnologias usadas para interação entre componentes do sistema, tais como Java RMI, EJB, Servlet, JDBC, ou, simplesmente, através de HTTP. A argumentação para o uso dessas tecnologias será no Capítulo 5.

## **4.5 Os processos de compra de créditos**

Idealmente, devem existir dois tipos de operações de compra de crédito de telefones pré-pagos:

1. O próprio cliente compra seus créditos, e
2. Existe um ator comerciante intermediando o processo de compra.

Na solução em que o próprio cliente executa a compra, este pode recarregar suas contas pré-pagas através de mensagens SMS diretamente de seus telefones, ou através de um computador conectado à Internet. Isso requer que o cliente tenha registrado no Sistema de Pagamentos os seus detalhes de pagamento (como cartão de débito, cartão de crédito). Clientes não cadastrados podem fazer pagamentos através de um computador ligado a Internet inserindo seus dados de pagamento a cada momento em que decidir fazer a recarga.

Por outro lado, existem situações onde é necessário um comerciante para intermediar o processo de compra, pois a solução em que o próprio cliente executa a compra funciona apenas quando este tem alguma forma de pagamento já disponível (como cartão de débito ou cartão de crédito). Além disso, pode ser que o cliente queira realmente fazer sua recarga com dinheiro.

Essa figura de “comerciantes” já existe atualmente, no cenário de pagamento *vis-a-vis*. Como já descrito no Capítulo 2, são os intermediários que compram e vendem cartões pré-pagos o que, conforme já discutido, é uma solução ineficiente e custosa. (Além dessas vantagens, com a solução emergente de pagamentos móveis, novos serviços poderão ser agregados futuramente, além da simples compra de créditos.)

Na operação que envolve comerciante, este pode fazer a recarga de seus clientes utilizando o seu próprio telefone móvel ou através de um computador conectado à Internet. Assim, os comerciantes têm uma conta já com créditos incluídos e estes são transferidos desta conta do comerciante para a conta dos clientes quando o comerciante recebe o pagamento em dinheiro do cliente.

Um sistema que permite ambos os métodos de compra é normalmente o ideal para as operadoras de telefonia móvel.

#### **4.5.1 Pagamento efetuado somente pelo cliente**

Como descrito anteriormente, essa opção de pagamento onde o próprio cliente executa a compra (sem intermediários) pode ser feita diretamente de seus telefones móveis ou usando um computador conectado à Internet.

Os três canais que os clientes podem utilizar para efetuar a recarga de suas contas de telefone são:

- Através de mensagens SMS, em que os assinantes respondem a uma mensagem de alerta ou enviando simplesmente uma mensagem pré-formatada para iniciar a transação de compra de créditos.
- Através da Internet utilizando uma interface Wap.
- Através da Internet utilizando uma interface Web.

Para todos os canais acima, os detalhes de pagamento dos usuários são recuperados de suas carteiras eletrônicas (por exemplo, número do cartão de crédito) e o pagamento é processado pela aplicação de pagamentos móveis através do provedor apropriado para a rede do adquirente do pagamento. Quando o pagamento é processado pelo adquirente, uma resposta é repassada de volta para a carteira através do *gateway* de pagamento e uma resposta apropriada é passada para a aplicação. Então, a aplicação completa a ação que no caso é a recarga da conta pré-paga do assinante. Caso haja falha em qualquer ponto do processo, o sistema deve prover um histórico de toda a transação.

O número do telefone (MSISDN, *Mobile Station ISDN*) e uma senha (PIN, *Personal Identification Number*) são utilizados pela aplicação de pagamentos e o usuário é autenticado baseado nessas informações.

No diagrama da Figura 11, estão representadas as principais etapas da transação de recarga individual da conta pré-paga utilizando o canal de SMS. Estas etapas estão descritas a seguir:

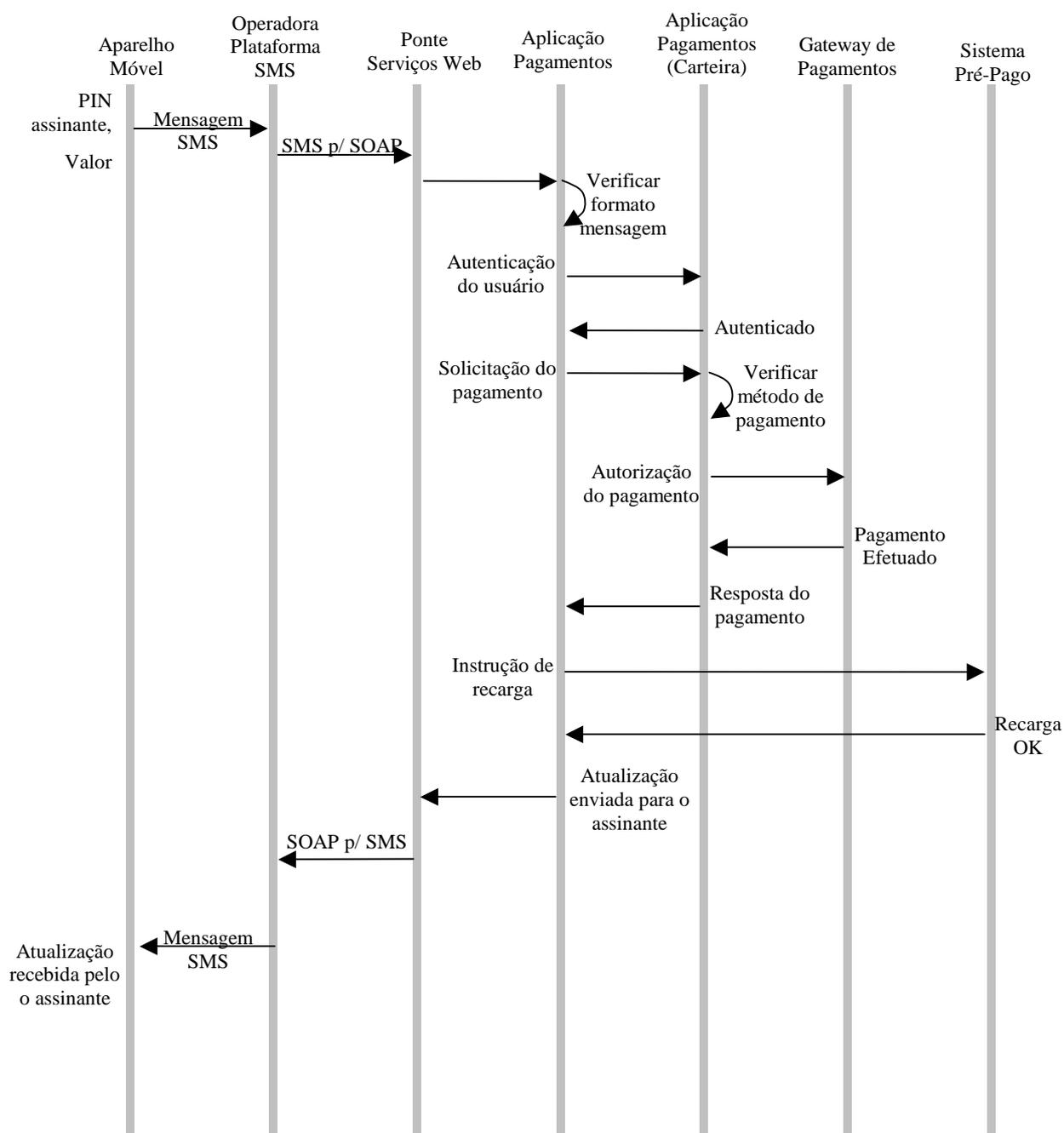


Figura 11. Cenário de pagamento móvel efetuado pelo próprio cliente.

O Usuário envia uma mensagem SMS pré-formatada para um número pré-estabelecido. Esta mensagem conterá uma palavra chave (para identificar a operação), o PIN (número de identificação pessoal do usuário) e o valor a ser carregado na conta do usuário. A Aplicação de Pagamento pode ser configurada para enviar uma mensagem

SMS para o usuário alertando-o do balanço de sua conta quando o valor estiver baixo. Nesse, caso o usuário simplesmente responderia a essa mensagem.

1. Essa mensagem SMS do usuário é convertida para o formato SOAP na Ponte de Serviços Web, que por sua vez é enviada para a Aplicação de Pagamentos.
2. A Aplicação de Pagamentos dá início ao pagamento e o crédito da sua conta pré-paga. Inicialmente, verifica-se se o formato da mensagem recebida é correto e depois se faz a autenticação do usuário com as informações contidas na mensagem. As informações dos usuários estão armazenadas na base de dados do sistema.
3. Após a autenticação, o método preferido de pagamento do usuário (débito em conta, cartão de crédito, cartão de débito, etc) é resgatado da base de dados.
4. Em seguida, a Aplicação de Pagamentos solicita o pagamento, que consiste de debitar do usuário do valor dos créditos a serem adicionados a sua conta, utilizando o método de pagamento preferido obtido anteriormente.
5. Através do *Gateway* de Pagamentos, o método de pagamento do usuário é acessado através da interconexão com os bancos e o pagamento efetuado. A Carteira Eletrônica do usuário recebe a informação de que o pagamento foi completado e repassa essa mensagem para a Aplicação de Pagamentos.
6. A Aplicação de Pagamentos, por sua vez, efetua a instrução de recarga onde a conta do usuário é efetivamente creditada.
7. Depois da recarga ter sido completada, uma confirmação do término da operação é enviada para a Ponte de Serviços Web no formato SOAP. Esta é convertida para o formato SMS e o recibo é enviado para o telefone móvel do usuário.

A Figura 11 e sua descrição consideram que a tecnologia SMS foi utilizada, entretanto poderia ser utilizada também a tecnologia WAP de forma análoga ao que foi ilustrado acima, mudando apenas o canal de transmissão.

O Sistema também deve ser capaz de enviar avisos de que a conta do usuário está quase sem saldos, ou de receber solicitações dos usuários sobre o valor ainda disponível em suas Carteiras Eletrônicas.

#### **4.5.2 Pagamento efetuado com a ajuda de um comerciante**

Quando o usuário não possui um método de pagamento preferido (como débito em conta do banco, cartão de crédito, cartão de débito) e/ou quer efetuar sua recarga em dinheiro, existe a necessidade de um comerciante ajudar no processo.

Assim, esse modelo também prevê essa opção de pagamento. Nesse caso, os comerciantes, que hoje já atuam vendendo cartões pré-pagos, poderão efetuar a recarga utilizando seu próprio telefone móvel como ponto de venda (POS – *Point of Sale*). Estes comerciantes possuem contas pré-pagas com valor já creditado e que poderá ser repassado para seus clientes, em troca de pagamento em dinheiro diretamente para o comerciante.

Nesse caso também existem três canais possíveis de acesso ao sistema:

- Através de mensagens SMS, onde os comerciantes podem enviar uma mensagem pré-formatada de seus telefones móveis para iniciar o processo de recarga do telefone de seus clientes.
- Através da Internet utilizando uma interface Wap.
- Através da Internet utilizando uma interface Web. Nesse caso o comerciante pode, ao receber o dinheiro do cliente, efetuar diretamente a recarga através da Internet ou imprimir um número, que pode ser utilizado pelo cliente para recarregar da mesma maneira como são utilizados os cartões pré-pagos atualmente.

Da mesma forma que no caso anterior, o número do telefone e uma senha do comerciante são utilizados pela aplicação de pagamentos e o comerciante é autenticado baseado nessas informações.

No diagrama da Figura 12, estão representadas as principais etapas da transação de recarga através de um comerciante da conta pré-paga do seu cliente utilizando o canal de SMS.

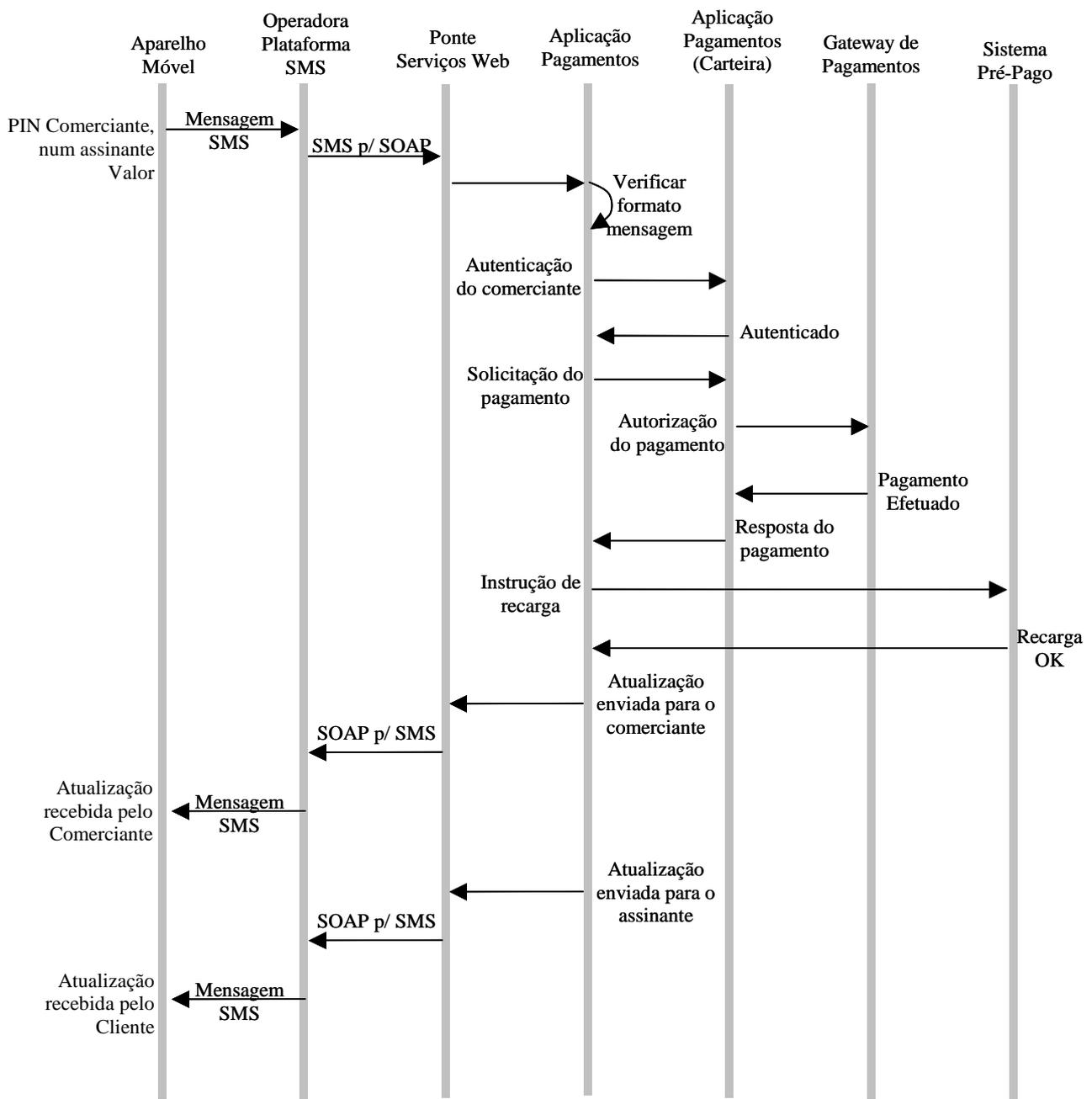


Figura 12. Cenário de pagamento móvel efetuado através de um comerciante.

No cenário do pagamento móvel efetuado através de um comerciante, existem poucas diferenças com relação ao descrito anteriormente. Existe a necessidade de se enviar a informação do número do cliente para onde se deve transferir os créditos previamente armazenados na carteira eletrônica do comerciante. Além disso, existe a necessidade de se mandar uma confirmação da conclusão da operação, tanto para o

comerciante como para o cliente. O sistema ainda deve checar se a carteira do comerciante possui créditos suficientes para transferir para o cliente e se isso não ocorrer uma nova recarga da conta do comerciante deve ser feita. Pode-se definir uma forma padrão de pagamento por parte do comerciante como débito em conta corrente, e com valores mínimos por operação maiores que aos comparados a recarga feita pelo cliente independentemente.

Neste caso também existe a necessidade de se definir previamente uma comissão a ser paga para o comerciante pelo o serviço de venda executado por ele. Propõe-se neste modelo que o comerciante pague um valor com desconto na compra de créditos. Esse desconto pode ser baseado no valor total da recarga escolhida pelo comerciante. Desta forma, qualquer usuário poderia se tornar um revendedor, oferecendo uma nova oportunidade de renda para milhares de pessoas, conforme descrito posteriormente em mais detalhes nesta dissertação.

## **4.6 Outros trabalhos relacionados**

### **4.6.1 A proposta de McKitterick [53]**

Foram encontrados na literatura alguns poucos trabalhos relacionados com o caso específico de pagamentos móveis utilizando-se a tecnologia de *web services*. No trabalho de McKitterick [53], é proposto um modelo genérico de pagamentos móveis enfatizando a utilizando a tecnologia de serviços web como principal tecnologia de *middleware* do modelo. No modelo de McKitterick, os usuários podem fazer qualquer tipo de aquisição de serviço ou mercadoria através de três métodos diferentes de pagamentos: cobrança através de conta com a operadora móvel, cobrança com cartão de crédito e também pagamento através de SMS reverso [54]. Este trabalho demonstra a facilidade de se utilizar uma interface de WSDL para que vários clientes (diferentes formas de pagamentos), que é um ponto em comum com o modelo proposto nesta dissertação. Esta proposta embora mais genérica do que a proposta por essa dissertação é um passo além do que as operadoras de telefonia móvel brasileira ou empresas independentes de pagamentos estariam preparadas para oferecer, tendo em vista a resistência que os usuários podem ter em efetuar qualquer tipo de pagamento através desse novo canal. Nesta dissertação se propõe um modelo que seria muito mais

facilmente aceito pelos usuários e com potencial de ser utilizado em larga escala rapidamente.

#### **4.6.2 O estudo de Marques [55]**

O trabalho de Marques faz um estudo detalhado de qual o *status* dos pagamentos móveis na Europa, e principalmente em Portugal, dando ênfase aos modelos de pagamentos móveis já implementados no mercado e focando na principal dificuldade enfrentada por estas implementações, que segundo ele é a questão da segurança. Trata-se de um trabalho que embora não faça um estudo mais detalhado das tecnologias envolvidas nas soluções, principalmente pela falta de informação disponível devido a confidencialidade das empresas, descreve as principais vulnerabilidades destes sistemas principalmente na plataforma sem fio. Trata-se de um trabalho complementar ao proposto nessa dissertação, tendo em vista que este não enfatizou o lado da segurança. Poder-se-ia considerar como um trabalho futuro estas vulnerabilidades que hoje existem e tentar evitá-las através de melhoramentos ao modelo proposto neste capítulo.

#### **4.6.3 O estudo de Martins, Rocha e Henriques [56]**

Já no trabalho de Martins, Rocha e Henriques, é feita uma análise também de segurança nos pagamentos móveis, entretanto levando em consideração os benefícios de novos protocolos de segurança que estão sendo definidos para compor a pilha dos Serviços Web (como XML *Signature* [57], XKMS [58], SAML [59]) e como eles podem ser utilizados para facilitar a adaptação do comércio eletrônico ao ambiente móvel. São listados alguns padrões recentemente estabelecidos, mas que ainda são muito pouco utilizados na prática. O trabalho desta dissertação procurou buscar uma solução que pudesse ser implementada sem grandes transtornos com as atuais tecnologias disponíveis no mercado. O uso destas tecnologias novas do protocolo de serviços web pode ser uma proposta de estudo para um trabalho posterior.

#### **4.6.4 O trabalho de Pousttchi [60]**

Um trabalho semelhante ao apresentado neste capítulo é a proposta de um cliente que utiliza uma conexão WAP e um *servlet* intermediário para acessar a plataforma proposta pela PayCircle. Este trabalho propõe a utilização da plataforma de pagamentos por comerciantes (representado pelo *servlet*) para efetuar pagamentos para autorizar

utilização de um jogo de ação no telefone móvel. Este trabalho propõe também um uso específico de utilização de pagamento para aquisição de um produto em específico, o que pode também ser visto como um modelo intermediário de fácil adoção na perspectiva dos usuários que pode em uma fase posterior ser expandido para um caso de pagamentos genérico.

## **4.7 Considerações finais**

Este Capítulo apresentou uma proposta de modelo de pagamentos móveis para compra de créditos móveis. O modelo foi composto baseado em arquiteturas e outros modelos definidos por Consórcios e trabalhos acadêmicos, conforme apresentado no Capítulo 2.

O modelo apresenta peculiaridades devido à aplicação alvo, e à realidade brasileira (que já possui esquemas consolidados de venda de créditos na forma não automatizada).

O modelo foi implementado parcialmente, através de um protótipo buscando verificar algumas de suas propriedades. Nessa etapa de implementação, alguns componentes do modelo foram revistos, assim como ferramentas utilizadas.

No próximo Capítulo são apresentados detalhes de implementação, experiências adquiridas, e algumas conclusões resultantes dessa atividade.

## 5. Implementação e avaliação do modelo

Este Capítulo apresenta os detalhes da implementação do sistema de pagamentos de créditos de telefones pré-pagos. Este protótipo é uma simplificação do modelo proposto no capítulo anterior e demonstra a utilização das diversas tecnologias descritas anteriormente de forma conjunta. Algumas partes do modelo não foram implementadas devido à necessidade de uma infra-estrutura não existente no laboratório como a conexão com a plataforma de pré-pago da operadora móvel ou a conexão com os bancos, também feita através da operadora móvel. Outras partes do sistema foram simuladas, como a infra-estrutura de telefonia e o próprio aparelho de telefone móvel, como descrito abaixo.

### 5.1 Descrição geral da implementação

Nesta implementação, ao invés de se seguir o caso descrito no Capítulo 4 (utilizando a tecnologia de mensagens SMS, e uma plataforma SMS fazendo conexão entre a mensagem SMS e a ponte de Serviços Web), utilizou-se uma conexão direta HTTP via WAP, entre um *midlet* [30] Java (aplicação que obedece ao padrão MIDP que faz parte do J2ME, como descrito no capítulo 3) em um simulador de telefone móvel e essa ponte de Serviços Web.

Existem vantagens e desvantagens em utilizar uma ou outra tecnologia e muito provavelmente a tecnologia preferida em casos reais de utilização será um misto das duas tecnologias, conforme descrito no capítulo 3. No caso dessa implementação, o WAP foi escolhido simplesmente pela maior facilidade de sua implementação, entretanto levando em conta a atual conjuntura da base de dispositivos em uso no Brasil, a opção de se utilizar a tecnologia SMS é a melhor, devido a maior penetração de telefones móveis que suportam esta tecnologia (quando comparado ao WAP).

Para efeito de demonstração da tecnologia, essa mudança é completamente transparente para o restante do sistema, sendo restrita apenas ao simulador de telefone móvel. Não existe a necessidade de se alterar outras partes do sistema em virtude disso, como o *gateway* de Serviços Web, provando a eficácia dessa tecnologia.

A implementação utilizou a especificação e implementação de referência de pagamentos móveis fornecida pela PayCircle [17] para a funcionalidade do Servidor de Pagamentos. Foi utilizada uma série de ferramentas ao se desenvolver esse protótipo. Essas ferramentas serão listadas e descritas abaixo.

O protótipo implementa a primeira proposta apresentada no modelo para recarga do telefone móvel, em que o próprio cliente faz a compra dos créditos a serem utilizados no seu telefone, sem a presença de um comerciante no processo.

O protótipo é constituído de dois servidores e um simulador de telefone móvel conforme ilustrado na Figura 13:

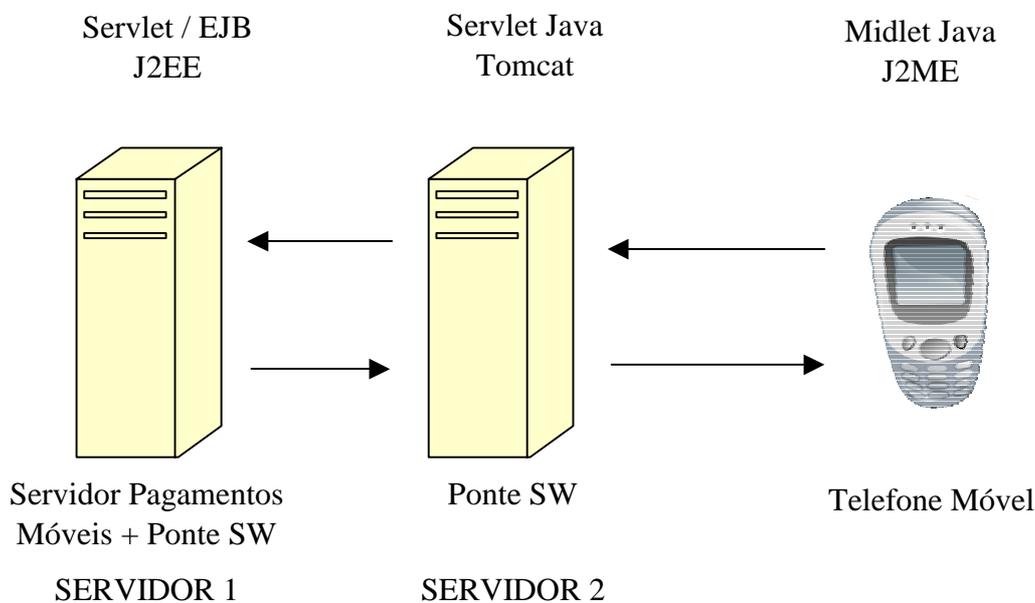


Figura 13. Componentes da implementação do protótipo.

### 5.1.1 Servidor 1

No Servidor 1, foi instalado o Servidor de Pagamentos juntamente com uma das pontas (*endpoints*) da ponte de Web Services. Neste computador foi necessária a instalação das seguintes ferramentas pré-requisitos para o funcionamento do protótipo:

- Sistema Operacional Windows 2000.

- Apache Ant [24]: ferramenta de construção (*builder tool*) para Java para facilitar o desenvolvimento.
- Apache Xerces [25]: *parser* XML para Java, utilizado pela Apache Axis.
- Apache Axis [26]: implementação do protocolo SOAP (*Simple Object Access Protocol* [23]), baseado na especificação do W3C e utilizado pela ponte de Serviços Web.
- J2SE [27]: Java 2 Standard Edition, implementação de referência da SUN que contém a máquina virtual, compilador Java e bibliotecas, utilizados pela ponte de Serviços Web e pelo Servidor de Pagamentos.
- J2EE [28] Java 2 Enterprise Edition, implementação de referência da SUN que contém entre outras ferramentas o Servidor de Aplicações J2EE, utilizado pela ponte de Serviços Web e pelo Servidor de Pagamentos. Essa implementação já inclui a base de dados Cloudspace que é automaticamente configurada durante a instalação para ser utilizada junto com o servidor de aplicações J2EE e também foi utilizada no protótipo.

### 5.1.2 Servidor 2

No Servidor 2, foi instalada a outra ponta da ponte de Serviços Web. Este servidor é responsável pelo recebimento das mensagens enviadas pelo telefone móvel, a tradução para o formato de Serviços Web e o envio para o Servidor de Pagamentos. Também é responsável por receber a mensagem do Servidor Web e enviá-la no formato apropriado para o telefone móvel.

Neste Servidor foram necessárias as seguintes ferramentas: J2SE [27], Apache Tomcat [29] (*container* de Servlets), Apache Xerces [25] e Apache Axis [26], todos utilizados pela ponte de Serviços Web.

### 5.1.3 Telefone Móvel

No simulador de telefone móvel, foi instalada uma aplicação responsável por fazer o pedido de pagamento pela recarga do celular e de recebimento de uma confirmação desse pagamento. Esta aplicação foi implementada como um *midlet* Java [30].

Neste computador foi instalada a plataforma J2ME WTK [30], que é um *toolkit* que contém um emulador de dispositivos sem fio MIDP [52].

Na seção a seguir são descritos detalhes de cada uma das partes do protótipo.

## 5.2 Servidor de Pagamentos

O Servidor de Pagamentos, baseado na proposta da PayCircle [17], foi desenvolvido de acordo com o modelo J2EE [28] e foi implementado como uma coleção de EJB's, Enterprise Java Beans [22] e componentes web.

Já a ponte (*front end*) de serviços web foi implementada como um conjunto de *servlets* Java. Essa ponte de serviços web acessa as funcionalidades oferecidas do Servidor de Pagamentos através de uma interface interna. Na Figura 14 estão ilustrados maiores detalhes sobre a arquitetura deste Servidor de Pagamentos.

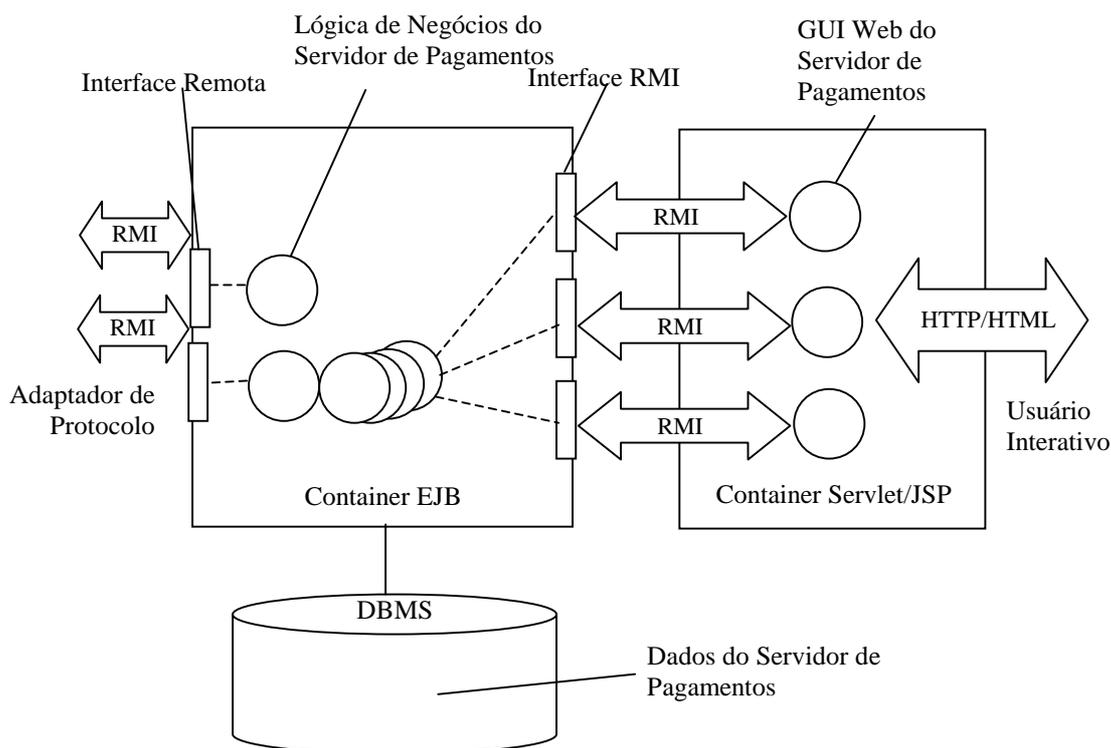


Figura 14. Servidor de Pagamentos baseado na especificação da PayCircle [17].

Os EJBs do Servidor de Pagamentos implementam a lógica de negócios que executa o serviço de pagamentos. Os EJBs são executados em um ambiente chamado Container de EJB, que executam tarefas como persistência, manuseio de transações,

gerenciamento de *threads*. Os EJBs armazenam os dados persistentes em uma base de dados, acesso que é provisionado pelo Container EJB. Portanto, a utilização de um container de EJB mostrou-se eficaz para o serviço de pagamentos, adicionando uma série de funções que oferecem maior robustez e confiança ao sistema.

A interface remota do Servidor de Pagamentos implementa a API de *Front Side*. Ela provê adaptadores de protocolos como a Ponte de serviços web, que acessa a funcionalidade do servidor de pagamentos. Através do adaptador de protocolos apropriado, aplicações podem acessar o servidor de pagamentos. Este acesso está sendo através de uma aplicação cliente no formato *servlet*, como explicado anteriormente.

Os componentes Web do Servidor de Pagamentos implementam uma interface web que permite gerenciar o servidor de pagamentos. Estes componentes fazem uso de interfaces internas com os EJBs para acessar os dados persistentes do servidor de pagamentos, como por exemplo, informações sobre os usuários do sistema e sobre suas contas. Os componentes web são implementados em um outro ambiente, chamado de container de Servlets ou de JSPs. Operadores ou usuários podem acessar o Servidor de Pagamentos através de uma interface web e, através dela, eles podem executar tarefas interativamente como, por exemplo, procurar pelos créditos nas suas contas ou adicionar ou remover usuários da base de dados.

### **5.3 Front End de serviços web**

A ponte de serviços web permite a outras aplicações acessarem o Servidor de Pagamentos utilizando a tecnologia de serviços web e foi implementada como uma coleção de Servlets Java. Como os componentes web do Servidor de Pagamentos, os Servlets Java executam em um container Servlet/JSP.

Os Servlets se comunicam com outras aplicações que precisam acessar o Servidor de Pagamentos através de mensagens HTTP que transportam mensagens SOAP. O protocolo HTTP é implementado pelo container; os Servlets decodificam os cabeçalhos das mensagens HTTP, que são esperados no formato SOAP/XML e destinam as solicitações recebidas da aplicação que originou as mensagens para os EJBs apropriados do servidor de pagamentos através da interface remota, como explicado anteriormente

Segue abaixo uma ilustração de como é implementada essa ponta da ponte de serviços web.

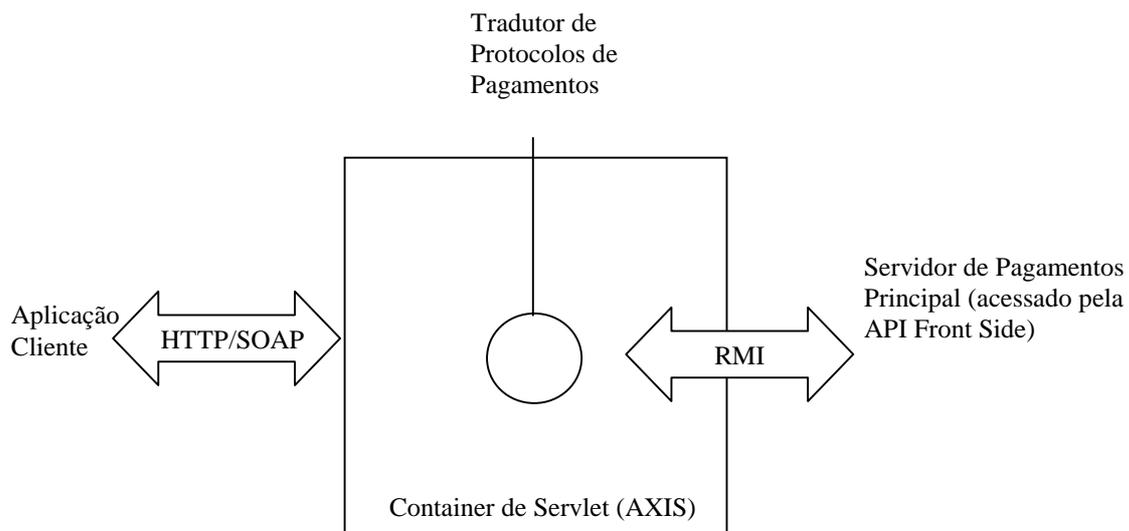


Figura 15. Ponte de Serviços Web baseado na especificação da PayCircle [17]

Para se acessar essa ponta (*endpoint*) da Ponte de Serviços Web através de uma aplicação cliente, em um ambiente real de *web services*, haveria a necessidade de se fazer a descoberta desse serviço através de uma pesquisa em um serviço de diretório apropriado, como o UDDI. Isso não foi realizado na implementação e, portanto, o serviço está sendo chamado diretamente no código da implementação sem a necessidade de uma descoberta desse serviço.

O serviço pode ser acessado através do seguinte endereço:

`http://servidor1:8000/PayCircleWS/services/AmmountChargingPort`

Esse endereço acessa, na verdade, um dos serviços definidos pela especificação da PayCircle, que é o suficiente para a implementação desse protótipo. Esse serviço simplesmente faz a cobrança do cliente dos créditos a serem adicionados na sua conta pré-paga.

## 5.4 Fluxo de mensagens entre os atores

Esta seção tem o objetivo de ilustrar um exemplo de como ocorre a troca de mensagens entre o simulador de telefone móvel, a ponte de serviços web e a aplicação de pagamentos móveis. Essa interação ocorre em quatro etapas:

1. Através de uma interface WAP, o simulador de telefone móvel solicita ao usuário as informações de login e senha no sistema e envia essas informações, utilizando uma simples mensagem HTTP, para a ponte de *web services* instalada no servidor 2. Foi utilizado o método GET deste protocolo.

```
GET /ponteWs/PonteWsServlet?u=99115974&p=pagar http/1.1
Content-Length:0
```

2. Essa mensagem é recebida pelo servlet do servidor 2, a ponte de *web services*, que funciona como um tradutor dessa mensagem HTTP, recebida para o formato SOAP, conforme exemplificado na Listagem 1.

```
POST /PayCircleWS/services/AmountChargingPort HTTP/1.0
Content-Type: text/xml; charset=utf-8
Accept: application/soap+xml, application/dime, multipart/related, text/*
User-Agent: Axis/1.1
Host: localhost
Cache-Control: no-cache
Pragma: no-cache
SOAPAction: "AmountCharging#chargeAmount"
Content-Length: 522
Authorization: Basic Y2hyaXN0b3BoZXI6cGF5
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <soapenv:Body>
    <chargeAmount xmlns="">
      <endUserIdentifier>
        <value>sip:99111234@test.com</value>
      </endUserIdentifier>
      <amount>40</amount>
      <billingText>ChargeAmount:Recarga créditos pré-pagos</billingText>
      <referenceCode>11111</referenceCode>
    </chargeAmount>
  </soapenv:Body>
</soapenv:Envelope>
```

Listagem 1: Ponte de Serviços Web.

Nesse caso será cobrado do usuário 99111234 o valor de R\$40 em troca da recarga de sua conta pré-paga no Sistema Pré-Pago da operadora de telefonia móvel.

Pode-se observar que nesta implementação a mensagem SOAP não transporta a senha do usuário. Isso ocorre pois a autorização do débito é feita durante o estabelecimento da sessão de acesso ao Servidor de Pagamentos como exemplificado no código da Listagem 2.

```
URL acessoUrl = new URL("http://" + servidor1 +
":8000/PayCircleWS/services/AmountChargingPort");
ps = new AmountChargingBindingStub(acessoUrl, new Service());
ps.setPassword(password);
ps.setUsername(user);
// estabelece uma sessão que mantém o seu estado automaticamente
ps.setMaintainSession(true);
```

Listagem 2: Sessão de acesso ao Servidor de Pagamentos.

3. Após o Servidor de Pagamentos efetuar o débito do cliente, ele envia para o *Servlet* uma resposta no formato SOAP informando resultado da operação (se houve sucesso ou não). A Listagem 3 mostra essa resposta SOAP.

```
HTTP/1.1 200 OK
Content-Type: text/xml; charset=utf-8
Connection: close
Date: Thu, 10 Feb 2005 15:36:51 GMT
Server: J2EE SDK/1.3.1 (HTTP/1.1 Connector)
Set-Cookie:
JSESSIONID=C22B7CEDFA9657B07F2468BD7AE8A5D6;Path=/PayCircleWS

<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <soapenv:Body>
    <chargeAmountResponse xmlns=""/>
  </soapenv:Body>
</soapenv:Envelope>
```

Listagem 3: Resposta SOAP sobre o resultado da operação.

4. O Servlet então envia uma confirmação para o simulador de telefone móvel no formato HTTP (Listagem 4).

```
HTTP/1.1 200 OK
Content-Type text/plain
Content-Length: 15
Server: Apache Coyote/1.1

Recarga Aceita!
```

Listagem 4: Confirmação em HTTP para o simulador de telefone móvel.

As classes que acessam o serviço `ChargeAmount` do Servidor de Pagamentos são gerados a partir de um arquivo WSDL padrão. Neste trabalho está se adotando por motivo de padronização, o arquivo WSDL especificado pela PayCircle, cujo código é mostrado na listagem 5.

```

<?xml version='1.0' encoding='UTF-8'?>
<!-- March 17, 2003 -->
<wsdl:definitions
  name='payment_service'
  targetNamespace='http://www.csapi.org/wsdl/parlayx/payment/v1_0/service'
  xmlns='http://schemas.xmlsoap.org/wsdl/'
  xmlns:wsdl='http://schemas.xmlsoap.org/wsdl/'
  xmlns:soap='http://schemas.xmlsoap.org/wsdl/soap/'
  xmlns:xsd='http://www.w3.org/2001/XMLSchema'
  xmlns:tns='http://www.csapi.org/wsdl/parlayx/payment/v1_0/service'
  xmlns:port='http://www.csapi.org/wsdl/parlayx/payment/v1_0/service_port'>

  <wsdl:import namespace='http://www.csapi.org/wsdl/parlayx/payment/v1_0/service_port'
  location='parlayx_payment_service_port.wsdl'/>

  <wsdl:binding name='AmountChargingBinding' type='port:AmountChargingPort'>
    <soap:binding style='rpc' transport='http://schemas.xmlsoap.org/soap/http'/>

    <wsdl:operation name='chargeAmount'>
      <soap:operation soapAction='AmountCharging#chargeAmount' style='rpc'/>
      <wsdl:input>
        <soap:body use='literal'/>
      </wsdl:input>
      <wsdl:output>
        <soap:body use='literal'/>
      </wsdl:output>
      <wsdl:fault name='UnknownEndUserException'>
        <soap:fault use='literal'/>
      </wsdl:fault>
      <wsdl:fault name='InvalidArgumentException'>
        <soap:fault use='literal'/>
      </wsdl:fault>
      <wsdl:fault name='ChargeFailureException'>
        <soap:fault use='literal'/>
      </wsdl:fault>
    </wsdl:operation>

    <wsdl:operation name='refundAmount'>
      <soap:operation soapAction='AmountCharging#refundAmount' style='rpc'/>
      <wsdl:input>
        <soap:body use='literal'/>
      </wsdl:input>
      <wsdl:output>
        <soap:body use='literal'/>
      </wsdl:output>
    </wsdl:operation>
  </wsdl:binding>
</wsdl:definitions>

```

Listagem 5: Arquivo WSDL do Serviço de Pagamentos Móveis.

## 5.5 Considerações sobre a implementação

O desenvolvimento do protótipo apresentado nesta seção permitiu a utilização de forma integrada de diversas tecnologias e possibilitou o entendimento geral das qualidades de cada uma e onde podem ser utilizadas de forma mais apropriada.

Para ilustrar a afirmação acima pode-se citar as diversas tecnologias utilizadas e as razões pelas quais elas foram escolhidas para cada parte do protótipo:

- A tecnologia de EJBs (*Enterprise Java Beans*) é a mais apropriada quando se trata de lidar com a lógica de negócio do sistema e, portanto, é a mais indicada para exercer o papel do servidor de pagamentos. A utilização dessa tecnologia permite ao servidor oferecer uma maior robustez e confiança ao sistema principalmente por causa da possibilidade de se utilizar serviços já embutidos nessa tecnologia como segurança (pode-se definir regras de acesso aos componentes permitindo níveis diferentes de acesso para cada tipo de cliente), persistência de dados (por meio do mapeamento das propriedades dos seus componentes com as tabelas do seu banco de dados, o container gerencia o acesso e as modificações, garantindo integridade e consistência a base de dados), transações (o *container* gerencia todas transações e se encarrega de garantir a consistência), escalabilidade (múltiplos *containers* em servidores físicos separados podem ser iniciados – *clustering* - garantindo a persistência de sessões de usuários, transações e balanceamento de carga de forma automática).
- Já a tecnologia de RMI é apropriada para conexões fortemente acopladas e normalmente são ideais para conexões entre partes do sistema contidas em uma mesma corporação. Além disso, no caso dessa implementação foi usada apenas a linguagem Java. Considerou-se, inicialmente, o uso da tecnologia Corba, que também uma tecnologia considerada fortemente acoplada. No entanto, como a linguagem Java foi utilizada em todo o sistema e o uso de RMI foi o suficiente para o caso deste protótipo. Além disso a implementação de referência da PayCircle já usava tanto o RMI como EJB como tecnologias de implementação.

- Já a tecnologia de serviços web é mais apropriada em ambientes onde ocorra o acoplamento fraco. Esse normalmente é o caso onde haja necessidade de se integrar sistemas de corporações diferentes, que é o cenário mais provável para conexão entre o servidor de pagamentos e a conexão com o ambiente sem fio. Portanto, os protocolos SOAP e WSDL permitiram a preparação deste protótipo para uma expansão simples para um modelo mais genérico e também permitiu a padronização do acesso e uma maior facilidade de se implementar clientes para acessar o servidor de pagamentos.
- As tecnologias SMS e WAP foram escolhidas pois já são tecnologias consagradas no mercado e presentes na maior parte dos aparelhos móveis disponíveis hoje. Essas tecnologias sozinhas, entretanto, não oferecem a segurança necessária para a implementação de um sistema de pagamento real. Embora o foco desta dissertação não tenha sido a questão de segurança, foi mencionado no Capítulo 3 que existem tecnologias de segurança que podem ser utilizadas em conjunto com SMS e WAP e devem ser consideradas para serem incluídas neste protótipo em um trabalho futuro.

## 5.6 Considerações finais

Este Capítulo apresentou em detalhes o protótipo que foi implementado tendo como base o modelo proposto no Capítulo 4, considerando as tecnologias (protocolo, *middlewares*, etc) disponíveis no cenário atual. Trata-se de um protótipo onde partes do modelo foram simuladas (como a rede de telefonia sem fio) e outras não foram implementadas devido à ausência de tais partes do modelo no laboratório (como a conexão com a plataforma pré-paga ou a conexão com os bancos).

O protótipo, no entanto, possibilitou a utilização de diversas tecnologias distintas empregadas em setores diferentes (como as tecnologias sem fio e as tecnologias de *middleware*) de forma integrada servindo como um bom exemplo da complexidade do sistema e como cada tecnologia pode ser utilizada em sua forma mais adequada e útil tendo-se como base as qualidades e restrições de cada uma para o funcionamento de cada parte do sistema.

## 6. Conclusões

### 6.1 Revisão das motivações e objetivos

O comércio eletrônico, mais especificamente o comércio móvel, está se tornando uma realidade, devido, principalmente, ao surgimento e a consolidação de novas tecnologias. Vários exemplos podem ser citados: redes sem fio, tais como GPRS, EDGE, UMTS; protocolos de segurança, tais como, SET e WTLS; serviços diversos para tecnologias de comunicação, tais como, SMS, WAP, Toolkit SIM, I-Mode, etc. O surgimento de novos serviços voltados para mobilidade (*m-services* ou serviços móveis) é propiciado por essas novas tecnologias. Um dos mais importantes serviços de apoio para o desenvolvimento do comércio móvel (*m-commerce*) em geral é o de pagamentos móveis, ou *m-payment*.

Em países onde se começa a introduzir esses serviços (ainda de forma proprietária) os usuários, na maior parte das vezes, estão relutantes em aderir às ofertas já disponíveis no mercado. Uma das questões relacionadas é a da falta de confiança nestas soluções oferecidas. Por isso, a proposição de modelos padronizados e adequados torna-se um importante tema para adoção desses serviços em larga escala.

Neste sentido, nos últimos 5 anos, estão surgindo consórcios para padronizar todo o processo de comércio móvel, e principalmente o serviço de pagamentos móveis. Muitos desses consórcios já começam a se unir ou estabelecer trabalhos conjuntos tentando chegar a uma proposição ideal para superar esses novos desafios. Ainda não existe, entretanto, um consenso nem por parte das empresas e nem por parte da Academia sobre o melhor modelo e tecnologias a serem adotadas.

A realidade brasileira não é muito diferente que a de outros países. A maior parte das empresas de telecomunicações móveis está interessada em iniciar serviços em que possam utilizar a sua rede para a compra e venda de mercadorias e serviços. No Brasil, isso começa a surgir na forma de soluções proprietárias, como hoje ocorre, por exemplo, ao se comprar um toque de celular ou um ingresso de cinema através da rede de telefonia sem fio. Essas soluções, entretanto, ainda são muito pouco utilizadas.

Este quadro é agravado ainda mais devido à escassez de trabalhos acadêmicos relevantes com esse objetivo de padronização no Brasil.

## 6.2 Visão geral do trabalho

Esta dissertação teve como objetivo pesquisar a área de pagamentos móveis. Foram analisadas as principais diferenças entre o pagamento móvel e o pagamento atualmente efetuado no comércio eletrônico convencional através da Internet. Foram estudadas as diversas propostas de modelos e padronizações existentes e as tecnologias principais que possibilitarão o desenvolvimento do comércio móvel em larga escala.

Foram também estudados os principais desafios que serão enfrentados pelas empresas para que os pagamentos móveis sejam adotados em larga escala e também as diversas formas de como estes serviços podem ser configurados, dependendo principalmente de qual tipo de empresa exerce os papéis de cada um dos atores envolvidos.

Além disso, este trabalho propôs um modelo de pagamentos móveis para créditos de telefones pré-pagos baseado nos resultados da pesquisa realizada e implementa um protótipo deste modelo.

No momento desta publicação, existem diversas soluções proprietárias para pagamentos móveis e algumas propostas de padronização com um conjunto de bibliotecas e implementações de referência. Uma destas bibliotecas e implementações de referência foi adotada durante a implementação do protótipo.

## 6.3 Contribuição e escopo do trabalho

Uma das contribuições deste trabalho foi a proposição de um modelo e desenvolvimento de um protótipo, baseados em especificações abertas, as quais estão sendo trabalhadas por consórcios de empresas e universidades para serem padronizadas.

Essa área de *m-payments* ainda é muito recente. Todos os trabalhos na área foram desenvolvidos nos últimos 5 anos. Este trabalho pretende incentivar e propiciar uma base para uma série de outros trabalhos no Brasil e, em específico, na UFSC.

O modelo proposto, além de baseado em outros modelos abertos também foi adaptado à realidade brasileira, na qual poucos usuários têm recursos sofisticados em seus telefones móveis e ainda não estão motivados a utilizar as poucas ofertas de *m-payments* no mercado brasileiro. Neste sentido escolheu-se um produto já de alta demanda que são os próprios créditos pré-pagos de conversação. Isso permite que o

usuário faça compra de algo realmente necessário para ele e pode representar um primeiro passo para a uma crescente e gradual utilização da tecnologia móvel para efetuar pagamentos.

Para avaliar este modelo proposto, foi construído um protótipo onde se procurou simular todo o ambiente sem fio das operadoras e as diversas interações entre os atores envolvidos no pagamento móvel. Além disso, foram estudadas diversas tecnologias que podem ser adotadas na construção de um sistema real e mais genérico. O protocolo UDDI da pilha de protocolos dos Serviços Web poderia ter sido utilizado para fazer uma descoberta automática do serviço de pagamento móvel, permitindo, por exemplo, que qualquer cliente pudesse utilizar esse serviço, o que pode ser interessante para o futuro em um modelo mais genérico. Tecnologias de Segurança, como WTLS ou o WIM, que garantiriam a segurança do protótipo também não foram incluídas neste modelo simplificado. Estas tecnologias não foram incluídas devido à atual base instalada de telefones no Brasil em que a grande maioria dos telefones móveis não suporta tais tecnologias. No entanto, a inclusão de segurança é essencial, a médio prazo, para o sucesso deste modelo.

Um estudo de desempenho do protótipo não foi realizado, uma vez que os dados coletados não seriam relevantes para qualquer tipo de conclusão mais específica. Isso ocorreu porque uma boa parte do protótipo simulou componentes do modelo real, sobretudo a rede de telefonia móvel. Essa simulação teve que ser feita devido à indisponibilidade de um ambiente real no laboratório. Dados como tempos de transmissão ou perdas de pacotes são completamente distintos dos valores reais ao se levar em conta a rede real de telefonia, e isso sem considerar eventuais e sazonais aspectos comuns na rede móvel como congestionamento ou variação no sinal de cobertura.

No início deste trabalho, um dos objetivos era o de fazer um estudo qualitativo e quantitativo entre as tecnologias de *web services* e Corba. Com a evolução do trabalho, esse objetivo foi direcionado para o estudo de pagamentos móveis, o que envolve não só o estudo de tecnologias de *middleware*, como também o estudo de tecnologias móveis além de todos os detalhes envolvendo esse problema específico de *m-payments*. O estudo comparativo entre Corba e serviços web foi adicionado na forma de Apêndice a este texto.

Apesar de ter sido feito um estudo extenso de CORBA, acabou-se optando por não adotá-lo no modelo e na implementação. Isso ocorreu pois todas os segmentos do modelo foram implementados na linguagem Java, bastando a utilização da tecnologia RMI para conexões dentro de um mesmo ator, representando uma comunicação inter-corporação, e a tecnologia de *web services*, na comunicação entre atores diferentes, ou seja, pretendendo já prever que os atores pudessem ser exercidos por entidades diferentes (inter-corporação).

Esse modelo de pagamentos móveis, no caso específico de ser efetuado através de um comerciante, pode representar uma interessante maneira de se criar uma forma de renda alternativa para milhares de pessoas no Brasil. Suponha-se uma localidade mais distante, onde o acesso seja difícil e que poucas pessoas tenham contas bancárias, caso bastante comum no Brasil. Se uma pessoa dessa sociedade tiver acesso a uma conta bancária, cartão de crédito ou débito, ela pode se tornar um “comerciante” para aquela localidade, vendendo créditos pré-pagos (desde de haja cobertura da rede de telefonia móvel naquela região).

Isso oferece uma maior comodidade para os usuários de telefonia móvel, evitando a necessidade de locomoção para centros maiores somente com o propósito de recarregar seus telefones, bem como uma oportunidade de renda extra para os novos comerciantes vendedores destes créditos. Além disso, representa uma forma de venda e de operação mais sofisticada que pode gerar retornos maiores para as operadoras móveis.

Uma outra vantagem deste sistema seria o de possibilitar a transferência de crédito entre duas pessoas quaisquer, bastando para isso que todos os usuários sejam considerados com *status* de “comerciante”. Assim, esses créditos poderiam ser passados de uma carteira eletrônica para outra carteira eletrônica e assim passar a ter valor de moeda no futuro. A preocupação com a regulamentação apareceria nesse caso.

No caso de operadoras internacionais, o modelo possibilitaria inclusive a entrada no mercado de transferências internacionais de recursos, principalmente de valores baixos. Hoje o mercado oferece soluções muito custosas para transferência de valores baixos entre países e pode representar uma nova fonte de renda para as operadoras de pagamentos móveis ou provedores independentes.

Todos esses fatores podem representar um grande benefício para a sociedade e um incremento na receita potencial das empresas atuantes no mercado de telefonia e de pagamentos.

## 6.4 Perspectivas futuras

Como trabalho futuro, propõe-se a inclusão no modelo de uma etapa no processo que seria a de descoberta do serviço de pagamentos móveis. Neste caso, haveria a necessidade de se fazer uma procura em um diretório de serviços utilizando-se o protocolo UDDI, o qual faz parte da estrutura dos serviços web. Isso possibilitaria que aplicações clientes pudessem descobrir como e onde acessar o serviço de pagamento móvel de uma forma mais automatizada e empregando mais uma tecnologia emergente que é o protocolo UDDI. Isso é pertinente para um caso mais abrangente onde diversas empresas procurariam por um provedor de serviços de pagamentos genérico que pudesse servir a todos os interessados, e da forma mais automatizada possível.

Propõe-se também que novos produtos e serviços sejam incluídos no modelo como possíveis objetos de transação ao se efetuar o *m-payment*, constituindo então um modelo genérico de pagamento móvel e não restrito ao pagamento de créditos de conversação.

Um outro aspecto importante é o de adicionar uma maior segurança ao protótipo. Isso pode ser feito através da inclusão de uma conexão segura (VPN) entre as pontes de serviços web e utilizando tecnologias que pudessem garantir a segurança no canal wireless de comunicação (WAP ou SMS) como as tecnologias de segurança WTLS e WIN.

Um outro aspecto interessante de ser estudado é uma análise do que existe hoje no mercado mundial e, sobretudo, as primeiras propostas que começam a aparecer no mercado brasileiro de tal forma a entender quais os principais problemas que tais implementações possuem de forma a inspirar a concepção de modelos mais robustos e seguros.

Poderia-se por fim também ser considerado o acesso dos dispositivos móveis à pontos de acesso de infra-estrutura de grids computacionais e a utilização de sistemas de arquivos altamente distribuídos, com por exemplo o Oceanstone.

Espera-se que esta dissertação possa servir de base para propostas de modelos mais abrangentes e sofisticados, buscando uma maior padronização do setor.

## Referências bibliográficas

- [1] KAYE, D. Loosely Coupled: The Missing Pieces of Web Services, RDS Press 2003.
- [2] MOBILE PAYMENT FORUM. Enabling Secure, Interoperable, and User-friendly Mobile Payments, Mobile Payment Forum White Paper, Dezembro 2002.
- [3] KRUEGER, M. Mobile Payments: A Challenge for Banks and Regulators, IPTS Report, Vol. 63, April 2002.
- [4] FORRESTER Research. European Mobile Payments – Can't Pay, Won't Pay Says Forrester, Maio 2001.
- [5] JONES N. Paybox: Pan-European Mobile Payments, Gartner Research, CS-14-2784, Setembro 2001.
- [6] SIAU, K. e SHEN, Z. Building Customer Trust in Mobile Commerce, Communications of the ACM, Vol 46, No. 4, Abril 2003.
- [7] BUHAN, D., CHEONG Y. C. e TAN, C. Mobile Payments in M-Commerce, Telecom Media Networks, Cap Gemini Ernest & Young, Setembro 2002.
- [8] WEBER, R. Chablis – Market Analysis of Digital Payment Systems, Technical Report TUM-19819, Technical University of Munich, Agosto 1999.
- [9] ABAD-PEIRO, J. L., ASOKAN, N. Steiner, M., and Waidner, M., Designing a Generic Payment Service, Technical Report 212ZR055, IBM Zurich Research Laboratory, Novembro 1996.
- [10] CHERCQ, K. Dividing the pie of mobile payment revenues: opportunity or threat to the traditional banking sector, Lessius Hogeschool, 2002.
- [11] WRONA, k., SCHUBA, M., and ZAVAGLI, G. Mobile Payments – State of the Art and Open Problems, 2001.
- [12] KRUEGER, M. The Future of M-Payments – Business Options and Policy Issues, Background Paper No.2, Electronic Payment Systems Observatory (ePSO), Agosto 2001.
- [13] TELECOM MEDIA NETWORKS. Mobile Payments: Money in Your Hands, Cap Gemini Ernest & Young.
- [14] KRUEGER, M.. M-Payments and the role of telcos, Electronic Payment Systems Observatory, ePSO-Newsletter Nr2, Outubro 2000.
- [15] DAHLBERG, T., Consumers Talk Back: Interview Based Findings about Customers' Willingness to Adopt Mobile Payment Solutions, Helsinki School of Economics, Abril 2002.
- [16] CHRISTENSEN, C. M. The Innovator's Dilemma: When New Technologies Cause Great Firms to Fail, Harvard Business School Press, 1997.
- [17] PayCircle. [www.paycircle.org](http://www.paycircle.org), acessado em fevereiro de 2005.

- [18] ADRIAN, B. Mobile Payments Consortia: What's the Difference?, Gartner Research, SPA-15-5775,22, Março de 2002.
- [19] LIBERTY ALLIANCE PROJECT. [www.projectliberty.org](http://www.projectliberty.org), acessado em fevereiro de 2005.
- [20] MOBEY FORUM. [www.mobeyforum.org](http://www.mobeyforum.org), acessado em fevereiro de 2005.
- [21] W3C WSDL. Web Services Description Language. <http://www.w3.org/TR/wsdl>, acessado em fevereiro de 2005.
- [22] EJBs. Enterprise Java Beans, <http://java.sun.com/products/ejb>, acessado em fevereiro de 2005.
- [23] W3C SOAP. Simple Object Access Protocol. <http://www.w3.org/2000/xp>, acessado em fevereiro de 2005.
- [24] APACHE ANT. <http://ant.apache.org>, acessado em fevereiro de 2005.
- [25] APACHE XERCES. <http://xml.apache.org/xerces2-j>, acessado em fevereiro de 2005.
- [26] APACHE AXIS. <http://ws.apache.org/axis>, acessado em fevereiro de 2005.
- [27] J2SE. Java 2 Standard Edition. <http://java.sun.com/j2se/index.jsp>, acessado em fevereiro de 2005.
- [28] J2EE. Java 2 Platform, Enterprise Edition. <http://java.sun.com/j2ee/index.jsp>, acessado em fevereiro de 2005.
- [29] APACHE TOMCAT. <http://jakarta.apache.org/tomcat>, acessado em fevereiro de 2005.
- [30] J2ME. Java 2 Micro Edition. <http://java.sun.com/j2me>, acessado em fevereiro de 2005.
- [31] INICIATIVA RADICCHIO. <http://www.radicchio.org>, acessado em fevereiro de 2005.
- [32] FISCHER M. Towards a Generalized Payment Model for Internet Services, Setembro 2002.
- [33] CLARENCE, N. W. e TAN, T. W. From E-commerce to M-commerce: The Power of the Mobile Internet, Idea Group Publishing, 2001.
- [34] SCHAPP, S., CORNELIUS, R., U-Commerce - Leading the New World of Payments, A Visa International and Accenture White Paper, [http://corporate.visa.com/md/dl/documents/downloads/u\\_whitepaper.pdf](http://corporate.visa.com/md/dl/documents/downloads/u_whitepaper.pdf), acessado em fevereiro de 2005.
- [35] PAUSON L. C. Verifying the SET Protocol: Overview, University of Cambridge, 2002.
- [36] ePSO. Paiement CB sur Mobile, France Telecom, ePSO Inventory DataBase, <http://www.jrc.es/cfapp/invent/details.cfm?uid=13>, acessado em fevereiro de 2005.

- [37] EMI. European Parliament and The Council of the European Union, EMI Directive, 2000, <http://register.consilium.eu.int/pdf/en/00/st03/03628en0.pdf>, acessado em fevereiro de 2005.
- [38] STUBER, W. D. e FRANCO A. C. P. O Comércio e a Prestação de Serviços via Internet, 2003.
- [39] PAYBOX. Empresa de pagamentos móveis, <http://www.paybox.net>, acessado em fevereiro de 2005.
- [40] TARASEWICH, P., NICKERSON, R., WARKENTIN, M. Issues in Mobile E-Commerce, Communication of the Association for Information Systems, 2002.
- [41] VISA. Visa Authenticated Payment Program, 3D Secure™, <http://international.visa.com/fb/paytech/secure/main.jsp>, acessado em fevereiro de 2005.
- [42] MASTERCARD. SPA – Secure Payment Application – ePSO Inventory Database, <http://www.jrc.es/cfapp/invent/details.cfm?uid=181>, acessado em fevereiro de 2005.
- [43] MOBILE PAYMENT FORUM, Risks and Threats Analysis and Security Best Practices, 2003.
- [44] BUHAN, D., CHEONG, Y. C., TAN C. Mobile Payments in M-Commerce, Cap Gemini & Ernst & Young, 2002.
- [45] TORVINEN, V. Wireless PKI Fundamentals, Radicchio, 2000.
- [46] VYAS A., O'GRADY P., A Review of Mobile Commerce Technologies, Department of Industrial Engineering, University of Iowa, 2001.
- [47] 3GPPE. Especificação GSM e EDGE, <http://www.3gpp.org/specs/releases.htm>, acessado em fevereiro de 2005.
- [48] SCOURIAS J., Overview of the Global System for Mobile Communications, 2003, <http://ccnga.uwaterloo.ca/~jscouria/GSM/gsmreport.html>, acessado em fevereiro de 2005.
- [49] ETSI. European Telecommunications Standards Institute, What is HSCSD (High Speed Circuit Switched Data), <http://corky.net/2600/wireless-networks/hscsd-high-speed-circuit-switched-data.shtml>, acessado em fevereiro de 2005.
- [50] BAUM, M., S., FORD W. Secure Electronic Commerce, Building the Infrastructure for Digital Signatures & Encryption, Prentice Hall New Jersey 1997.
- [51] BALTIMORE Technologies Ltd., Telepathy WAP Security Toolkit-Developer's Guide v1.2, 2000.
- [52] MIDP. Especificação final MIDP 2.0 (Mobile Information Device Profile), <http://jcp.org/aboutJava/communityprocess/final/jsr118/index.html>, acessado em fevereiro de 2005

- [53] MCKITTERICK, D. A Web Service Framework for Mobile Payment Services, Universidade de Dublin,, 2003.
- [54] ICSTIS Guideline, “Reverse-Billed Premium Rate SMS”, Technical Paper, May 2002.
- [55] MARQUES, P. R. O. R, O Pagamento Eletrônico: O Caso dos Pagamentos Móveis na Europa, Universidade Fernando Pessoa, 2003.
- [56] MARTINS, R., ROCHA, J., HENRIQUES, P., Segurança dos Web Services no Comércio Móvel, Universidade do Minho, 2003.
- [57] IETF/W3C. XML-Signature Syntax and Processing, W3C Recommendation, 2000.
- [58] WEBMETHODS, Verisign, Microsoft, Xml key management specification (xkms), 2001.
- [59] OASIS. Organization for the Advancement of Structured Information Standards, Especificação SAML, 2001.
- [60] POUSTTCHI Key, Charging for a Mobile Game, University of Augsburg, 2004.
- [61] W3C, Extensible Markup Language (XML) Specification, 2000.
- [63] W3C, Web Services Description Language (WSDL) Specification, 2001.
- [65] Parlay Group, <http://www.parlay.org>, acessado em fevereiro de 2005
- [64] UDDI, Universal Description, Discovery and Integration Specification, 2003.
- [65] IBM. WebSphere software, <http://www-306.ibm.com/software/websphere>, acessado em fevereiro de 2005.
- [66] MICROSOFT. .NET software, <http://www.microsoft.com/net>, acessado em fevereiro de 2005.
- [67] ONDRUS, J. Mobile Payments: A Tool Kit For A Better Understanding Of The Market, Universidade de Lausanne, 2003.
- [68] GOKHALE, A., KUMAR, B.,SAHUGUET, A. Reinventing the Wheel: Corba vs. Web Services, Vanderbilt University & Lucent Technologies, 2002.
- [69] MICROSOFT, COM: Component Object Model, <http://www.microsoft.com/com>, acessado em fevereiro de 2005.
- [70] OMG, CORBA, Common Object Request Broker Architecture, <http://www.omg.org>, acessado em fevereiro de 2005.
- [71] SSL, Secure Socket Layer Specification, <http://wp.netscape.com/eng/ssl3/>, acessado em fevereiro de 2005
- [72] Parser XML, [http://www.xml.com/pub/rg/XML\\_Parsers](http://www.xml.com/pub/rg/XML_Parsers), acessado em fevereiro de 2005
- [73] XML Schemas <http://www.w3.org/TR/xmlschema-0/>, acessado em fevereiro de 2005

- [74] GIANLUIGI ME, A Secure Mobile Local Payment Application Framework, Universidade de Roma "Tor Vergata", 2002
- [75] B. MENEZES, C. LAMB, J. PULLIKOTTIL, J TANZOLA, M-Commerce Payment Systems : Architectures and Protocols, University of New Mexico, 2003
- [76] Q. DAI, R J. KAUFFMAN, An Evaluative Model for e-Procurement Channel Adoption, University of Minnesota, 2002
- [77] S. NAMBIAR, CHANG-TIEN LU, M-Payment Solutions and M-Commerce Fraud Management, Virginia Polytechnic Institute, 2004
- [78] S. GROSS, R. MÜLLER, M. LAMPE, E. FLEISCH, Requirements and Technologies for Ubiquitous Payment, University of St. Gallen, Swiss Federal Institute of Technology, UBS AG, 2004
- [79] C. HORT, S. GROSS, E. FLEISCH, Critical Success Factors of Mobile Payment, Institute of Technology, University of St. Gallen, 2002
- [80] N. KREYER1, K. POUSTTCHI, K. TUROWSKI, Characteristics of Mobile Payment Procedures, University of Augsburg, 2002
- [81] J. HENKEL, Mobile Payment - The German and European Perspective, Ludwig-Maximilians-Universität München, 2001
- [82] G. HORN, B. PRENEEL, Authentication and Payment in Future Mobile Systems, Katholieke Universiteit Leuven, 2001

# Apêndice I: Análise crítica de serviços web e CORBA

## I.1 Introdução

A web foi inicialmente projetada para a troca de informações de forma não estruturada, e que, rapidamente, passou a ser utilizada por mecanismos de comércio eletrônico. Entretanto, em um primeiro momento, não existia um mecanismo uniforme para o acesso de serviços pela Internet, e cada serviço acabou expondo suas interfaces de uma maneira apropriada para seu uso particular (*ad-hoc*). Isso implicou em uma baixa ou inexistente interoperabilidade entre serviços. Esse problema aconteceu principalmente pelo fato de que o conteúdo e serviços disponíveis na web foram projetados para utilização humana e não para utilização por outras máquinas ou serviços.

Para facilitar um acesso automatizado para serviços complexos, um grupo de empresas lideradas pela Microsoft e IBM (e agora sendo tratado pelo *XML Protocol Activity Group* dentro do W3C) padronizou o SOAP (*Simple Object Protocol*) [23] como um protocolo simples baseado em XML para a troca de mensagens através da web. Esforços similares têm sido feitos para camadas de serviços mais altas como o WSDL (*Web Service Description Language*) [21] e UDDI (*Universal Description, Discovery and Integration*) [64].

Agora a tecnologia de serviços web está sendo considerada como a solução para os problemas hoje existentes no comércio eletrônico [68]. Estruturas básicas, necessárias para desenvolver serviços complexos em aplicações distribuídas, têm sido desenvolvidas já por vários anos. As mais populares são a COM [69] (*Component Object Model*), DCOM (*Distributed COM*) [69], COM+ [69] e .NET [66], que são específicas da Microsoft, EJB (*Enterprise Java Beans*) [22] e o RMI (*Remote Method Invocation*) [28] que são específica para Java, e CORBA (*Common Object Request Broker Architecture*) [70] que é independente de plataforma e de linguagem. CORBA em particular tem sido usado com sucesso como uma estrutura básica de componentes distribuídos em diversas áreas, incluindo telecomunicações, finanças, *e-commerce*, saúde, etc.

Uma diferença chave entre as tecnologias CORBA e serviços web é que CORBA provê uma arquitetura de componentes verdadeiramente orientada a objetos e, ao contrário, serviços web são primariamente baseados em mensagens. E ainda, CORBA também já inclui um grupo de serviços padrões (eventos, de nomes, negociação) que permitem aos desenvolvedores de aplicações focarem na lógica de negócios em vez de detalhes da infraestrutura de comunicação. Comparando, portanto, o trabalho atual sendo desenvolvido com a tecnologia de serviços web, pode-se questionar se não há uma repetição do que foi feito anteriormente com outras tecnologias [68].

Considerando que essas tecnologias, CORBA e serviços web, podem ser usadas no desenvolvimento de sistemas de pagamentos móveis, neste apêndice são investigadas e confrontadas suas principais características, e verificando até que ponto cada uma é adequada para determinadas partes do sistema.

## **I.2 CORBA versus serviços web**

Esta seção compara as tecnologias CORBA e serviços web baseados em dois aspectos diferentes. Primeiro, faz-se uma comparação baseada no modelo computacional. Em seguida, na Tabela 2, compara-se as tecnologias baseadas nas características de cada tecnologia.

Tabela 2. Comparação entre CORBA e serviços web [68].

Aspecto	CORBA	Serviços Web
Modelo de Dados	Modelo Objeto	Modelo SOAP de troca de mensagens
Acoplamento Cliente-Servidor	Forte ( <i>tight</i> )	Livre ( <i>loose</i> )
Transparência de localização	Referências a objetos	URL
Sistema de tipos	IDL Estático + verificação em tempo de execução	XML schemas Apenas verificação em tempo de execução
Tratamento de erros	Exceção de IDL	Mensagens de falta do SOAP
Serialização	Construção dentro da ORB	Pode ser escolhida pelo usuário
Passagem de Parâmetros	Por referência Por valor ( <i>valuetype</i> )	Por valor (não há noção de objetos)
Sintaxe de transferência	CDR Formato binário	XML Unicode
Estado	Com estado	Sem estado
Semântica de requisição	<i>At-most-once</i>	Definido pelo SOAP
Composição em tempo de execução	DII	UDDI/WSDL
Registro	Repositório de interfaces Repositório de implementações	UDDI/WSDL
Descoberta de Serviços	Serviço de nomes do CORBA Registro RMI	UDDI
Suporte de Linguagem	Qualquer linguagem com mapeamento de IDL	Qualquer linguagem
Segurança	Serviço de segurança CORBA	HTTP/SSL, assinatura XML
Passagem por <i>firewall</i>	Em desenvolvimento	Usa HTTP na porta 80
Eventos	Serviço de eventos CORBA	N/A

Uma importante observação a respeito de CORBA e serviços web é que qualquer serviço que pode ser construído com CORBA pode também ser construído com tecnologias de serviços web e *vice versa*, entretanto a quantidade de esforço para o desenvolvimento pode ser razoavelmente diferente. Em particular, pode-se implementar CORBA sobre SOAP, ou SOAP sobre CORBA.

A Tabela 3 provê uma comparação de alto nível da pilha de tecnologias em CORBA e nos serviços web comparando as camadas que são utilizadas na construção de um serviço distribuído.

Tabela 3. Pilha de tecnologias em CORBA e em serviços web [68]

Pilha do CORBA	Pilha de Serviços Web
IDL	WSDL
Serviços de nome CORBA	UDDI
Stubs/Skeletons de CORBA	Mensagem SOAP
Codificação binária do CDR	Codificação Unicode do XML
GIOP/IOP	HTTP
TCP/IP	TCP/IP

Nas próximas seções, comparam-se ambas as tecnologias através das dimensões especificadas nestas tabelas. Além disso, para cada uma dessas características, identificam-se os prós e contras de cada uma.

### I.3 Modelos de computação distribuída em CORBA e serviços web

A seguir são descritas as diferenças entre CORBA e serviços web, baseadas nos modelos computacionais de cada uma das tecnologias e como elas tratam as complexidades oriundas da distribuição [68].

#### Modelo de Dados:

Uma importante distinção que deve ser considerada ao examinar-se CORBA e serviços web é como uma aplicação é modelada em cada caso. CORBA apresenta uma estrutura de componentes verdadeiramente orientada a objetos, enquanto serviços web são baseados paradigma de passagem de mensagens simplesmente, sem a noção de objetos. SOAP, independentemente do seu nome, não lida com objetos. Existiu um esforço tardio de se redesignar o nome SOAP para “*Service Oriented Access Protocol*”, mas o *XML Protocol Activity Group* não aderiu a este acrônimo. Assim, nos últimos trabalhos do W3C, este protocolo é simplesmente chamado de SOAP 1.2, sem uma explicação do que significa.

No CORBA, existe um acoplamento forte entre o cliente e o servidor:

- ambos devem compartilhar a mesma interface, com um *stub* no lado do cliente e um *skeleton* correspondente no lado do servidor, e deve-se executar uma ORB em ambos os lados.
- A interação entre cliente e servidor pode ser feita diretamente sem necessidade por uma intermediação adicional (com exceção da ORB obviamente). O cliente obtém um identificador especial (*handle*) para um objeto CORBA em que pode aplicar os métodos.

Em serviços web essas etapas são desacopladas. O cliente envia uma mensagem e recebe uma mensagem. A resposta não oferece um acesso imediato ao próximo passo.

### **Semânticas de Requisição:**

Com o objetivo de manter a consistência dos dados, a infraestrutura deve prover a semântica *at most once*. Esta semântica garante em frente a múltiplas execuções de um mesmo cliente uma resposta do servidor.

ORBs do CORBA são obrigadas a prover a semântica *at most once*, garantindo, portanto, a integridade dos dados. CORBA também especifica um serviço de transação que provê suporte para modelos de transação múltipla como o *flat* e o *nested*.

Em serviços web, a semântica de mensagem é definida pelo protocolo utilizado pelo SOAP, o HTTP que não provê a semântica *at most once*. E ainda, SOAP possui uma noção de exceções/erros (especificação de faltas do SOAP), que podem ser retornados por serviços web. Esta parte da especificação do SOAP, entretanto, tem sido criticada uma vez que ela requer que um serviço retornando uma falta SOAP, também retorne um erro de status HTTP 500 (quando utilizando SOAP sobre HTTP), e portanto infringindo a natureza de camadas dos protocolos (ou seja, uma camada de baixo invocando uma camada superior).

### **Escalabilidade e Confiança**

Muitas aplicações como transações B2B e transações de comercialização de ações, entre outras, devem escalar de maneira confiável para milhões de transações por dia.

Em CORBA, as diretrizes do POA (*Portable Object Adapter*) combinadas com as características de tolerância a faltas e o serviço de balanceamento de carga provêm a

escalabilidade desejada a aplicações CORBA. A tolerância a falhas do CORBA usa o paradigma da redundância de entidade para prover tolerância a falhas em objetos CORBA.

Essas questões não fazem parte dos padrões dos serviços web, sendo deixadas para os componentes implementarem estes padrões. Servidores de Aplicação (como o WebSphere, por exemplo) implementam seus mecanismos proprietários para lidar com escalabilidade e confiança.

## **Serialização**

Serialização tem impacto sobre vários aspectos como persistência, desempenho, capacidade de extensão, e facilidade de interoperabilidade com outras estruturas.

A especificação de objetos por valor (*valuetypes*) do CORBA provê de forma independente da linguagem um equivalente à funcionalidade de serialização da linguagem Java. A especificação dos *valuetypes* permite funcionalidades como o mapeamento reverso de Java para IDL que permite que objetos Java RMI operem em conjunto como objetos CORBA; e o mapeamento XML/Valor que permite que documentos XML sejam representados como tipos nativos do CORBA.

SOAP permite mecanismos de serialização definidos pelo usuário. A codificação embutida no SOAP é baseada em XML e provê funções avançadas como *arrays* esparsos para reduzir os custos de transporte. Tem sido argumentado que o SOAP, sendo baseado em XML, é muito detalhado quando comparado com o formato binário IIOP do CORBA, e portanto introduz um problema de desempenho. Isso pode ser verdade para alguns tipos de aplicação, mas muitas aplicações complexas de negócio, o custo da passagem de mensagem é pequeno quando comparado com o custo do processamento da lógica do negócio. Portanto, essa natureza do SOAP, de ter mensagens maiores, pode não ser considerada um problema em muitas aplicações.

## **Controle estático e de tempo de execução**

A plataforma de programação deve oferecer algumas garantias estáticas ou em tempo de execução do comportamento de execução da aplicação.

CORBA utiliza IDL como uma linguagem de contrato. IDL é fortemente tipificado e provê algumas garantias estáticas. O DII (*Dynamic Invocation Interface*)

por outro lado não provê uma verificação estática. A implementação pode também tirar proveito da linguagem alvo (por exemplo, Java) com alguma verificação em tempo de execução (por exemplo, verificação de limites de *arrays*).

Quando se constroem serviços web, não existe um suporte de infraestrutura padronizada para oferecer verificações estáticas. Em tempo de execução, apenas a estrutura da mensagem SOAP é analisada, e um *payload* é necessário somente para ser uma parte de um documento XML bem formado. É responsabilidade da aplicação verificar o *payload* mais adiante (isto é, validar comparando com um *schema*). No futuro, WSDL poderia ser utilizado para gerar um mapeamento para uma linguagem de programação para oferecer algumas garantias estáticas.

Note, entretanto, que as verificações envolvidas durante uma validação de mensagem SOAP são de granularidade bem mais fina que as baseadas em IDL. *Schemas* XML são mais expressivos que IDL e definem algumas verificações de sintaxe (isto é, expressões regulares descrevendo o formato de uma data, etc.), e também verificações de semântica, que não podem ser capturadas pela IDL.

## **I.4 Suporte a características no CORBA e serviços web**

A seguir estão descritos características comuns e requisitos de aplicações representativos. Também é mostrado como CORBA e serviços web provêm suporte para cada uma destas características [68].

### **Transparência de localização**

Aplicações cliente devem ser capazes de interoperar com os serviços perfeitamente, sem a preocupação com a localização do serviço.

Aplicações cliente em CORBA obtêm referências para objetos e invocam operações nelas para realizar tarefas da aplicação sem a preocupação se os objetos estão remotos ou na mesma máquina relativamente ao cliente.

Aplicações cliente em serviços web (usando SOAP) referem-se a serviços usando URLs que implicitamente codificam a localização (endereço IP). Entretanto, informação de localização pode ser alterada via DNS. Um outro efeito de se codificar a informação de rede em URLs, é que isso permite uma manipulação semântica de endereços de rede diretamente no nível da aplicação, tornando mais fácil escrever serviços de *proxy*.

## Registro

Repositórios eficientes de serviços que mantêm toda a informação específica de serviços deve estar disponível.

O padrão CORBA define um repositório de interfaces que provê informação em tempo de execução sobre as interfaces IDL. Em tempo de execução, os clientes podem utilizar esse repositório para descobrir as operações que podem ser executadas em um objeto, e fazer invocações nele usando a Interface Dinâmica de Invocação (DII). O padrão CORBA também define um repositório de implementação que contém informação que permite a uma ORB ativar os servidores para processar uma requisição, e também outras informações específicas do servidor como controle administrativo, alocação de recursos, segurança, e modos de ativação.

Para serviços web, o UDDI provê uma estrutura baseada nos padrões XML/SOAP para descrever e gerenciar os serviços web. Em particular, o UDDI provê repositório centralizado de procura utilizando um mecanismo de publicação/assinatura que armazena definições de serviço. Um registro UDDI pode opcionalmente armazenar informação estrutural sobre o serviço no formato da especificação WSDL, que define um grupo de interfaces e mensagens usados pelo serviço. Informações sobre os próprios dados (metadados) para os serviços é armazenada no formato de *Schemas XML* para permitir a descoberta utilizando ferramentas padrões de procura.

## Descoberta de serviço

A procura por serviços deve ser bem simples, isto é, encontrar um serviço pelo seu nome ou funcionalidade oferecida.

O Serviço de Nomes do CORBA define uma referência a um objeto no formato de URL chamada de *corbaloc* que aplicações podem utilizar para alcançar serviços remotos. Uma segunda URL chamada *corbaname* permite aplicações invocar diretamente o serviço remoto. O Serviço de Negociação de Objeto suporta uma procura avançada, registro e descoberta de serviços baseado no tipo de serviço.

Em serviços web, registros UDDI permitem a descoberta de serviços combinando com uma determinada interface. O próprio UDDI é um serviço web acessível via uma interface SOAP.

## Firewall

Requisições de aplicação deveriam ser capazes de atravessar *firewalls* de forma transparente depois de uma verificação apropriada de segurança. Isso é crucial para aplicações que transpõem corporações.

Existe uma proposta de especificação de passagem de *firewall* do CORBA que permitirá requisições CORBA a serem roteadas através de *firewalls*.

Para serviços web, o protocolo de transporte preferencial é o SOAP sobre HTTP. Uma vez que esse é um protocolo presente em toda web com um uma porta bem definida, *firewalls* são normalmente configurados para permitir tráfico HTTP de entrada e de saída, e portanto permitindo a mensagens SOAP atravessar os limites dos *firewalls* com facilidade. A presença de um serviço web não requer nenhuma mudança na configuração do *firewall*. SOAP sobre HTTP seguro (usando SSL [71]) é tratado da mesma maneira.

## Segurança

Segurança em aplicações distribuídas requer uma variedade de características como autenticação [82], autorização, codificação, integridade dos dados, delegação, não repudição e auditoria.

Todas estas características são suportadas pelo serviço de segurança do CORBA. Entretanto, não existem serviços de segurança padronizados na pilha de serviços dos serviços web. Apesar disso, alguns aspectos de segurança podem ser tratados no nível de protocolo de transporte. SOAP não especifica nenhuma característica de segurança, mas torna mais fácil estabelecer uma segurança usando tecnologias da Internet com SSL [71] ou assinatura XML para uma interoperabilidade mínima. Além disso, produtos de serviços web começaram a oferecer alguns serviços de segurança (por exemplo, *Passport* da Microsoft). Entretanto, as soluções de segurança que estão sendo oferecidas para serviços web estão trabalhando em algo já bem desenvolvido como o serviço de segurança do CORBA.

## **Persistência**

Certas aplicações como “compras *online*” mantêm o estado do comprador no formato de carrinhos de compra. Esse tipo de informação deve ser persistente para proteção contra falhas no sistema ou como determinado pela lógica do negócio.

O serviço de persistência de estado do CORBA (PSS) provê o mecanismo para manter um estado de um objeto persistente. O PSS é uma camada abstrata que provê uma API única para utilizar qualquer tipo de armazenamento de dados como arquivos, bases de dados, diretórios, etc.

Serviços web não definem um mecanismo padrão de persistência, ao invés disso, deixam para a aplicação lidar com isso. Por exemplo, uma aplicação escrita em Java pode utilizar a serialização Java para criar objetos persistentes.

## **Facilidade de implantação e construção**

A estrutura deve permitir criar, construir e implantar serviços, integrando componentes novos assim como legados, e ainda oferecer interfaces abertas e padronizadas para os clientes.

O modelo de componentes do CORBA (CCM) provê um container similar ao EJB, e pode suportar EJBs como componentes CORBA. Além disso, o CCM provê a possibilidade de se desenvolver componentes em linguagens múltiplas. A especificação provê um formato de distribuição de software multi-plataforma que inclui um instalador e ferramentas de configuração baseadas em XML. Por causa desta característica independente desta plataforma, CORBA é bem apropriada para empacotar aplicações legadas como objetos CORBA e usá-los em conjunto.

A principal motivação do SOAP (e dos serviços web de forma mais geral) é endereçar a complexidade de se construir e implementar componentes de software. E o SOAP procura endereçar isto das seguintes formas.

SOAP conta com formatos de dados da web e protocolos que já consagraram seu sucesso, como o XML e o HTTP.

SOAP possibilita a interoperabilidade com a imposição de um protocolo simples baseado em mensagem que é independente do modelo, da linguagem e da plataforma.

O modelo de dados fundamental é baseado em XML (*XML Schemas*) o que o faz expressivo e extensível.

SOAP tem sido enriquecido por novas tecnologias (como WSDL e UDDI) para tornar mais fácil a criação, construção e implementação de serviços web.

### **Independência de plataforma**

Ofertas de novos serviços podem necessitar usar componentes construídos em plataformas heterogêneas, envolvendo hardware e software diferentes, incluindo diferentes sistemas operacionais e linguagens de implementação.

CORBA foi projetado para ser independente de plataforma. Isto inclui hardware, sistemas operacionais e linguagens de programação ou de script.

Em serviços web, toda comunicação de mensagem é feita via SOAP, e nenhuma outra restrição (por exemplo, similaridade de plataformas) é imposta ao cliente ou ao servidor. A única necessidade é de ser capaz de ler e escrever mensagens SOAP (isto é, documentos XML).

### **Capacidade de processamento (*footprint*)**

A utilização de dispositivos móveis como PDAs demanda a utilização de uma aplicação que consuma pouca capacidade de processamento (e de outros recursos, tais como memória) no lado do cliente (ou até do lado do servidor).

A especificação mínima do CORBA provê um subconjunto do CORBA padrão e é direcionado primeiramente para sistemas embutidos. A OMG também está trabalhando em uma especificação de CORBA sem fio [10] que permite acesso sem fio, mobilidade de terminal, e provisão de serviços em CORBA.

Em serviços web, dependendo da complexidade do cliente e servidor (por exemplo, se WSDL/UDDI são necessários), a necessidade de capacidade de processamento irá variar. Em casos extremos (exemplo, clientes *thin* acessando serviços simples), é possível até que o cliente não precise nem de um *parser* XML completo.