ANDRE GROSSI MACEDO
RAPHAEL PINHEIRO DA SILVA
MURILO FUKUSHIMA FREITAS

INTERAÇÃO REMOTA COM BOLSA DE VALORES

Dissertação Apresentada à Escola
Politécnica da Universidade
de São Paulo para obtenção do
Título de Graduação em Engenharia

Área de Concentração:
Engenharia da Computação

Orientadora:
Prof.ª Dr.ª Tereza Cristina Melo de Brito Carvalho

São Paulo
2004

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

À minha mãe e minha namorada que foram o meu apoio nos momentos difíceis e partilharam comigo os melhores momentos de minha vida.

André Grossi Macedo

À minha família, meu cunhado, minha ex-namorada pelo carinho e apoio em todos os momentos. Aos meus amigos da faculdade e do projeto, que compartilharam comigo momentos de desespero, tristeza e alegria.

Murilo Fukushima Freitas

Aos meus pais, namorada e irmão pelo carinho, incentivo e por estarem sempre presentes. Aos amigos de faculdade e de truco que compartilharam os difíceis anos de POLI, tornando-os mais agradáveis.

Raphael Pinheiro da Silva

AGRADECIMENTOS

A todos nossos professores que nos ajudaram durante os anos de POLI, e aos nossos colegas que de alguma forma colaboraram e contribuíram na execução desse projeto.

1 RESUMO

O sistema é destinado aos investidores de ações que não têm tempo de acompanhar seus investimentos a todo momento.

Para prover um rápido acesso aos investimentos, o sistema previsto será implementado em dispositivos móveis como palms e celulares e manterá o investidor atualizado de informações relevantes sobre suas ações, podendo também enviar ordens de compra e venda rapidamente de qualquer lugar, bastando apenas estar conectado à Internet por um canal wireless.

A principal função do sistema é permitir ao o investidor o envio de ordens de compra e venda a qualquer momento, estando conectado a Internet por uma rede wireless.

O sistema consiste basicamente de dois módulos, o módulo Web (Home Broker) e o módulo móvel (Mobile Broker), conectados ao Web Service conforme desenho abaixo:

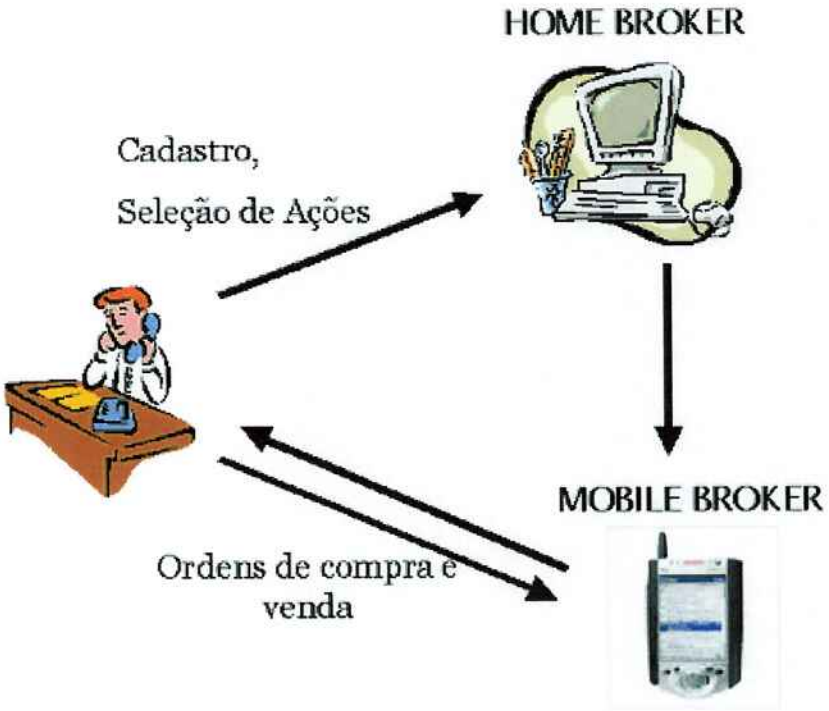

Figura 1.1 – Visão Geral do Sistema

Ao final do projeto deve-se ser capaz de enviar uma ordem através de um dispositivo móvel conectado à Internet para um Web Service, utilizando algoritmo de criptografia adequado, efetuando a negociação com segurança. Não é escopo do projeto tratar essa negociação diretamente com a bolsa de ações, sendo esta negociação apenas registrada em banco de dados.

Caso não seja possível obter esse dispositivo móvel e/ou conectá-lo a Internet, a demonstração será feita através de um emulador apropriado.

2 ABSTRACT

The system is destined to stock market investors with very short time to take care of their investments.

In order to supply fast access to investments, the system will be implemented for mobile devices, such as palms and cell phones, and will keep the user up-to-date, giving him relevant information about his stocks. The system will also allow the user to buy and sell stocks very quickly, wherever he goes, as long as he is connected to the Internet through a wireless network.

The main system's functionality is to allow investors to send buy and sell orders anytime he wants, as long as he is connected to the Internet through a wireless network.

The system consists in basically two modules: web home broker and the mobile broker using Web Services to communicate, as shown below:

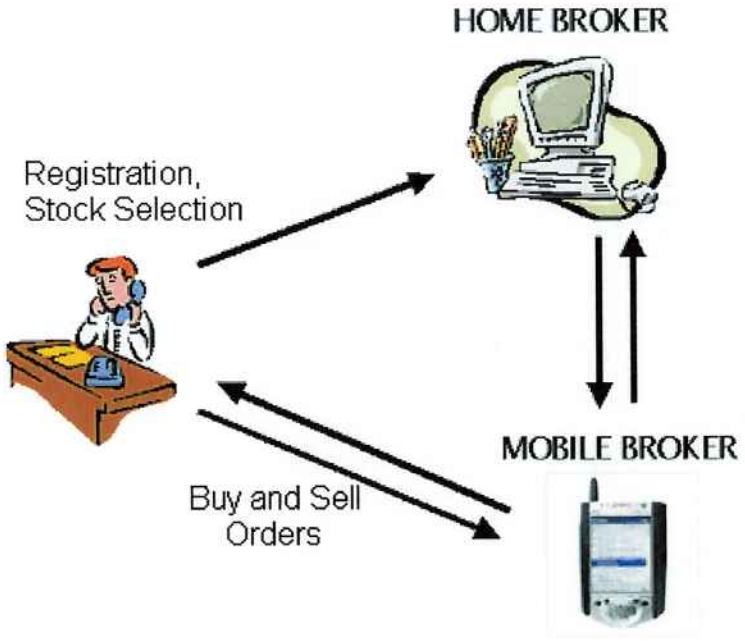

Figura 2.1 – Visão Geral do Sistema

At the end of the project, we will be able to send orders through a mobile device connected to the Internet to a Web Service and that way communicating with the home broker. The communication will use encrypting and will assure data security.

The communication with the real Stock Market and making real stock operations are not part of the project target. The Mobile Broker will communicate with our own Home Broker and all the operations concerning the stocks will only be registered in the data base.

Not being able to connect the mobile broker to the Internet for the final presentation, a demonstration will be done using a proper emulator.

3 ESCOLHA DO TEMA

3.1 MOTIVAÇÃO DO PROJETO

Pode-se notar na história da Bolsa de Valores uma grande evolução na maneira que a compra e venda de papéis era realizada e como as informações eram disponibilizadas para os interessados.

Até 1972 a Bolsa caminhava na "idade da pedra", onde um funcionário anotava numa lousa os negócios feitos no pregão e registrados pelos operadores.

Neste ano houve uma evolução e a lousa, inadequada para aquele fim, foi trocada por vídeos e um painel magnético para divulgação das informações do pregão. Surgiu assim o sistema on-line de negociações. Os cartões codificados T-Scan, lidos pelo terminal de computadores da Bolsa, cujos dados passaram a figurar nos aparelhos de vídeo, substituíram o boleto, ultrapassado.

Os registros automatizados de informações, índices, volumes e quantidades de ações transacionadas eram atualizados de quinze em quinze minutos, alterando completamente a dinâmica da Bolsa. Um painel central informava o último preço das 288 ações mais cotadas.

Em 1974, após inovações nesse sistema, foi substituído por uma central de processamento de dados.

Em 1976 foi instalado o sistema em rede no pregão viva-voz, permitindo contato direto entre as corretoras e a Bolsa.

Na década de 80 foi instalado um sistema privado de operações por telefone, o sistema Spot. Com mil e quinhentos ramais, interligava os maiores centros financeiros do País e do mundo.

Em 1994 o sistema Cats passou a divulgar dados do pregão viva-voz de forma simultânea. Todas as ações de empresas listadas na Bolsa passaram a ser negociadas eletronicamente. Em seguida vieram o Disque Bovespa, Internet, Fax Custódia, Press Information e Informe Técnico em disquete.

Em 1996, o software do Cats, que possibilitava um número máximo de 10 mil mensagens, não podia ser ultrapassado, foi substituído pelo MegaBolsa.

Em abril de 2003, o modelo 380 do MegaBolsa exigiu a troca de todos os equipamentos para permitir a ampliação do volume de transações. Atualmente o

potencial deste sistema é muito grande. Um exemplo disso foram as 100 milhões de mensagens enviadas em um único dia.

Com este potencial de difusão de informações, o tempo corre contra os investidores, que precisam receber as informações relevantes o mais rápido possível, para que não percam bons negócios.

Tendo em vista este cenário e as ferramentas disponibilizadas atualmente no mercado, a utilização de dispositivos móveis, com o intuito de minimizar o tempo de ação de um investidor, faz-se mais do que necessária.

3.2 Cenário Atual da Bolsa de Valores

O mercado acionário ofereceu sinais positivos entre o final do primeiro e o início do segundo semestre de 2004, época em que a abertura de capital de empresas de diversos ramos de atividade ou a captação de novos recursos junto a investidores foi bem-sucedida. Deve-se dar ênfase ao fato de que dezenas de milhares de pessoas físicas aplicaram em ações, entre junho e julho do mesmo ano.

Esses resultados são atribuídos tanto à melhora das perspectivas econômicas como ao avanço da idéia de atrair mais investidores para o mercado, conseguido principalmente com o programa "Bovespa Vai Até Você". Os indicadores desta campanha, iniciada em maio de 2002, são expressivos. Houve acréscimo de 40 mil investidores em ações e a formação de mais de 400 clubes de investimento. Em fins de julho de 2004, apenas o fundo do BNDES (PIBB), com cotas de uma carteira que reúne as 50 empresas com maior liquidez em bolsa, atraiu 25 mil aplicadores individuais, além de investidores institucionais.

Outro foco do programa é chamar empresas para a abertura de capital, desenvolvendo desta maneira o mercado acionário. O foco principal são as empresas com elevados padrões de governança corporativa, dispostas a seguir programas de responsabilidade social e de entrosamento com a comunidade à qual pertencem.

Companhias que atuam em sintonia com a sociedade e têm altos padrões de governança tornam-se mais atrativas e são mais valorizada, no entanto precisam também ter boa rentabilidade, fundamental para atração de novos investidores.

Neste tipo de empresa se incluem as sociedades abertas que integram o Novo Mercado da Bovespa. Os responsáveis pelo Plano Diretor do Mercado de Capitais

não hesitaram em propor melhor tratamento tributário para os acionistas, com ênfase nas empresas que valorizam os minoritários. É um passo fundamental visando o aumento da qualidade dos investimentos em ações, cujo risco é minimizado quanto melhores forem as empresas emissoras.

Lançamentos bem-sucedidos de ações, entre o final do primeiro semestre e o início do segundo de 2004, atraíram participantes em busca de boas ofertas, na expectativa de obter bons resultados, às vezes no curtíssimo prazo. Alguns exemplos de lançamento destas ações foram as da empresa de cosméticos Natura, da ferrovia América Latina Logística (ALL) e da companhia aérea Gol. A demanda pelas ações destas empresas superou muito a oferta, ou seja, as empresas poderiam ter captado bem mais do que inicialmente pretendiam, podendo fortalecer ainda mais seu capital de giro e seus investimentos.

A economia brasileira, demonstrada pelos indicadores do primeiro semestre de 2004 sobre o setor externo, emprego, renda e, sobretudo, produção industrial e comércio, tornou as empresas atrativas para os acionistas, permitindo a recuperação dos preços no mercado acionário, ajudando muito no êxito das operações acionárias. É, sem dúvida, altamente contrastante com o cenário de anos anteriores onde, com grande freqüência, havia mais empresas dispostas a fechar do que a abrir o capital, ou seja, o contrário do que fizeram Natura, ALL e Gol.

Deve-se lembrar da capitalização das pequenas e médias empresas, hoje ainda praticamente ausentes da Bolsa. O relançamento do mercado de acesso (Soma), espécie de degrau intermediário que antecede a chegada no pregão, tem por objetivo ampliar os serviços oferecidos aos pequenos e médios empresários, trazendo-os para a abertura de capital, o que pode atrair novos investidores.

Os gráficos abaixo mostram o volume médio diário negociado na Bolsa, o volume total negociado e o número de negócios efetuados, ambos segregados em tipos de mercado:

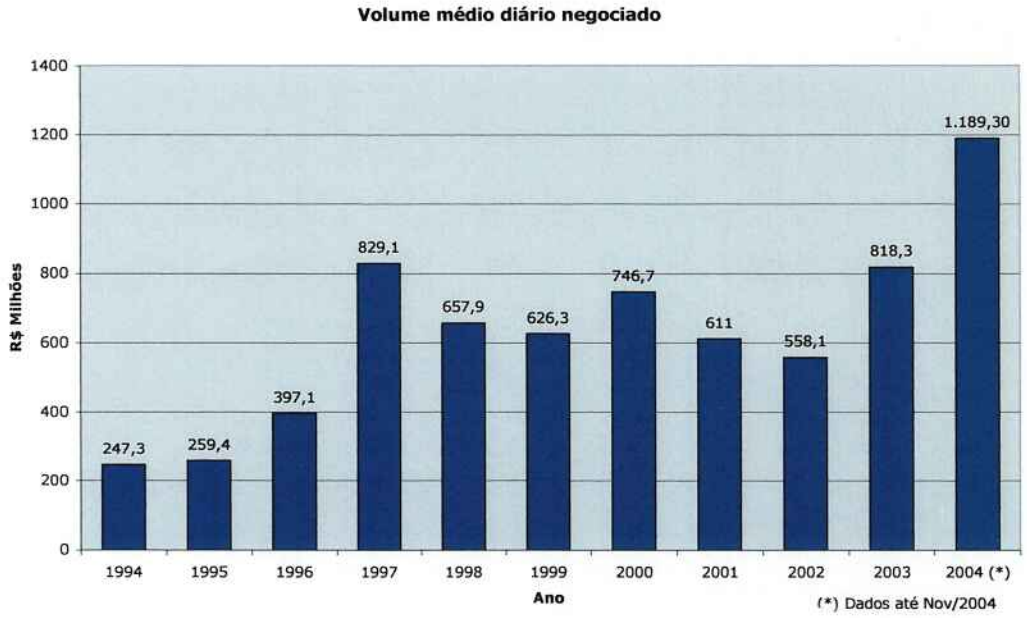

Figura 3.1 – Volume médio diário negociado na Bolsa

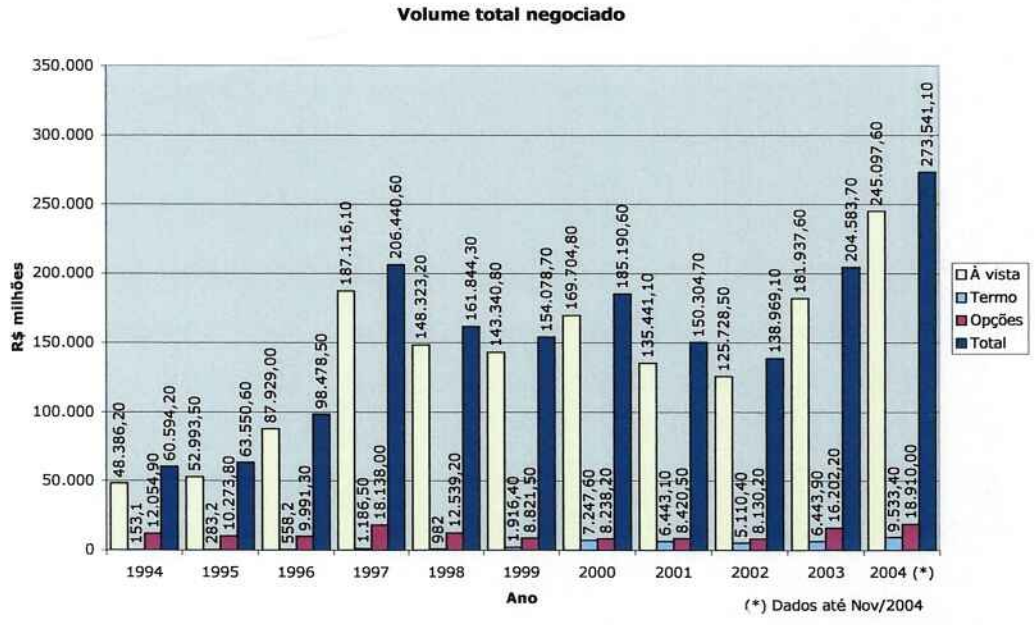

Figura 3.2 – Volume total negociado na Bolsa

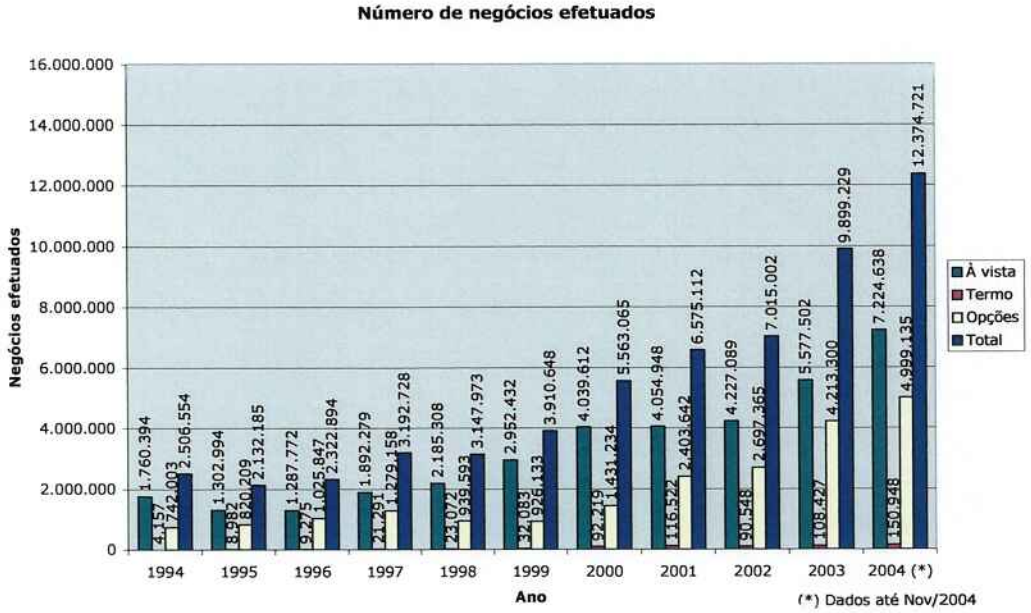

Figura 3.3 – Número de negócios efetuados na Bolsa

Com estes gráficos pode-se notar nitidamente o aumento do volume de negócios e do volume negociado, indicando uma expansão neste tipo de mercado, gerando oportunidades futuras.

3.3 Aliar Novas Tecnologias ao Projeto

A viabilização do projeto do Mobile Broker deve-se principalmente às inovações tecnológicas, de onde são frutos os PDAs, computadores mais potentes, estrutura de redes, conexões wireless, entre outras.

Para a implementação do Mobile Broker foi necessário dispor das seguintes tecnologias:

- Hardware:
  - Servidores;
  - PDAs para acesso wireless;
  - Placas de rede Wi-Fi para conexão entre o PDA e o Access Point;
  - Access Points para conexão com os PDAs;
  - Estrutura de rede.
- Software:
  - Tomcat versões 4.1.3 e 5.0.25;

- Eclipse versão 3.0;
- Plugins utilizados: Lomboz, Aston, Sysdeo e SolarEclipse.
- Banco de Dados SQL Server 2000;
- Emulador de PDA Sun Wireless Toolik versão 2.2;

A plataforma Java foi escolhida para desenvolvimento do software residente no PDA devido à sua grande difusão entre estes dispositivos e também pela grande aceitação no mercado. Seguindo esta linha, as páginas da parte Web do projeto foram desenvolvidas em HTML e JSP, utilizando-se a mesma plataforma (Java) nas duas pontas, facilitando o trabalho de união das mesmas.

Foram desenvolvidos ainda Web Services para que a parte Web acessasse os bancos de dados e também se comunicasse com os PDAs.

A inovação do projeto está no desenvolvimento da parte de segurança entre o dispositivo móvel e a Internet, utilizando-se o protocolo 802.11. A segurança é necessária pois dados sigilosos como senhas e ordens serão trafegados e não podem ser lidos por terceiros.

3.4 Utilizar Dispositivos Difundidos na Atualidade

A mobilidade necessária para implementação do projeto pôde ser alcançada com a utilização de PDA's, pois são dispositivos móveis de alta capacidade de processamento e armazenamento, dando grande agilidade para o investidor.

No mercado há desde modelos muito simples até modelos extremamente robustos, sendo o preço de cada dispositivo proporcional à sua complexidade.

Abaixo pode-se ver uma tabela com os dispositivos disponíveis no mercado:

PDA	Preço (US$)	Sist. Oper.	Mem RAM	Mem ROM	Processr	Tela	Expansão	Connecti vidade	Tipo de bateria
Treo 600	$600	5.2	32MB	MB	144 MHz A	R 4K Cores	SDIO	CDMA, 1xRTT	RLI
Tungsten C	$500	5.2.1	64MB	N/A	400 MHz XScale	T 64K Cores	MMC, PUC, SDIO	WiFi	RLP
Treo 600	$495	5.2	32MB	MB	144 MHz A	R 4K Cores	SDIO	GSM, GPRS	RLI
Tungsten T3	$400	5.2.1	64MB	MB	400 MHz XScale	T 65K Cores	SD, MMC, SDIO	Blue	RLI
Tungsten T5	$400	PPC 2K3	256MB	MB	400 MHz XScale	T 65K Cores	SD, MMC, SDIO	Blue, WiFi	RLI
Tungsten T5	$400	PPC 2K3	256MB	MB	400 MHz XScale	T 65K Cores	SD, MMC, SDIO	Blue, WiFi	RLI
Zire 72	$300	5.2.1	32MB	8MB	300 MHz XScale	T 65K Cores	SD, SDIO	Blue	RLP
Tungsten E	$190	5.2	32MB	MB	16 MHz XScale	T 65K Cores	SD, MMC	N/A	RLI, RB

Zire 31	$150	5.2.1	16MB	MB	200 MHz XScale	T 4K Cores	SD, MMC, SDIO	N/A	RLP
A730	$500	PPC 2K3 SE	64MB	64MB	520 MHz Bulverde	T 64K Cores	CF, MMC, SDIO	Blue	RLI, RB
A716	$400	PPC 2K3	64MB	64MB	400 MHz XScale	T 64K Cores	SD, CF, MMC	Blue, WiFi	RLI
A620 Bluetooth	$300	PPC 2K3	64MB	64MB	400 MHz XScale	T 64K Cores	CF	Blue	RLI
A620	$280	PPC 2K3	64MB	32MB	400 MHz XScale	T 64K Cores	CF	N/A	RLI
Evesham CoPilot Pocket PC	$700	PPC 2K3	64MB	32MB	300 MHz XScale	T 65K Cores	SDIO	N/A	RLI
Evesham CoPilot GPS	$500	PPC 2K3	64MB	32MB	300 MHz XScale	T 4K Cores	SDIO	N/A	RLI
GL3000	$200	PPC 2K3	64MB	32MB	300 MHz XScale	T 64K Cores	SD, MMC	N/A	RLI
hx4705	$650	PPC 2K3 SE	64MB	128MB	624 MHz Bulverde	T 64K Cores	SD, CF, MMC, SDIO	Blue, WiFi	RLI, RB
hx4700	$650	PPC 2K3 SE	64MB	128MB	624 MHz Bulverde	T 64K Cores	SD, CF, MMC, SDIO	Blue, WiFi	RLI, RB
h5550	$580	PPC 2K3	128MB	48MB	400 MHz XScale	T 64K Cores	MMC, SDIO	Blue, WiFi	RLP, RB
h5555	$580	PPC 2K3	128MB	48MB	400 MHz XScale	T 64K Cores	MMC, SDIO	Blue, WiFi	RLP, RB
h5150	$550	PPC 2K3	64MB	32MB	400 MHz XScale	T 64K Cores	MMC, SDIO	Blue	RLP, RB
h6315	$500	PPC Phone 2003	64MB	64MB	168 MHz OMAP	T 64K Cores	MMC, SDIO	Blue, GSM, WiFi	RLI, RB
h4350	$450	PPC 2K3	64MB	32MB	400 MHz XScale	T 64K Cores	MMC, SDIO	Blue, WiFi	RLI, RB
h4355	$450	PPC 2K3	64MB	32MB	400 MHz XScale	T 64K Cores	MMC, SDIO	Blue, WiFi	RLI, RB
h4155	$400	PPC 2K3	64MB	32MB	400 MHz XScale	T 64K Cores	MMC, SDIO	Blue, WiFi	RLI, RB
h4150	$380	PPC 2K3	64MB	32MB	400 MHz XScale	T 64K Cores	MMC, SDIO	Blue, WiFi	RLI, RB
h2210	$350	PPC 2K3	64MB	32MB	400 MHz XScale	T 64K Cores	CF, MMC, SDIO	Blue	RLI, RB
h2215	$350	PPC 2K3	64MB	32MB	400 MHz XScale	T 64K Cores	CF, MMC, SDIO	Blue	RLI, RB
h1945	$300	PPC 2K3	64MB	32MB	266 MHz Samsung	T 64K Cores	MMC, SDIO	Blue	RLI, RB
rz1715	$260	PPC 2K3	32MB	32MB	203 MHz Samsung	T 64K Cores	SD, MMC, SDIO	N/A	RLI
i-mate PDA2K Pocket PC Phone	$850	PPC Phone 2K3	128MB	64MB	400 MHz XScale	T 64K Cores	MMC, SDIO	Blue, GSM, WiFi, GPRS	RLP
i-mate Pocket PC Phone	$800	PPC 2K3	128MB	32MB	400 MHz XScale	T 64K Cores	MMC, SDIO	Blue, GSM, GPRS	RLP
Mio168	$450	PPC 2K3	64MB	32MB	300 MHz XScale	T 65K Cores	SDIO	N/A	RLI
Mio168	$450	PPC 2K3	64MB	32MB	300 MHz XScale	T 65K Cores	SDIO	N/A	RLI
Navman PIN	$500	PPC 2K3	64MB	32MB	300 MHz XScale	T 65K Cores	SDIO	N/A	RLI
Skywalker GPS 500	$460	PPC 2K3	64MB	32MB	300 MHz XScale	T 65K Cores	MMC, SDIO	N/A	RLI
PPT8846 Rugged Pocket PC	$2095	PPC 2K3	64MB	64MB	400 MHz XScale	T 64K Cores	N/A	WiFi	RLI
PPT8860 Rugged Pocket PC	$2095	PPC 2K3	64MB	64MB	400 MHz XScale	T 64K Cores	N/A	Blue	RLI
PPT8860 Rugged	$1795	CE.NET	32MB	32MB	300 MHz XScale	T 64K Cores	N/A	Blue	RLI

CE.NET Device									
PPT8800 Rugged Pocket PC	$1795	PPC 2K3	64MB	64MB	400 MHz XScale	T 64K Cores	N/A	N/A	RLI
PPT8846 Rugged CE.NET Device	$1795	CE.NET	32MB	32MB	300 MHz XScale	T 64K Cores	N/A	WiFi	RLI
PPT8800 Rugged CE.NET Device	$1495	CE.NET	32MB	32MB	300 MHz XScale	T 64K Cores	N/A	N/A	RLI
Recon 400 - Gray	$1600	PPC 2K3	64MB	128MB	400 MHz XScale	T 65K Cores	CF	N/A	RB, RNiMH
Recon 200 - Gray	$1300	PPC 2K3	64MB	64MB	200 MHz XScale	T 65K Cores	CF	N/A	RB, RNiMH
SPH-i700	$750	PPC Phone	64MB	32MB	300 MHz XScale	R 65K Cores	MMC, SDIO	CDMA, 1xRTT	RLI, RB

Tabela I – Dispositivos Móveis disponíveis no mercado

4 PLANO DE NEGÓCIO

4.1 MISSÃO

Permitir maior mobilidade e agilidade na compra e venda de ações em um ambiente seguro utilizando PDA's.

4.2 MODELO DE NEGÓCIOS

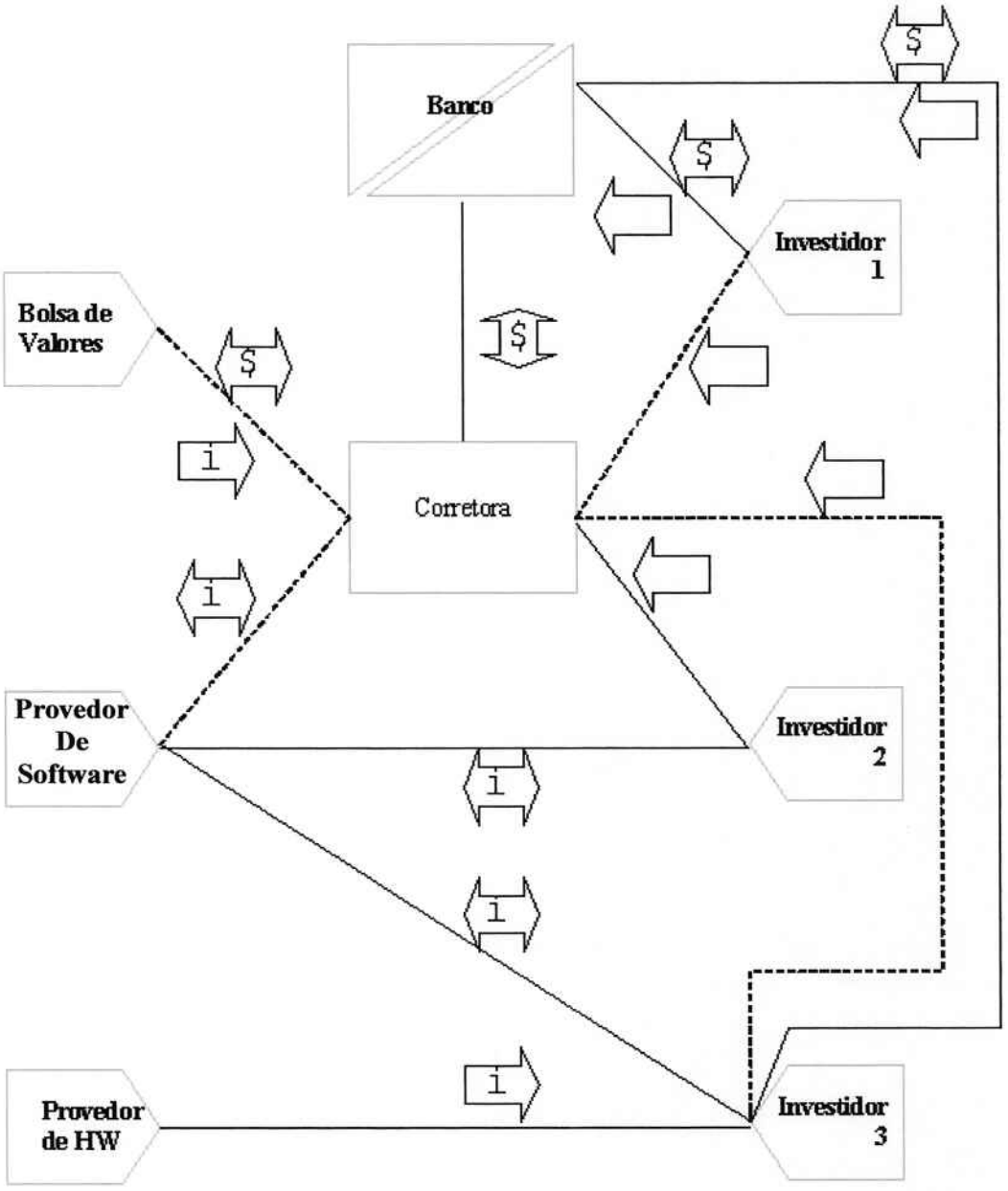

Figura 4.1 – Visão Geral do Sistema

4.3 ANÁLISE SWOT

A análise de SWOT ou PFOA consiste em uma ferramenta de planejamento estratégico para avaliação de potencialidades (pontos fortes), fragilidades (pontos fracos), oportunidade e ameaças do projeto.

PONTOS FORTES

- Mobilidade;
- Facilidade e rapidez no acesso às informações;
- Melhor acompanhamento das variações do mercado de ações;
- Versatilidade dos equipamentos;
- Domínio pioneiro da tecnologia wireless utilizando o protocolo 802.11 para fins de conexão entre PDA's e computadores;
- Economia de tempo do cliente;
- Melhor aproveitamento espacial;
- Agilizar as negociações, podendo gerar melhores negócios.

PONTOS FRACOS

- Insegurança quanto à utilização de PDA's para transações financeiras;
- Estrutura de rede wireless não muito difundida;
- Necessidade de aquisição de aparelhos móveis de última geração;
- Restrições de memória e processamento, impactando a solução, impostas pelos dispositivos móveis.

OPORTUNIDADES

- Aumento do número de pessoas física atuante no mercado acionário;
- Crescimento do número de usuários de sistemas on-line para compra e venda de ações (Home Brokers);

- Crescimento das vendas de PDA's;
- Ausência de solução no mercado que utilize a mesma tecnologia.

AMEAÇAS

- Maior número de funcionalidades disponibilizadas pelos sistemas de Home Broker;
- Provedores do serviço de Home Broker disponibilizarem solução similar para dispositivos móveis utilizando tecnologia wireless;
- Captura de informações sigilosas por terceiros mal intencionados;
- Problemas na rede wireless acarretando na perda de ordens de compra ou venda;
- Não recebimento de confirmação das ordens pelos motivos supracitados.

4.4 COMPETÊNCIAS

- Enlace confiável com BOVESPA e instituições financeiras;
- Garantir alta disponibilidade dos sistemas;
- Dispor de pessoal técnico especializado para dar suporte ao cliente;
- Capacidade de desenvolvimento de um sistema amigável;
- Disponibilização de informações sobre atualização de SW;
- Bom manual e tutorial;
- Fornecimento de equipamento em caso de perda;
- Suporte e solução de segurança;
- Monitoramento da rede.

4.5 PÚBLICO ALVO

Investidores individuais que têm facilidade com novas tecnologias:

- Pessoa Física;
- Idade entre 35 a 40 anos;

- Curso superior concluído;
- Renda em torno de R$50.000 anuais;
- Perfil arrojado;
- Investidores com acesso a redes wireless locais em empresas, aeroportos, etc;

4.6 FATORES CRÍTICOS

- Implementação da rede wireless e a segurança da mesma;
- Criptografia dos dados trafegados pela rede;
- Autenticação do usuário;
- Disponibilidade da rede para os usuários;
- Sigilo das informações armazenadas nos servidores;
- Conhecimento da tecnologia de PDA's;
- Acesso à Internet para cadastro dos dados do cliente;
- Tempo de resposta à ação do cliente (ordem de compra ou venda);
- Aceitação do produto (competição com Home Brokers já existentes).

5 MERCADO ATUAL

5.1 QUANTIDADE DE INVESTIDORES

O número de investidores pessoa física aumentou consideravelmente nos últimos anos devido a maior divulgação do mercado de capitais e difusão de informações deste segmento. A Bovespa também lançou em maio de 2002 um programa de incentivo à pessoa física e aos clubes de investimento, chamado "Bovespa Vai Até Você", para popularizar o investimento em ações e esclarecer as pessoas sobre a importância do mercado de capitais para o desenvolvimento do País.

A tarefa de educar e atrair o investidor tem tido enorme apoio de sociedades corretoras que se engajaram no programa de constituição dos clubes de investimento. Esta também é uma mudança de atitude do intermediário, que quer conquistar o pequeno aplicador, antevendo um futuro em que milhões de novos investidores deverão chegar ao mercado trilhando esse caminho. Apoios do novo governo e do Legislativo, como a reforma previdenciária, fortalecendo os fundos de pensão e, conseqüentemente, as aplicações de longo prazo, como as ações, também faz com que este público cresça.

Outro aspecto que aumentou a visibilidade deste mercado foi a oferta de venda de ações do Banco do Brasil, na esteira das colocações bem-sucedidas de Petrobrás e Vale do Rio Doce, com a possibilidade de usar recursos do FGTS.

Tais campanhas de popularização refletiram no aumento do número de pessoas que se mostram interessadas em participar do mercado acionário como também pela crescente consciência, entre elas, de que a Bolsa não é um centro de negócios inatingível, acessível apenas aos iniciados.

Com os programas de incentivo, principalmente o "Bovespa Vai Até Você", criado em maio de 2002, o número de usuários cresceu muito. O gráfico abaixo ilustra este crescimento:

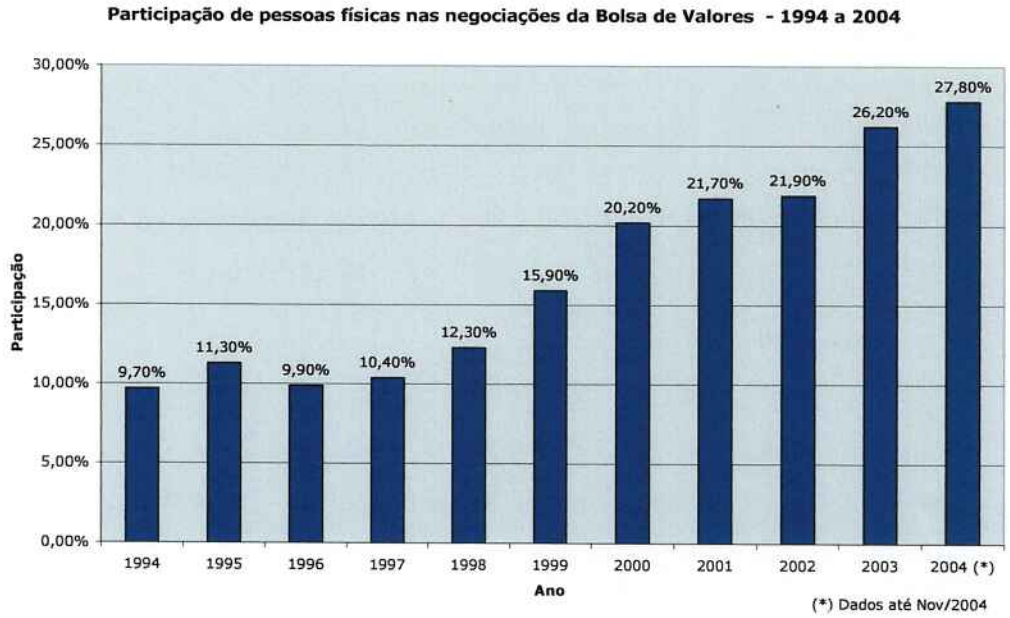

Figura 5.1 – Participação de pessoas físicas nas negociações da BOVESPA entre 1994 e 2004

A distribuição de investimentos entre os investidores ainda é muito desigual, oferecendo um potencial de crescimento para o Brasil. Abaixo pode-se ver tal distribuição.

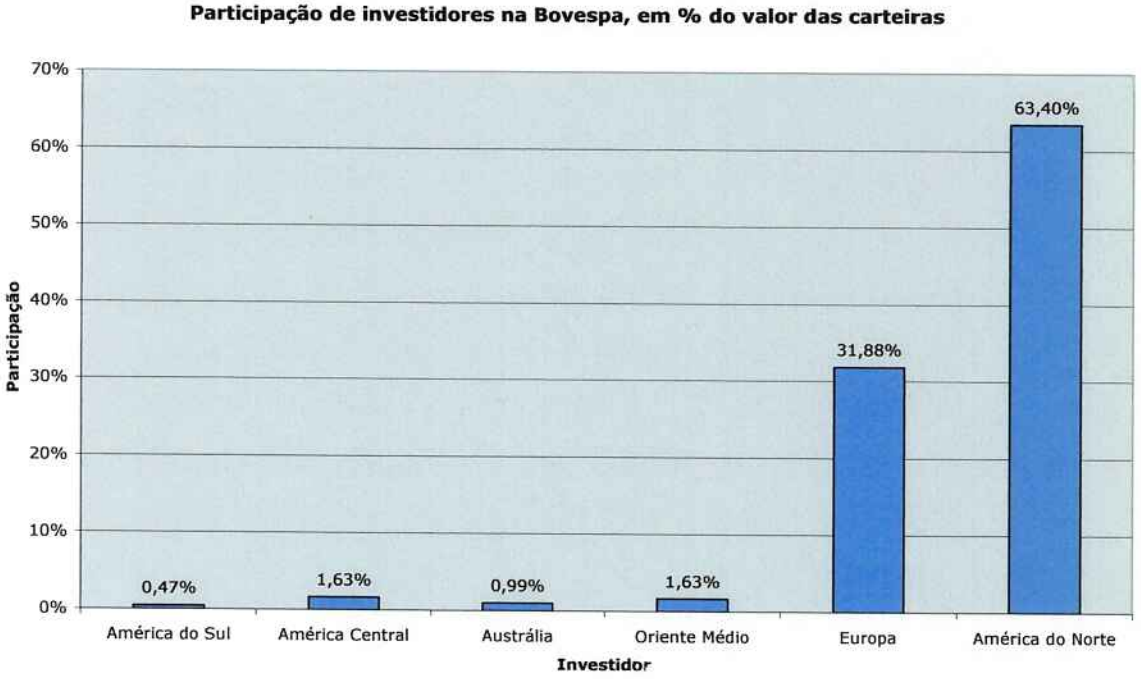

Figura 5.2 – Participação de investidores na BOVESPA, em % do valor das carteiras

5.2 PROGRAMAS DE INCENTIVO

A Bovespa está tentando aumentar o número de investidores pessoa física e/ou clubes de investimento atuantes na bolsa de valores e, para isto, criou um programa chamado "Bovespa Vai Até Você".

O projeto "Bovespa Vai Até Você" foi criado em maio de 2002 e ganhou impulso com o lançamento do primeiro clube de investimentos em 12 de setembro do mesmo ano. Com o objetivo de informar o maior número possível de brasileiros sobre o mercado de capitais, o projeto está dividido em programas diversificados para atender a públicos específicos:

- "Bovespa vai à Fábrica";
- "Bovespa vai à Universidade";
- "Bovespa vai às Academias de Tênis";
- "Bovespa vai aos Clubes";
- "Bovespa vai à Praia";
- "Bovespa vai ao Aeroporto";
- "Bovespa vai ao Metrô";
- "Bovespa vai às Barcas";
- "Bovespa vai Teatro";
- "Bovespa vai ao Conjunto Nacional"
- e também a outras cidades e estados, visitando empresas e participando de feiras e eventos diversos.

Em fevereiro desse ano, o lançamento do "Bovespa Vai Aos Municípios" estendeu o projeto também aos empresários com o objetivo de atrair novas companhias para a Bolsa. O programa percorreu o interior do estado de São Paulo com o suporte de um veículo equipado com material didático e equipamentos, que funciona como um escritório itinerante do "Bovespa vai até Você", o Bovmóvel. A primeira cidade visitada foi Jaú, entre 12 e 14 de fevereiro. Também foram visitadas São José do Rio Preto, em 19 e 20 de maio e Marília e Assis em junho e julho, respectivamente.

Dados do programa:

- De setembro de 2002 a abril de 2004 o "Bovespa vai até Você" já havia atingido mais de 122 mil pessoas;

- O número mensal de visitas ao site da bovespa saltou de 370 mil para mais de 1 milhão;
- 466 visitas foram feitas pelos promotores de negócios a grupos interessados em abrir clubes de investimento, representando mais de uma visita por dia útil no ano;
- 820 clubes de investimento criados, abrangendo grupos de pessoas de classes sociais e profissões diferenciadas como esportistas, donas-de-casa e estudantes universitários, comprovando o sucesso da campanha junto a novos investidores;
- O resultado refletiu-se na participação das pessoas físicas no volume financeiro da Bovespa, que subiu de 20,5%, em setembro de 2002, para 27%, em abril de 2004.

Dados de setembro de 2002 a fevereiro de 2003 da campanha "Bovespa Vai até você" [2]

Grande Procura	
Número de pessoas que contataram equipes da Bovespa para obter informações sobre o mercado	
Teatro	2.300
Site e telefone da Bovespa	6.953
Conjunto Nacional	6.400
Praias de São Paulo	9.688
Praias do Rio Grande do Sul	5.111
Total	30.452

Tabela II – Número de pessoas que contactaram Bovespa pedindo informações de mercado

O número dos clubes formados por jovens investidores cresceu também. A atração desse público jovem foi incentivada pelo sistema de negociação Home Broker pois a negociação ficou mais fácil e transparente. E, com as vantagens dos clubes, como custo menor, a presença dos jovens se ampliou ainda mais nos negócios com ações.

O projeto de popularização do mercado de ações abrange também o "Mulheres em Ação", com iniciativas voltadas para setores e segmentos femininos, e o "Bovespa Delivery", que conta com o suporte de uma van equipada com terminais de

computador e equipe de profissionais treinados que se desloca para o atendimento a pessoas interessadas em conhecer os conceitos básicos do mercado de capitais.

O programa Mulheres em Ação completa um ano de vida em 2004 com êxito crescente. O programa nasceu como parte de um projeto democratização do mercado, de ampliação da base acionária, que procura disseminar a cultura do investimento em ações. Abriu canais de relacionamento com a mulher, pelos quais fluem informação, educação e esclarecimento a respeito do papel e do funcionamento do mercado de capitais, tanto para o investidor como para a economia do País. O programa levou em consideração os dados atuais, onde reconhece a mulher como peça chave na sociedade moderna.

Há algum tempo, de cada dez investidores, apenas um era mulher. Após este programa, a participação feminina triplicou, elevando-se para três em cada dez investidores. Com isto o programa entra em uma nova fase, abrindo espaço para que as mulheres se expressem, revelando o apoio a este público de alto potencial, cada vez mais atuante na organização do orçamento familiar, na educação dos filhos e na gestão da própria carreira, mas que não investia em ações temendo o risco e por carência de informação, rumando desta forma para a caderneta de poupança.

Hoje em dia, a mulher é vista sob um novo conceito, o da "mulher transformadora" ou a "mulher protagonista", partícipe dessa grande revolução que ocorre no mercado de trabalho e na sociedade.

Um reflexo das campanhas pode ser notado no número de usuários que utilizam Home Broker para realizar suas transações. Mesmo o índice Bovespa caindo em anos anteriores, o que poderia afugentar investidores, o número de usuários foi crescente, principalmente em 2003 e 2004, anos em que os programas já estavam estabelecidos. No gráfico abaixo há uma relação entre o índice Bovespa e o número de usuários de Home Brokers:

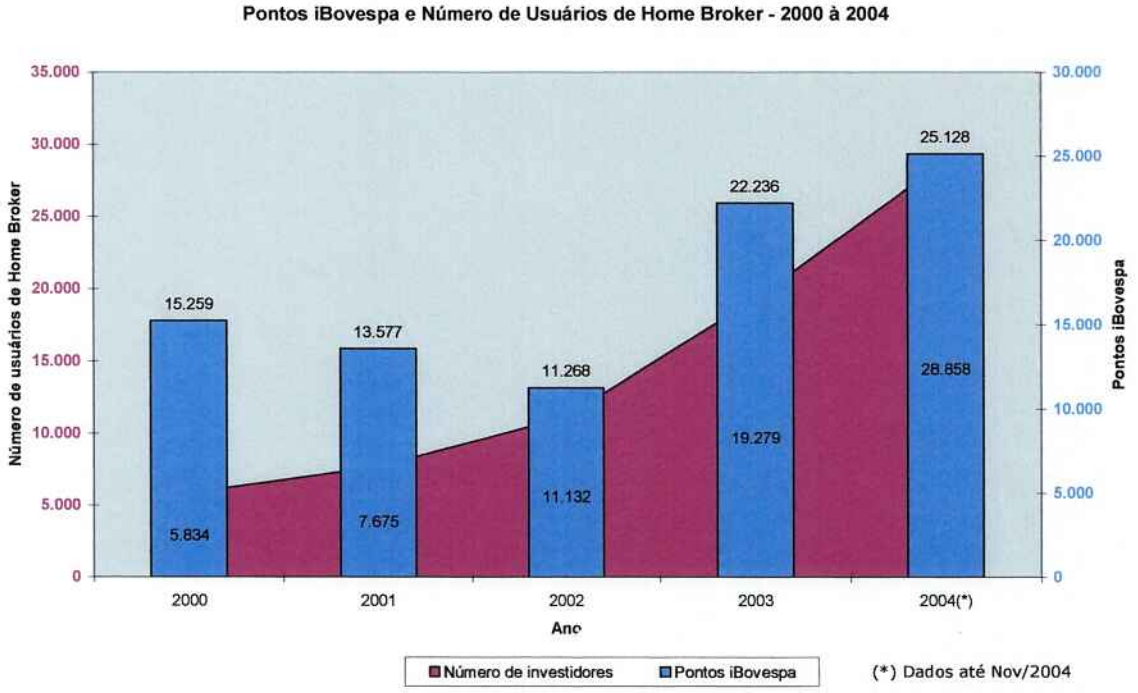

Figura 5.3 – Relação Índice Bovespa X Número de usuários de Home Broker entre 2000 e 2004

5.3 SOLUÇÃO POUCO EXPLORADA

A pouca informação que o público em geral tem é uma das grandes barreiras para sua entrada no mercado acionário. Fala-se muito em índices como iBovespa, Dow Jones, Nasdaq, Risco País, Taxa Selic, C-Bonds, mas tudo isso é muito nebuloso, afastando o investidor deste do mercado acionário e levando-o para portos teoricamente mais seguros como fundos de renda fixa e cadernetas de poupança.

O medo devido à desinformação afasta os usuários deste tipo de mercado. Isto reflete-se em diminuição do uso de Home Brokers, uma vez que esta é uma ferramenta muito utilizada por este público. No gráfico abaixo pode-se ver o comportamento dos usuários de acordo com o índice Bovespa:

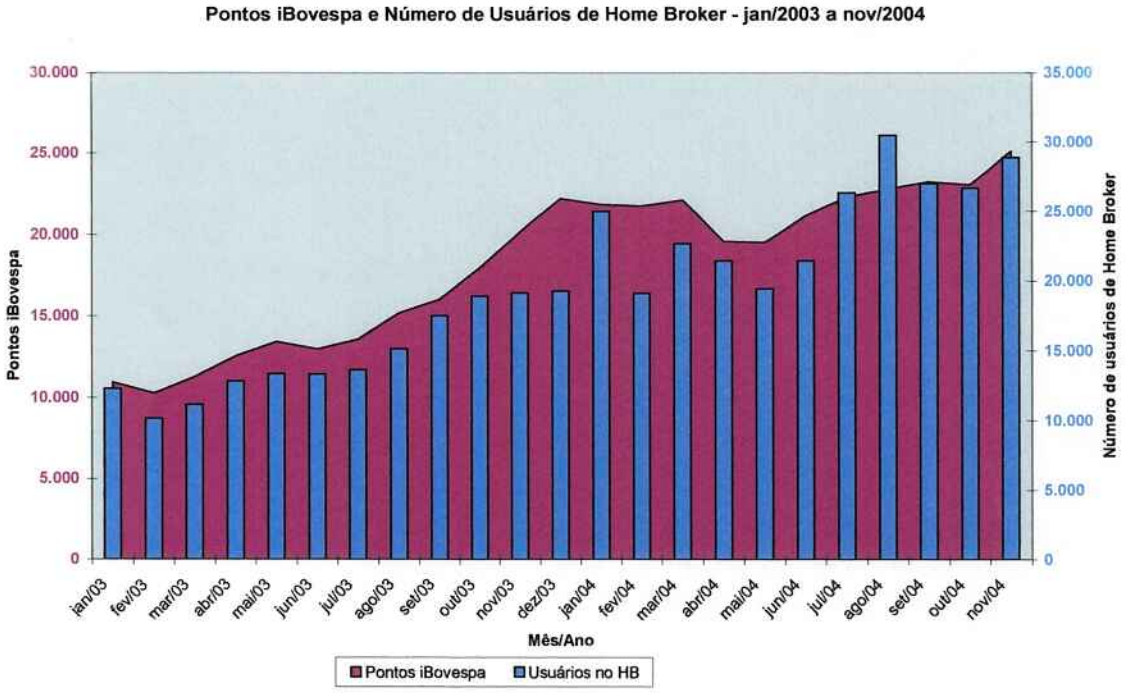

Figura 5.4 – Relação Índice Bovespa X Número de usuários de Home Broker entre 2003 e 2004

Felizmente este quadro tende a mudar, com os programas de incentivo aos novos investidores, difundindo mais o mercado acionário.

Pensando no aumento do número de pessoas física que podem vir a atuar neste ramo, a utilização de ferramentas que disponibilizem informações mais eficientes e precisas se faz necessária, dinamizando os processos de compra e vendas de papéis. Os Home Brokers são hoje a solução mais prática para o investidor que quer controlar sua carteira de ações sozinho, sem intermediários, podendo escolher as empresas nas quais pretende investir. Isso lhe dá poder de escolha e dinamiza o processo. Daí o aumento do número de usuários de Home Brokers. No gráfico abaixo pode-se ver o aumento do número de pessoas que utilizam os Home Brokers.

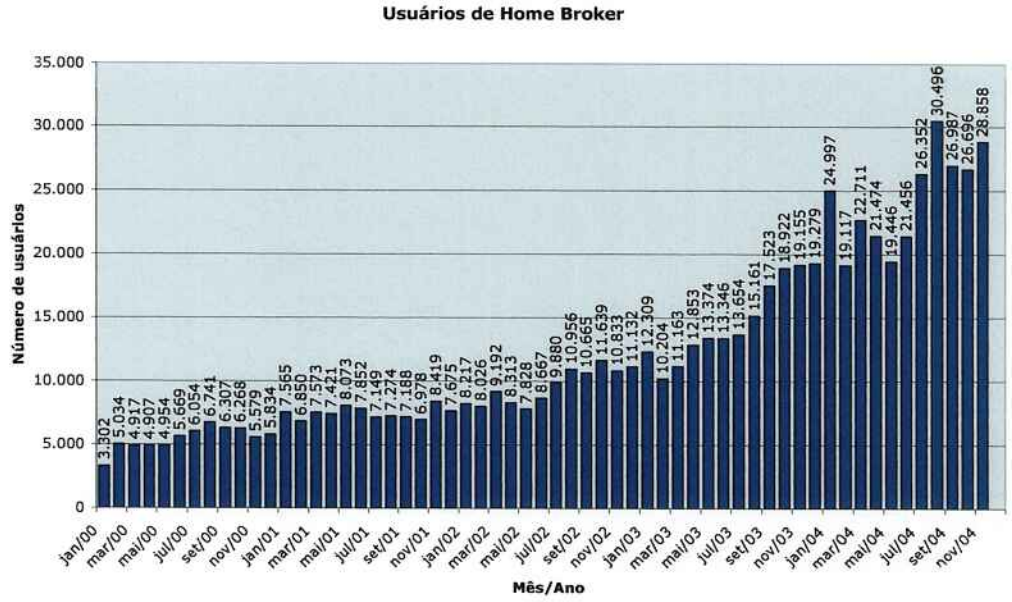

Figura 5.5 – Crescimento do Número de usuários de Home Broker entre jan/00 e nov/04

Com esta vantagem de tempo, fundamental para a atuação neste mercado, foi que veio a idéia de criar um sistema mais rápido e móvel que os próprios Home Brokers. O que o Mobile Broker pretende é encurtar o tempo entre o investidor pensar em comprar ou vender uma ação e de fato executar esta tarefa. A grande vantagem sobre os Home Brokers é a mobilidade, possível graças às novas tecnologias utilizadas.

6 ESPECIFICAÇÃO FUNCIONAL

6.1 ESCOPO DO SISTEMA

Um investidor que deseja aplicar seu dinheiro em ações deve primeiro procurar uma das corretoras de ações licenciadas e abrir uma conta. A partir daí, está habilitado a comprar e vender ações. A grande maioria destes investidores faz isso através dos sites das corretoras na internet, os chamados "Home Brokers". Após comprar a ação de uma empresa, este investidor deve estar atento às variações de mercado, isto é, deve estar sempre atualizado com as informações divulgadas pela empresa ou análises feitas por analistas especializados antes de tomar a decisão de vender ou comprar.

Este acompanhamento torna-se inviável caso o investidor não possa gastar grande parte de seu tempo atento às informações na Internet ou nos jornais. O sistema proposto visa atender às necessidades destes investidores que não têm tempo para manterem-se atualizados adequadamente.

O sistema previsto será implementado em dispositivos móveis como PDA's e celulares e manterá o investidor atualizado de informações relevantes sobre suas ações e poderá também enviar ordens de compra e venda rapidamente de qualquer lugar apenas estando conectado à Internet.

6.2 DEFINIÇÕES, SIGLAS E ABREVIATURA

WS - Web Service
MB - Mobile Broker
HB - Home Broker

6.3 PERSPECTIVAS DO PRODUTO

O Sistema Mobile Broker será projetado como parte de um sistema maior, os chamados Home Brokers. Serão implementadas algumas funcionalidades do HB necessárias para utilização do MB como Cadastro e Seleção de Ações. A figura abaixo ilustra o relacionamento entre o HB, o MB e o investidor:

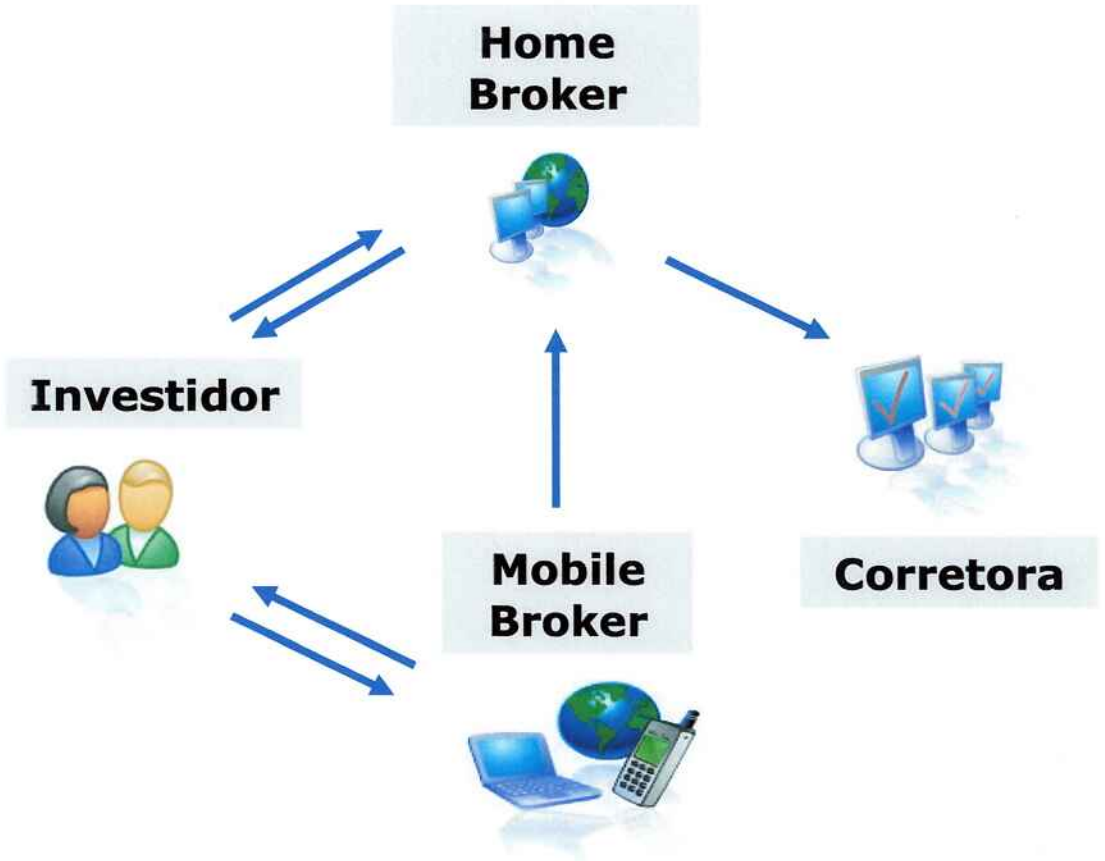

Figura 6.1 – Modelo do Sistema

6.4 INTERFACE COM O SISTEMA

Neste trabalho será feita a simulação do Home Broker através de um site que acessa um Web Service implementado em JAVA.

Neste mesmo Web Service também serão implementados os serviços que atenderão ao Mobile Broker.

6.5 INTERFACE COM O USUÁRIO

A interface do sistema MB com os usuários dos dispositivos móveis será feita utilizando a Tecnologia J2ME que pode ser utilizada tanto por celulares como por PALMs e Pocket PCs.

6.6 FUNÇÕES DO SOFTWARE

As funções do HB que serão implementadas serão:

- Inclusão/Exclusão de Clientes: cadastro dos clientes do sistema;
- Alteração de dados dos Clientes: alteração dos dados dos clientes cadastrados previamente no sistema;
- Captura das Cotações: dados das cotações negociadas na Bolsa de Valores de São Paulo. Estes dados deverão conter:
    - Oscilação;
    - Valor atual;
    - Valores Máximo e Mínimo atingido no dia e
    - Valores de Abertura e Fechamento do Mercado
- Seleção de Ações: o cliente selecionará quais ações deseja visualizar em seu dispositivo móvel e também que tipo de informação (recomendações e notícias);

As funções do MB são:

- Enviar ordens de compra e venda: o cliente enviará ordens de compra e venda de determinada ação. Estas ordens de compra podem não ser executadas imediatamente ou nem mesmo chegarem a ser executadas porque dependem de fatores de mercado;
- Visualização de Ações: o cliente poderá visualizar no HB os dados das ações previamente selecionadas;

6.7 CARACTERÍSTICAS DOS USUÁRIOS

Os usuários do sistema MB são "investidores moderados" de ações, ou seja, o investidor que tem interesse no mercado porém não quer, ou não pode, ficar o dia todo acompanhando informações de suas ações.

6.8 Restrições

Restrições para utilizar o Mobile Broker:

- O usuário deverá possuir um PDA que possua compatibilidade com aplicações em JAVA
- O usuário deverá ter acesso a uma rede ligada à internet.
- O PDA deverá possuir uma placa de rede wireless

Restrições para a utilização do Home Broker:

- Possuir um PC com acesso à internet e browser instalado

6.9 Modelo de Casos de Uso

6.9.1 Casos de Uso do Mobile Broker

Identificador: ELA

Nome: Exibe Lista Ações pré-selecionadas

Descrição: Sistema exibe lista de ações pré-selecionadas

Seqüência de eventos:

1. Investidor seleciona a opção "Exibir Ações" no menu inicial;
2. Sistema verifica as ações que o investidor pré selecionou;
3. Sistema mostra uma lista com as informações das ações(Código, Oscilação, Valor e Hora da Última Atualização)

Evento Iniciador: Investidor seleciona a opção "Exibir Ações" no menu inicial

Atores: Investidor

Pré-condição: usuário logado

Pós-condição: lista de ações exibida na tela

Extensões:

Investidor não tem ações pré-selecionadas: emite mensagem direcionando o investidor para utilizar o HB e selecionar ações desejadas.

Inclusões: não se aplica

Identificador: EDA

Nome: Exibe Dados da Ação

Descrição: Sistema dados da ação desejada

Seqüência de eventos:

1. Investidor seleciona a ação de uma lista;
2. Sistema mostra uma tela com os dados da ação selecionada e as opções de emitir ordem

Evento Iniciador: Investidor seleciona a ação de uma lista.

Atores: Investidor

Pré-condição: Ações listadas na tela (caso de uso ELA executado)

Pós-condição: tela de dados da ação exibida.

Extensões: não se aplica

Inclusões: caso de uso ELA

Identificador: EO

Nome: Envio de Ordem

Descrição: Investidor envia ordem de compra

Seqüência de eventos:

1. Investidor Selecione a ação na tela de Dados da Ação
2. Sistema exibe uma tela com os dados da ordem;
3. Investidor altera os dados da ordem
4. Usuário Seleciona a opção "Envia Ordem";
5. Uma tela de confirmação é exibida;
6. Investidor seleciona a opção "Confirma";

Evento Iniciador: Investidor seleciona a opção "Emitir Ordem" na tela de Dados da Ação

Atores: Investidor

Pré-condição: Tela de dados da ação exibida(caso de uso EDA executado);

Pós-condição: ordem de compra enviada com sucesso

Extensões:

(Passo 3) Investidor seleciona "Voltar" ao invés de "OK": volta para a tela de emissão de ordem de compra com os dados preenchidos

(Passo 6) Investidor seleciona "Cancelar" ao invés de "Confirma": volta para o menu principal

Inclusões: caso de uso EDA

6.9.2 Casos de Uso do Home Broker

Identificador: CAC

Nome: Cadastro de Cliente

Descrição: Cadastra o cliente para este poder utilizar os serviços disponibilizados pelo HB e MB.

Seqüência de eventos:

1. Investidor entra no site e seleciona opção de cadastro;
2. Sistema pede CPF do cliente;
3. Investidor insere dados solicitados;
4. Sistema verifica consistência dos dados e prossegue se dados estão corretos;
5. Sistema pede inserção dos dados cadastrais;
6. Investidor insere seus dados cadastrais como pedido na página;
7. Sistema verifica consistência dos dados (se investidor se CPF é válido, etc). Se dados estão OK, sistema apresenta-os e pede confirmação;
8. Investidor confirma os dados inseridos;
9. Sistema exibe tela de "Cadastro realizado com sucesso".

Evento Iniciador: Investidor seleciona no site opção de cadastro.

Atores: Investidor.

Pré-condição: Investidor acessou o site.

Pós-condição: Investidor cadastrado.

Extensões:

- (Passo 7) Dados do cliente não são consistentes (CFP, RG, etc). A mesma tela de cadastro é apresentada, com um indicador de erro.

Inclusões: Não se aplica

Identificador: ADC

Nome: Altera dados do Cliente

Descrição: Cliente entra nos seus dados cadastrais e altera-os de acordo com suas necessidades.

Seqüência de eventos:

1. Investidor entra no site e seleciona opção de alteração de cadastro;
2. Sistema pede CPF e senha do investidor;
3. Investidor insere dados solicitados;
4. Sistema verifica a consistência dos dados e prossegue se dados estão corretos;
5. Sistema exibe dados cadastrais;
6. Investidor altera seus dados;
7. Sistema verifica consistência dos. Se dados estão OK, sistema apresenta-os e pede confirmação;
8. Investidor confirma os dados inseridos;
9. Sistema exibe tela de "Cadastro alterado com sucesso".

Evento Iniciador: Investidor seleciona no site opção de alteração de cadastro.

Atores: Investidor.

Pré-condição: Investidor acessou o site.

Pós-condição: Dados cadastrais alterados com sucesso.

Extensões: análogo ao caso de uso CAC.

Inclusões: Não se aplica.

Identificador: CCC

Nome: Cancela Cadastro de Cliente

Descrição: Cliente cancela o seu cadastro pois não deseja mais utilizar os serviços do HB nem do MB.

Seqüência de eventos:

1. Investidor entra no site e seleciona opção de cancelar cadastro;
2. Sistema pede CPF e senha do investidor;
3. Investidor insere dados solicitados;
4. Sistema verifica veracidade dos dados e prossegue se dados estão corretos;
5. Sistema pergunta se cliente realmente deseja cancelar seu cadastro.

6. Sistema exibe tela de "Cadastro cancelado com sucesso".

Evento Iniciador: Investidor entra no site e seleciona opção de cancelar cadastro.

Atores: Investidor.

Pré-condição: Investidor acessou o site.

Pós-condição: Cadastro cancelado com sucesso.

Extensões:

- (Passo 4)Dados do cliente não são consistentes (CFP, RG, etc). A mesma tela de cadastro é apresentada, com os dados já digitados mas com os campos em que os dados errados foram digitados já em branco e com um indicador de erro do lado.

Inclusões: Não se aplica.

Identificador: SEA

Nome: Seleções das ações

Descrição: Investidor seleciona as ações que quer saber notícias.

Seqüência de eventos:

1. Investidor acessa o site e seleciona opção 'Seleção de ações";
2. Sistema apresenta todas as ações disponíveis;
3. Investidor Seleciona as ações desejadas
4. Sistema mostra ações selecionadas e pede confirmação;
5. Investidor confirma seleção
6. Sistema mostra tela com mensagem "Seleção cadastrada com sucesso".

Evento Iniciador: Investidor acessa o site e seleciona opção "Seleção de ações".

Atores: Investidor.

Pré-condição: Investidor acessa o site.

Pós-condição: Ações selecionadas de acordo opções do investidor.

Extensões:

Inclusões: Não se aplica.

Identificador: ENC

Nome: Captura das cotações das ações

Descrição: Sistema captura cotações das ações que fazem parte da Bolsa de valores.

Seqüência de eventos:

1. Sistema verifica se há cotações mais atualizadas;
2. Sistema atualiza cotações;
3. Sistema disponibiliza cotações no site.

Evento Iniciador: Sistema verifica se há cotações mais atualizadas.

Atores: Sistema

Pré-condição: Sistema verificando se há cotações mais atualizadas.

Pós-condição: Cotações atualizadas com sucesso.

Extensões:

- (Passo 1) Se o sistema de fornecimento de cotações não estiver disponível, as cotações não serão recebidas. Como resultado, as cotações não serão atualizadas

Inclusões: Não se aplica.

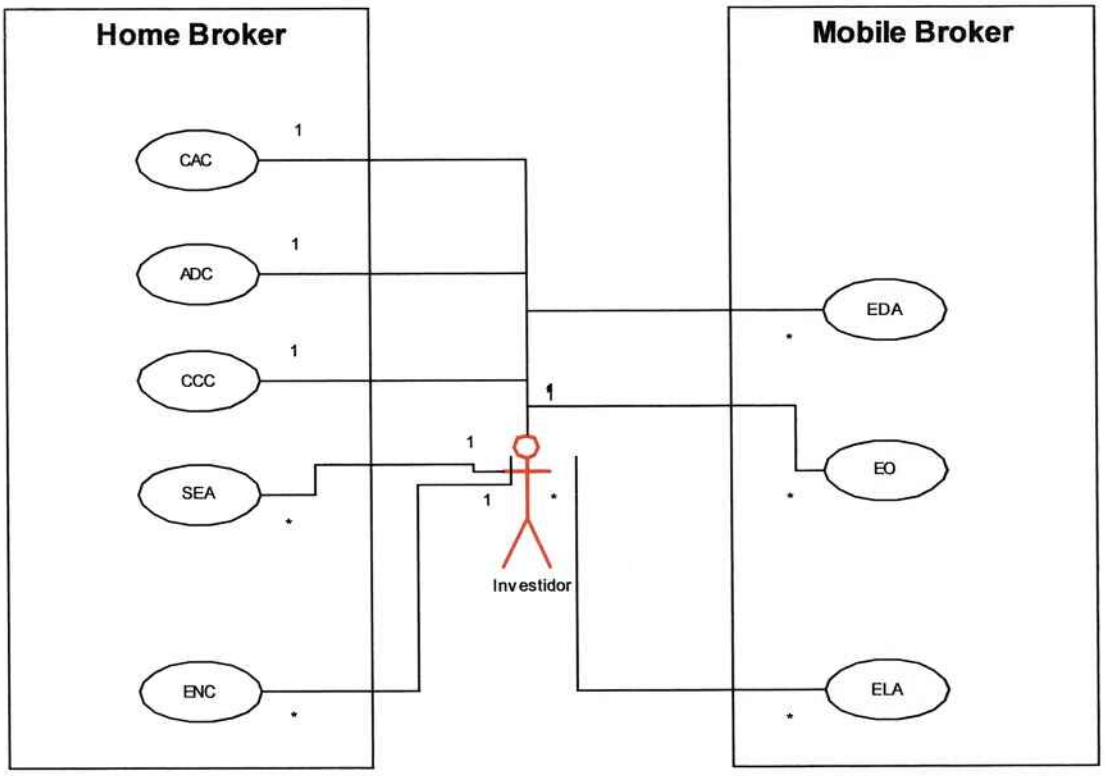

Figura 6.2 – Diagrama de Casos de Uso

7 TECNOLOGIAS UTILIZADAS

Uma das grandes motivações do grupo para a realização deste projeto de formatura era a utilização de tecnologias não conhecidas pelos integrantes, aumentando o valor agregado pelo projeto ao nosso conhecimento.

Neste capítulo serão apresentadas as principais tecnologias utilizadas no desenvolvimento, destacando as suas vantagens e funcionalidades.

7.1 WEB SERVICES

Uma boa definição do que é um Web Service foi publicada pela IBM: "Web Services é um novo conceito para aplicações Web. Ela permite o desenvolvimento de aplicações modulares, auto descritas que podem ser publicadas, localizadas, e invocadas através da web. Web Services provê funções que vão desde uma simples requisição até um complicado processo de negócio."

Este middleware necessita ainda de um modelo de transação estendida que construa padrões sobre Web Services e defina um protocolo de transação interoperável e fluxos de mensagens para auxiliar a negociação de garantias da transação.

Os seguintes padrões estão relacionados com Web Services [1]:

- BTP (Business Transaction Protocol): estabelecido para garantir o atendimento o atendimento dos requerimentos de longas aplicações colaborativas (mas mesmo assim é otimizado), através de um relaxamento das tradicionais propriedades do ACID (atomicidade, consistência, isolamento e duração) na maneira de controle específica do Web Service;
- Propriedades ACID sobre transações;
- XML para codificação de mensagens;
- SOAP (Simple Object Access Protocol) sobre HTTP1.1
- Business Transactions: mudança consistente no estado de relação de negócio entre as partes;

[1] LITTLE M., Transaction and Web Service – Communication of ACM, v46 n10 Outubro de 2003

- Transações atômicas: garantem consistência na presença de falhas;
- ACID (Atomicity, Consistency, Isolation e Durability): garantem que a consistência de estado seja preservada, independente de acessos concorrentes e falhas.

É importante ressaltar aqui o padrão SOAP, que é a base para a utilização do Web Service. Consiste de um padrão para troca de informações em ambientes descentralizados e distribuídos. É baseado em XML e consiste em três partes: Um envelope que define o framework para descrever o que tem na mensagem e como processá-la, um grupo de regras para expressar instancias de tipos definidos na aplicação e convenções para representar processos remotos de "calls" e "responses". A implementação deste padrão utilizada no projeto foi o Apaxe Axis 1.2

7.2 HIBERNATE

A primeira questão levantada no desenvolvimento foi um método de acesso ao banco de dados que provesse um acesso fácil e com alto grau de reutilização. A solução adotada foi o Hibernate. Uma ferramenta criada pelo australiano Gavin King e logo adotada pelo mercado devido às dificuldades de utilização dos entity beans. Logo depois esta ferramenta foi adotada e financiada pelo Jboss Group, a empresa criadora do servidor de aplicações Jboss. Atualmente o Hibernate é um software de código aberto suportado pela licença LGPL, que permite a utilização de graça do software até por projetos comerciais.

Hibernate é uma ferramenta que realiza a persistência de objetos em banco de dados relacionais. Permite que o desenvolvedor crie classes persistentes seguindo a linguagem java, incluindo associação, polimorfismo, herança e todo o framework JAVA[2]. O *Hibernate Query Language* permite que sejam realizadas consultas utilizando código SQL nativo ou critérios baseados em JAVA.

A seguir é apresentado um exemplo de uma consulta realizada a uma base de dados utilizando código JAVA:

```
Acao example = new Acao();
example.setCodigo(1);
```

[2] FONTE: www.hibernate.org

```
find(Filter.createFilter(example), codigo);
```

Neste exemplo está sendo feita uma consulta à tabela Ação em todos os registros com código 1. A classe Filter é uma classe que auxilia a criação de filtros para a consulta. Esta classe, assim como as demais classes utilizadas no acesso, estão detalhada mais adiante neste documento.

7.3 XDOCLET

Xdoclet é um gerador de código também de código aberto. A utilização desta ferramenta juntamente com o Hibernate trouxe ao projeto um enorme ganho de produtividade pois gerava automaticamente, através de uma tarefa previamente desenvolvida, arquivos que mapeavam as classes persistentes e também criava e rodava os scripts de atualização para qualquer base de dados.

Através da utilização do Xdoclet, também foi criada uma tarefa que atualizava a nova versão no servidor de forma rápida e fácil.

7.4 JAVA 2 PLATAFORM, MICRO EDITION (J2ME)

O J2ME é uma plataforma robusta, flexível para aplicações que rodam em dispositivos móveis como celulares, PDAs e *TVs set-top boxes*. J2ME inclui uma java virtual machine e uma gama de APIs Java definidas no *Java Community Process*, que inclui membros de empresas de fabricação destes dispositivos, vendedores de software e provedores de serviço.

J2ME inclui uma flexível interface de usuário, um modelo robusto de segurança, uma grande gama de protocolos de rede e um extenso suporte para aplicações offline que podem ser baixadas dinamicamente e aplicações em rede. A especificação J2ME foi escrita para uma enorme variedade de dispositivos e explora todas as capacidades dos mesmos.

Para utilizar esta plataforma, é necessária uma máquina virtual, que fornece funcionalidades básicas como conectividade em rede e gerenciamento de memória. Atualmente existem duas configurações J2ME: a Connected Limited Device Configuration (CLDC) e a Connected Device Configuration (CDC).

O J2ME pode ser estendido, utilizando-se dos pacotes opcionais que podem ser incluídos tanto no CLDC quanto no CDC. Criados para aplicações específicas, os pacotes opcionais fornecem às configurações básicas outras funcionalidades existentes e novas tecnologias como acesso à banco de dados, comunicação wireless, multimídia, bluetooth e web services. Estes pacotes opcionais são modulares fazendo com que as aplicações não carreguem funcionalidades não utilizadas.

No projeto foram utilizadas os pacotes opcionais MMAPI que disponibilizam funcionalidades multimídia e também o pacote J2MEWS que fornece acesso aos web services. A utilização destes pacotes está descrita mais adiante neste documento.

7.5 J2ME Web Services

Desenvolvido pelo Java Community Process, o JSR 172, ou J2ME Web Services API (WSA) é um dos pacotes adicionais mencionados anteriormente e utilizado na comunicação entre o Mobile Broker e o Web Service.

WSA foi desenhado para trabalhar com configurações J2ME baseadas tanto em CDC como CLDC. Esta API é baseada em algumas partes do Java API for XML-based RPC (JAX-RPC) com algumas classes de invocação remota (RMI) incluídas para satisfazer dependências do JAX-RPC. A API para realizar a leitura do XML é baseada na API para XML versão 2 (SAX2).

O objetivo da WSA é integrar chamadas à Web Services e tradução de XML em dispositivos móveis, para que os desenvolvedores não tenham que criar esta funcionalidade em cada aplicação que for desenvolvida.

JSR 1723 é um padrão para o lado cliente que utiliza tecnologia J2ME consumir serviços remotos em um Web Service comum.

---

[3] Java Community Process, JSR 172: J2ME Web Services Specification, Março de 2004

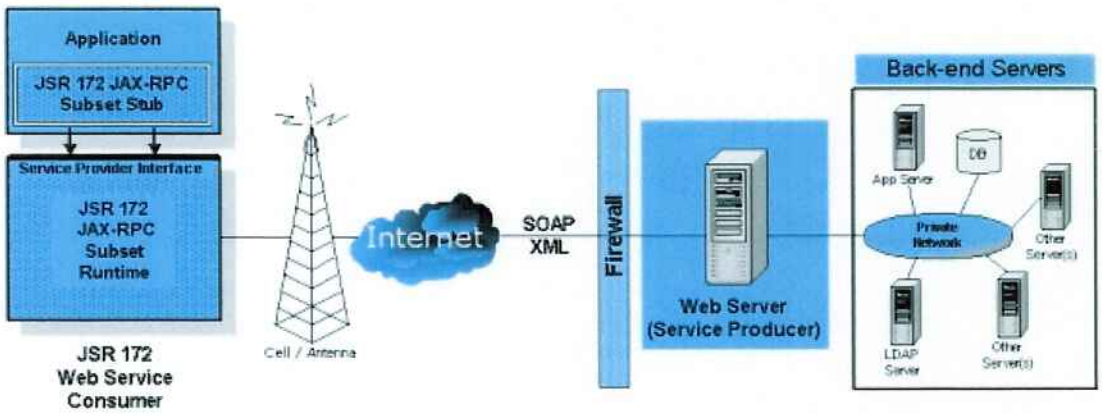

Figura 7.1 – J2ME Web Service em uma típica arquitetura de Web Service

7.6 JSR135 Mobile Media API (MMAPI).

Para que seja possível adicionar os recursos multimídia no sistema, é necessário levar em consideração todas as restrições percebidas, em relação aos dispositivos móveis utilizados (como os celulares e PDA's).

Como é possível observar, esses são dispositivos com recursos muito limitados, e por isso, temos que adotar uma solução que seja compatível com os mesmos.

Para isso, utilizaremos outro pacote adicional ao J2ME, JSR135 Mobile Media API[4] (MMAPI). Essa API estende as funcionalidades da plataforma J2ME oferecendo suporte multimídia (como áudio e vídeo) aos dispositivos com problemas de capacidade como os dispositivos móveis.

Para acomodar essas diversas configurações e capacidade de processamento de multimídia para dispositivos móveis, é necessário um alto nível de abstração.

As principais funcionalidades dessa API são:

- Oferece suporte a qualquer conteúdo de vídeo e áudio, oferecendo ferramentas para controle de fluxo do stream da mídia;
- Ênfase nas restrições de memória, estabelecendo limite pequeno para o consumo de memória;
- Possibilidade de separar um subconjunto da API para suportar apenas alguns tipos de mídia, como somente áudio, por exemplo, podendo

[4] Java Community Process, JSR 135: Mobile Media API, Junho de 2003

assim adaptar-se a dispositivos que não suportam todos recursos oferecidos pela API completa;

- Facilidade em adicionar novas funcionalidades à API;
- Permite flexibilidade na implementação, ou seja, permite que nem todas as funcionalidades sejam implementadas;
- Deve-se levar em consideração que para alguns tipos de mídia, algumas características são obrigatórias. outras recomendadas e outras totalmente opcionais.

A API foi desenvolvida para ser compatível com as configurações CDC e CLDC.

8 CONCEITOS DE SEGURANÇA

Ao pensar sobre sistemas de informação, transações online, ou qualquer outro tópico que envolva a transmissão de dados sigilosos por uma rede de computadores, uma questão que está diretamente interligada com esses assuntos é a segurança da informação.

Não é possível pensar na realização de operações bancárias, através de qualquer computador acessando a Internet, sem se preocupar com a segurança disponibilizada pelos bancos para tais operações.

No caso deste projeto, com informações sigilosas sendo trocadas pela rede, não poderia ser diferente.

O usuário recebe dados sigilosos, como cotações das ações em tempo real, confirmações de ordens de compra e venda de ações, em seu dispositivo móvel, através da rede Wireless, e envia dados sigilosos para os servidores, como ordens de compra e venda, e seus respectivos valores.

Com isso, é necessário garantir ao usuário que todas as informações serão devidamente protegidas, e que a comunicação é a mais segura possível. Uma falha na segurança da informação acarretaria na perda da credibilidade do sistema, e conseqüentemente no fracasso do projeto. E é por isso, que a questão da segurança da informação é um dos pontos chaves do projeto.

A segurança será aplicada à conexão do usuário com o sistema, e à comunicação entre o cliente e servidor através de um canal seguro. Este canal será encarregado de cuidar da parte da criptografia das mensagens trocadas entre cliente e servidor diminuindo os riscos envolvidos na transmissão de informações sigilosas.

A segurança da informação é a proteção do sistema contra a negação de serviço aos usuários autorizados, assim como contra a proteção contra intrusos, e modificações não autorizadas de dados ou informações, armazenadas, em processamento e transmissão. Trata-se de prevenir, detectar e deter eventuais ameaças ao sistema.

Para garantir a segurança da informação é necessário garantir princípios básicos como confidencialidade, disponibilidade, integridade, autenticidade, não-repúdio, legalidade e privacidade.

8.1 CONFIDENCIALIDADE

A confidencialidade, ou sigilo, é a propriedade de certas informações que não podem ser disponibilizadas ou divulgadas sem autorização para pessoas, entidades ou processos. Refere-se ao conceito de garantir a divulgação da informação confidencial, limitada para um grupo apropriado de pessoas ou organizações.

Ou seja, através da confidencialidade, garante-se que apenas o nosso sistema é capaz de reconhecer, decifrar, as informações confidenciais enviadas através da rede pelos nossos clientes.

8.2 DISPONIBILIDADE

A disponibilidade pode se referir à capacidade de acesso de um sistema de computadores ou recursos de rede.

Um sistema possui uma alta disponibilidade quanto maior for a capacidade de prover acesso ao usuário no momento em que o mesmo solicitar os recursos do sistema.

No que diz respeito à segurança, disponibilidade refere-se à propriedade da informação ser entregue à pessoa correta no momento em que ela precisar.

8.3 INTEGRIDADE

A integridade é uma propriedade que assegura que qualquer modificação indevida nos dados transmitidos pela rede seja detectada.

Garantindo a integridade do sistema, garante-se que as informações enviadas por ele ao sistema estão protegidas contra modificações não autorizadas. Ou seja, as informações recebidas e aceitas pelo sistema, não foram modificadas por terceiros durante o tráfego pela rede.

8.4 AUTENTICIDADE

A autenticidade refere-se à propriedade do sistema de verificar e confirmar a identidade do usuário, para permitir o acesso aos recursos do sistema.

Esse conceito de autenticidade abrange também o aspecto de garantir de forma indubitável a autoria das informações trafegadas pela rede.

8.5 NÃO-REPÚDIO

O não-repúdio, ou não recusa, é a garantia que o emissor de uma mensagem ou a pessoa que executou determinada transação de forma eletrônica, não poderá posteriormente negar sua autoria.

8.6 LEGALIDADE

A legalidade é uma propriedade que garante que a informação utilizada, está de acordo com as leis em vigor.

8.7 PRIVACIDADE

A privacidade refere-se à implementação de condições apropriadas para garantir a segurança e a confidencialidade de informações, assim como para protegê-las contra vazamentos indevidos que possam resultar em embaraços ou qualquer outro tipo de constrangimentos para as pessoas.

Com isso, garante-se aos usuários que os dados fornecidos aos sistemas, e todas as informações trocadas durante as transações serão utilizadas apenas pelo sistema, e não serão divulgadas para pessoas, ou sistemas não autorizados.

Antes da solução de segurança escolhida para ser implementada no sistema ser apresentada, é necessário que sejam explicados e apresentados alguns conceitos e definições sobre segurança.

Assim, pretende-se que quando a solução for descrita posteriormente, os conceitos envolvidos e utilizados na mesma já estejam compreendidos, e já tenham sido abordados nesse documento.

Por isso, os próximos itens desse documento apresentarão conceitos sobre criptografia, SSL (Secure Sockets Layer) e segurança XML.

9 CRIPTOGRAFIA

A palavra criptografia tem sua origem no Grego: kryptos significa oculto, envolto, escondido, secreto; graphos significa escrever, grafar.

A criptografia é uma ciência que tem um papel fundamental para a segurança da informação, pois serve de base para diversas tecnologias e protocolos. Possui certas propriedades como confidencialidade, integridade, autenticação e não-repúdio, já abordadas nesse documento, e garante o armazenamento, as comunicações e transações seguras, de grande importância e relevância ao âmbito do projeto do sistema de compra e venda de ações.

Sobre o papel da criptografia, pode-se dizer que ela possui funções e importância fundamentais no que diz respeito às soluções de segurança das organizações. A função primária da criptografia é a de garantir a confidencialidade das informações envolvidas no sistema, mas também pode ser responsável pela integridade, autenticação, certificação e não-repúdio.

Terminologias:

- Cifrar: é o ato de transformar dados em alguma forma ilegível. Seu propósito é garantir a privacidade, mantendo a informação escondida, ilegível a qualquer pessoa não autorizada, mesmo que a mesma consiga visualizar os dados criptografados.

- Decifrar: é o processo inverso, ou seja, transformar os dados criptografados na sua forma original, inteligível.

Para cifrar ou decifrar uma mensagem são necessárias informações confidenciais geralmente denominadas chaves ou senhas. Dependendo do método de criptografia empregado, a mesma chave pode ser utilizada tanto para criptografar como para decriptografar mensagens, enquanto outros mecanismos utilizam senhas diferentes para os dois processos.

O número de chaves possíveis depende do tamanho (número de bits) da chave. Por exemplo, uma chave de 8 bits permite uma combinação de no máximo 256

chaves (28). Quanto maior o tamanho da chave mais difícil quebrá-la, pois o número de combinações é maior.

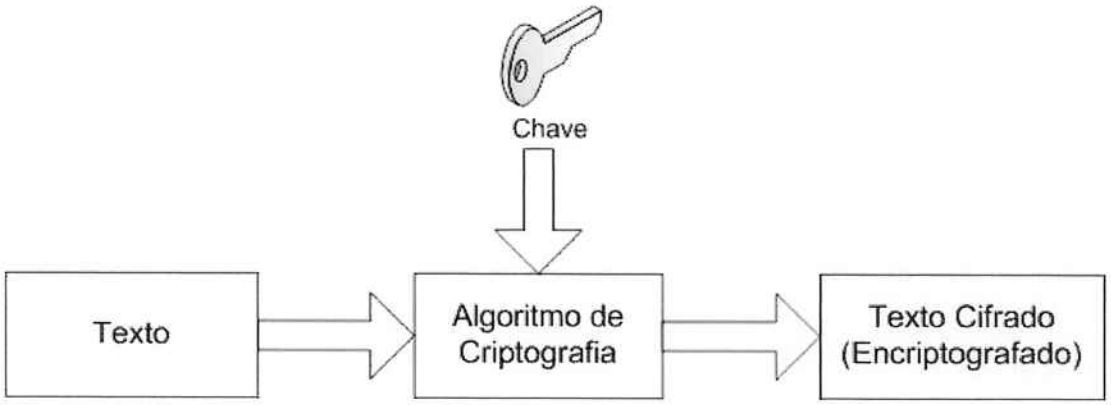

Figura 9.1 – Criptografia de Texto

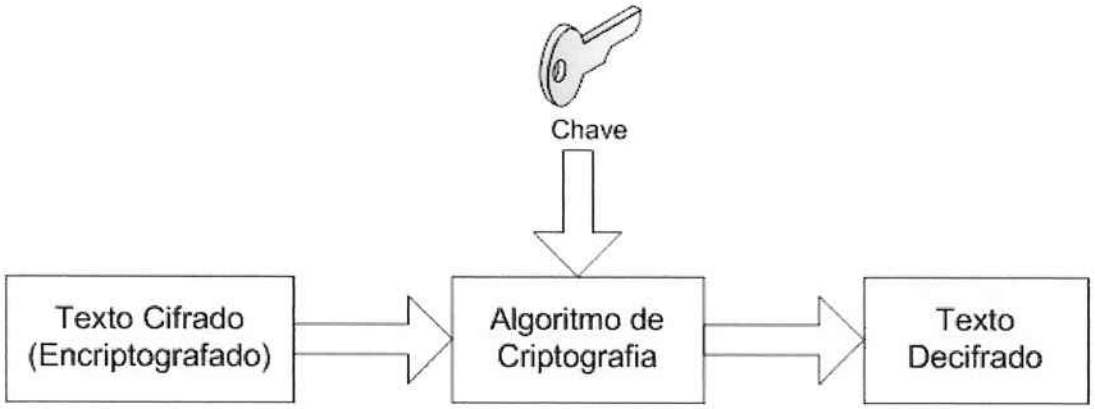

Figura 9.2 – Decriptografia de Texto

Como citado anteriormente, os algoritmos de criptografia podem utilizar a mesma chave para cifrar e decifrar a informação, ou utilizar chaves diferentes para cada um dos processos.

Quando a chave utilizada para cifrar é a mesma que a chave para decifrar, os algoritmos de criptografia são denominados simétricos. E quando são utilizadas chaves diferentes, os algoritmos são denominados assimétricos.

9.1 Criptografia Simétrica

A criptografia simétrica, como dito anteriormente, refere-se aos algoritmos de criptografia que utilizam a mesma chave tanto para cifrar, como decifrar as informações.

Os algoritmos simétricos incluem duas variáveis: criptografia de bloco e criptografia de stream.

A criptografia de bloco, cifra um texto na forma de um bloco de tamanho definido. O tamanho do bloco é relacionado com o algoritmo específico e o tamanho da chave utilizada. Criptografia de blocos é muito comum, e oferece suporte à criptografia de XML.

Criptografia de stream é um pouco diferente, e baseia-se em uma função de derivação da chave para gerar uma stream da mesma. Então é utilizada uma operação XOR (OU-Exclusivo), entre cada byte do texto a ser criptografado e cada byte da stream da chave, de modo a gerar o texto cifrado, criptografado.

As criptografias de stream, geralmente são mais rápidas e menores para implementar em relação aos algoritmos de criptografia de bloco, porém possuem um revés, no que diz respeito à segurança. Se uma mesma stream da chave for reutilizada, certos tipos de ataques utilizando apenas o texto cifrado podem revelar informações a respeito do texto original. E, embora a criptografia de XML tenha suporte para criptografia de stream, não há nada especificado atualmente.

Atualmente os dois algoritmos de criptografia simétrica de blocos mais utilizados na criptografia de XML são: Triple-DES e AES.

O conceito da chave simétrica pode ser reduzido a uma string de byte do tamanho apropriado. Qualquer string formada por um conjunto de bytes é uma chave simétrica apropriada do ponto de vista matemático. Isso quer dizer que não há restrições quanto a semântica dessa cadeia de bytes.

Algo que deve ser levado em consideração, no entanto, diz respeito ao modo como esses bytes da chave simétrica devem ser escolhidos.

Chaves simétricas devem ser derivadas de uma fonte randômica de informação. Se um hacker puder, de alguma maneira, reproduzir a geração da chave simétrica, a proteção oferecida pela criptografia é nula, já que a chave passa a ser conhecida.

É importante entender que os números gerados por programas de computador nunca são randômicos, e sim pseudo-randômicos. A razão disso é que o computador é consiste em uma grande máquina de estados, e retornando o computador para o estado apropriado, o número randômico correspondente pode ser reproduzido. Devido a esse fato que os números gerados por computadores não podem ser considerados randômicos.

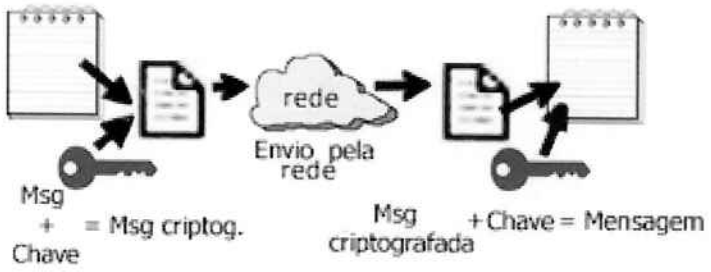

Figura 9.3 – Criptografia Simétrica

Vantagens e desvantagens da utilização de chaves simétricas:

- Vantagem - Rapidez na criptografia e decriptografia das informações.
- Desvantagem - A chave secreta deve ser transmitida ou comunicada para o receptor, tornando-a mais vulnerável a roubo.

Exemplos de Algoritmos Simétricos:

Algoritmo Simétrico	**Bits**	**Descrição**
DES	56	O Data Encryption Standard (DES) é o algoritmo simétrico mais disseminado no mundo. Foi criado pela IBM em 1977 e, apesar de permitir cerca de 72 quadrilhões de combinações (2^{56}), seu tamanho de chave (56 bits) é considerado pequeno, tendo sido quebrado por "força bruta" em 1997 em um desafio lançado na Internet.
Triple-DES	112 ou 168	O 3DES é uma simples variação do DES, utilizando-o em três ciframentos sucessivos, podendo empregar um versão com duas ou com três chaves diferentes. É seguro, porém

		muito lento para ser um algoritmo padrão.
IDEA	128	O International Data Encryption Algorithm foi criado em 1991 por James Massey e Xuejia Lai e possui patente da suíça ASCOM Systec. O algoritmo é estruturado seguindo as mesmas linhas gerais do DES. Mas na maioria dos microprocessadores, uma implementação por *software* do IDEA é mais rápida do que uma implementação por *software* do DES. O IDEA é utilizado principalmente no mercado financeiro e no PGP, o programa para criptografia de e-mail pessoal mais disseminado no mundo.
Blowfish	32 a 448	Algoritmo desenvolvido por Bruce Schneier, que oferece a escolhe entre maior segurança ou desempenho através de chaves de tamanho variável. O autor aperfeiçoou-o no Twofish, concorrente ao AES.
RC2	8 a 1024	Projetado por Ron Rivest (o R da empresa RSA Data Security Inc.) e utilizado no protocolo S/MIME, voltado para criptografia de e-mail corporativo. Também possui chave de tamanho variável. Rivest também é o autor do RC4, RC5 e RC6, este último concorrente ao AES.
AES	128 ou 192 ou 256	Algoritmo é o novo padrão de criptografia simétrica utilizado inclusive pelo governo dos EUA. O AES é o algoritmo de criptografia de bloco Rijndael, e especifica um bloco de tamanho de 16 bytes, e três alternativas para o tamanho da chave 128,192 e 256 bits.

Tabela III – Algoritmos Simétricos de Criptografia

9.2 Criptografia Assimétrica

Algoritmos de criptografia assimétricos (ou algoritmos de chave pública) são aqueles que utilizam chaves diferentes para criptografia e decriptografia das informações. Assim, entram em contraste com os algoritmos de criptografia simétricos que utilizam a mesma chave para ambos os processos.

Nesses algoritmos assimétricos, as chaves utilizadas na criptografia das mensagens, tornam-se totalmente inúteis na decriptografia da mesma.

O algoritmo de criptografia assimétrico mais comum, e mais utilizado é o RSA. Esse algoritmo é também um dos únicos atualmente especificados nos padrões de segurança XML.

Para exemplificar a utilização de chaves assimétricas, usualmente é utilizado o caso: Alice, Bob e Eve. Alice deseja enviar uma mensagem para Bob, mas não quer que ninguém intercepte ou decifre sua mensagem. A solução é a seguinte, cada um dos pontos da transmissão da mensagem (Alice e Bob) deve gerar um par de chaves. Portanto, Alice deve gerar um par de chaves matematicamente relacionadas entre si, e o mesmo acontecendo com Bob. Desse par de chaves, uma delas deve ser utilizada na criptografia das mensagens, sendo denominada chave pública, e outra apenas para a decriptografia das mensagens, chamada chave privada. A chave privada deve ser mantida em segredo, e somente o possuidor dessa chave consegue decifrar as mensagens enviadas a ele. Já a chave pública não deve ser mantida em segreda e deve ser acessível para que outras pessoas consigam criptografar mensagens e enviá-las ao possuidor da chave privada correspondente a essa chave pública. Portanto, para Alice transmitir a mensagem para Bob, ela utilizará a chave pública de Bob para criptografar a mensagem e depois enviá-la. Mesmo que Eve possua a chave pública de Bob, e consiga interceptar a mensagem de Alice, Eve não conseguirá decifrar a mensagem, pois não possui a chave privada de Bob, que é a única capaz de realizar a decritpografia. Quando a mensagem chegar para Bob, ele utilizará sua chave privada, e assim, conseguirá decifrar a mensagem enviada por Alice.

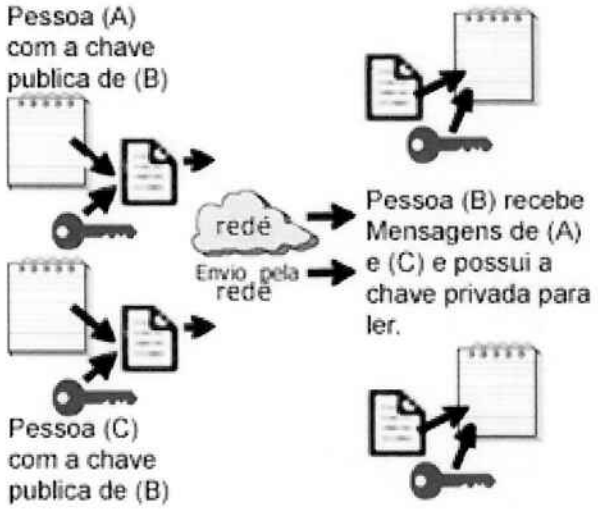

Figura 9.4 – Criptografia Assimétrica

Vantagens e desvantagens da utilização de chaves simétricas:

- Vantagens - mais seguras que a criptografia simétrica, por não precisar comunicar ao receptor a chave necessária para decriptografar a mensagem, e pode ser utilizada em assinatura digital
- Desvantagem – a geração de chaves pode ser muito demorada, e operações envolvendo chaves assimétricas são muito lentas em comparação com operações similares envolvendo chaves simétricas

Exemplos de Algoritmos Assimétricos:

Algoritmo	**Descrição**
RSA	O RSA é um algoritmo assimétrico que possui este nome devido a seus inventores: Ron Rivest, Adi Shamir e Len Adleman, que o criaram em 1977 no MIT. É, atualmente, o algoritmo de chave pública mais amplamente utilizado, além de ser uma das mais poderosas formas de criptografia de chave pública conhecidas até o momento. O RSA utiliza números primos. A premissa por trás do RSA é que é fácil multiplicar dois números primos para obter um terceiro número, mas muito difícil recuperar os dois primos a partir daquele terceiro número. Isto é conhecido como *fatoração*. Por

	exemplo, os fatores primos de 3.337 são 47 e 71. Gerar a chave pública envolve multiplicar dois primos grandes; qualquer um pode fazer isto. Derivar a chave privada a partir da chave pública envolve fatorar um grande número. Se o número for grande o suficiente e bem escolhido, então ninguém pode fazer isto em uma quantidade de tempo razoável. Assim, a segurança do RSA baseia-se na dificuldade de fatoração de números grandes. Deste modo, a fatoração representa um limite superior do tempo necessário para quebrar o algoritmo. Uma chave RSA de 512 bits foi quebrada em 1999 pelo Instituto Nacional de Pesquisa da Holanda, com o apoio de cientistas de mais 6 países. Levou cerca de 7 meses e foram utilizadas 300 estações de trabalho para a quebra. Um fato preocupante: cerca de 95% dos sites de comércio eletrônico utilizam chaves RSA de 512 bits.
ElGamal	O ElGamal é outro algoritmo de chave pública utilizado para gerenciamento de chaves. Sua matemática difere da utilizada no RSA, mas também é um sistema comutativo. O algoritmo envolve a manipulação matemática de grandes quantidades numéricas. Sua segurança advém de algo denominado problema do logaritmo discreto. Assim, o ElGamal obtém sua segurança da dificuldade de se calcular logaritmos discretos em um corpo finito, o que lembra bastante o problema da fatoração.
Diffie-Hellman	Também baseado no problema do logaritmo discreto, e o criptosistema de chave pública mais antigo ainda em uso. O conceito de chave pública aliás foi introduzido pelos autores deste criptosistema em 1976. Contudo, ele não permite nem ciframento nem assinatura digital. O sistema foi projetado para permitir que dois indivíduos entrem em um acordo ao compartilharem um segredo tal como uma chave, muito embora eles somente troquem mensagens em público.
Curvas Elípticas	Em 1985, Neal Koblitz e V. S. Miller propuseram de forma independente a utilização de curvas elípticas para sistemas

	criptográficos de chave pública. Eles não chegaram a inventar um novo algoritmo criptográfico com curvas elípticas sobre corpos finitos, mas implementaram algoritmos de chave pública já existentes, como o algoritmo de Diffie e Hellman, usando curvas elípticas. Assim, os sistemas criptográficos de curvas elípticas consistem em modificações de outros sistemas (o ElGamal, por exemplo), que passam a trabalhar no domínio das curvas elípticas, em vez de trabalharem no domínio dos corpos finitos. Eles possuem o potencial de proverem sistemas criptográficos de chave pública mais seguros, com chaves de menor tamanho. Muitos algoritmos de chave pública, como o Diffie - Hellman, o ElGamal e o Schnorr podem ser implementados em curvas elípticas sobre corpos finitos. Assim, fica resolvido um dos maiores problemas dos algoritmos de chave pública: o grande tamanho de suas chaves. Porém, os algoritmos de curvas elípticas atuais, embora possuam o potencial de serem rápidos, são em geral mais demorados do que o RSA.

Tabela IV – Algoritmos de Criptografia Assimétricos

10 CERTIFICADO DIGITAL

Um certificado digital, ou identidade digital, pode ser visto como uma carteira de identidade para uso na Internet. Com ele é possível comprovar tanto a identidade de uma pessoa navegando na Internet, como a de um site.

Os certificados digitais possuem uma forma de assinatura eletrônica de uma instituição reconhecida por todos como confiável, e que, graças à sua idoneidade, faz o papel de "Cartório Eletrônico".

Por exemplo, ao acessar uma conta bancária, o certificado do servidor do banco assegura que o site acessado é realmente o do banco.

A Certificação Digital garante três princípios básicos da comunicação segura em ambiente de rede de computador: autenticidade, privacidade e integridade.

Tecnicamente, um certificado digital é um conjunto de dados (um arquivo, basicamente), assinado digitalmente pela autoridade certificadora e contendo tipicamente certas informações:

- Chave Pública correspondente ao certificado
- Nome e endereço eletrônico do dono do certificado
- Nome e assinatura digital da autoridade certificadora

Os próximos tópicos irão explicar o significado de assinatura digital e autoridade certificadora.

10.1 ASSINATURA DIGITAL

A assinatura digital é um mecanismo criado para atribuir confiabilidade a um documento eletrônico.

Pela verificação da autenticidade da assinatura, pode-se obter a confirmação da participação de determinada pessoa em uma transação eletrônica.

A assinatura digital permite também proteger a integridade de um documento.

10.2 AUTORIDADE CERTIFICADORA

É uma entidade de confiança que administra a gestão de certificados digitais através da emissão, revogação e renovação dos mesmos por aprovação individual.

A Autoridade Certificadora pode emitir diferentes tipos de certificados, atribuindo diferentes níveis de confiança a cada tipo de certificado. Para cada um desses tipos é utilizado um processo diferente para realizar a verificação da identidade do solicitante.

Assinando digitalmente os certificados que emite, a Autoridade Certificadora cria um relacionamento entre ela e o certificado emitido. Este relacionamento fica explícito no próprio certificado pela cadeia de certificação. Assim, a confiança em um determinado certificado digital está atrelada à confiança na Autoridade Certificadora que o emitiu.

Alguns exemplos de Autoridades Certificadoras:

- CeriSign
- VeriSign
- EuroSign
- GlobalSign

11 SSL

O Secure Socket Layer (SSL, atualmente na versão 3) é um protocolo de comunicação que implementa um duto seguro para comunicação de aplicações na Internet, de forma transparente e independente da plataforma.

Foi desenvolvido pela Netscape Communications em sua versão inicial em julho de 1994. Em abril de 1995 foi lançada a referência para implementação da versão 2 (sendo distribuído junto os Browsers Netscape e Internet Explorer e os servidores web mais comuns - Apache, NCSA httpd, IIS, Netscape Server etc), apoiado pela Verisign e Sun, transformando-se em um padrão em e-commerce, tendo a sua especificação submetida ao grupo de trabalho W3C.

Sua proposta é permitir a autenticação de servidores, criptografia de dados, integridade de mensagens e, como opção, a autenticação do cliente, operando nas comunicações entre aplicativos de forma interoperável.

Visa garantir os seguintes objetivos:

- Segurança criptográfica para o estabelecimento de uma ligação segura entre duas máquinas/aplicativos, assegurando a privacidade na conexão
- Autenticação do Servidor (e, opcionalmente do Cliente)
- Confiabilidade na conexão

A questão do desempenho foi levada em consideração no projeto, para reduzir o número de conexões e minimizar o tráfego na rede pode ser usado opcionalmente um esquema de cache em memória durante o estabelecimento da sessão, com a finalidade de reduzir o número de conexões e reduzir a atividade no acesso à rede.

O protocolo SSL provê a adição de uma camada de Socket Seguro em relação às camadas padrões do TCP/IP.

Protocolo TCP/IP com SSL	
Camada	Protocolo
Aplicação	http, Telnet, FTP, etc.
Socket Seguro (Secure Sockets)	SSL

Transporte	TCP
Rede	IP

Tabela V – Camadas TCP/IP com inclusão do SSL

O exemplo mais óbvio da utilização do SSL é em transações e-commerce. Nessas transações não se pode simplesmente assumir que a identidade do servidor com o qual se está comunicando é correta. Qualquer um pode criar uma página falsa, fazendo-se passar por uma entidade respeitável, e pedir o número do cartão de crédito dos usuários por um serviço inexistente.

O SSL permite que o cliente autentique a identidade do servidor, e uma vez que o cliente possui a certeza sobre a identidade do servidor, o SSL provê privacidade e integridade das informações durante a conexão, permitindo o tráfego seguro dos dados do cliente pela rede.

Abaixo segue um esquema representando o hand-shake do SSL, com a troca das mensagens entre cliente e servidor.

Figura 11.1 – Mensagens Trocadas no Hand-Shake SSL

Abaixo seguem breves comentários sobre cada uma das mensagens do hand-shake SSL:

Hello Cliente – O cliente envia ao servidor informações incluindo a versão mais recente do SSL suportada por ele, e informações sobre os tipos de criptografia que ele suporta.

Hello Servidor – O servidor escolhe a versão do SSL mais recente possível e escolhe como será dada a criptografia.

Certificado – O servidor envia ao cliente um certificado, com sua chave pública e o certificado da Autoridade Certificadora.

Requisição Certificado – Se o servidor necessitar autenticar o cliente, ele envia uma requisição de certificado ao client. Em aplicações para a Internet, essa mensagem raramente é enviada.

Chave Servidor – O servidor envia ao cliente essa mensagem quando as informações enviadas no certificado não são suficientes para troca de chaves.

Hello Servidor Terminado – O servidor avisa ao cliente que acabou o processo de envio das mensagens preliminares.

Certificado – Se o servidor enviar uma requisição de certificado, o cliente envia seu certificado assim como o servidor o fez na mensagem 4.

Chave do Cliente – O cliente gera informações utilizadas para criar uma chave que será utilizada na criptografia simétrica. Essa chave é então encriptada utilizando a chave pública do servidor e enviada ao servidor.

Verificação Certificado – Em aplicações para a Internet essa mensagem raramente é enviada. Seu propósito é de permitir que o servidor complete o processo

de autenticação do cliente. Quando o cliente manda essa mensagem, ele assina digitalmente usando criptografia. O servidor recebe a informação e decriptografa utilizando a chave pública do cliente, e então o cliente é autenticado.

Muda Modo Criptografia – O cliente envia uma mensagem avisando o servidor para mudar para o modo criptografado.

Fim – O cliente avisa ao servidor que está pronto para transmitir dados seguros.

Muda Modo Criptografia – O servidor envia uma mensagem ao cliente para mudar para o modo criptografado.

Fim – O servidor avisa ao cliente que está pronto para transmitir dados seguros. Essa mensagem corresponde ao fim do processo de handshake do SSL.

Dados Encriptados – O cliente e o servidor comunicam-se utilizando algoritmos simétricos de criptografia, utilizando a chave e os algoritmos estabelecidos durante o hand-shake

Após o processo de hand-shake o canal seguro SSL encontra-se estabelecido e inicia-se a troca das mensagens entre cliente e servidor. O cliente e o servidor criptografam as mensagens utilizando a chave de sessão estabelecida durante o hand-shake. Essa chave é gerada do lado do cliente, criptografada pelo cliente, utilizando a chave pública do servidor, e depois é enviada ao servidor, que a decriptografa.

12 DESAFIOS E PROBLEMAS ENCONTRADOS

O primeiro desafio dos integrantes do grupo foi elaborar uma proposta de um projeto de um sistema inovador ou que não tivesse uma solução bem conhecida e aplicada no mercado. A solução adotada foi muito bem aceita pois envolvia o mercado de ações, que nos parecia muito desafiador.

A partir de então, o problema encontrado foi a escolha das tecnologias encontradas. Optamos por tecnologias já conhecidas e utilizadas no mercado como o Web Service e J2ME.

A falta de conhecimento destas tecnologias levou a uma série de equívocos durante a implementação. A adoção da ferramenta Hibernate para realizar acesso à base de dados acarretou uma perda de tempo em estudos maior do que o previsto. Outra atividade que gerou retrabalho foi a implementação do Web Service no padrão JAVA-RPC, que se mostrou incompatível no momento da construção da interface entre o dispositivo J2ME e o Web Service, sendo necessária a alteração do padrão do Web Service para Document/Literal. Para implementar esse padrão foi necessária a alteração da versão do Axis de 1.1 para 1.2 pois a primeira não suportava tais características. A falta de documentação destes padrões compatíveis entre as tecnologias Web Service e J2ME também dificultou a implementação.

Outro grande problema encontrado nesta conexão entre o J2ME e o Web Service foi a restrição de algumas operações, que gerou uma reprogramação do acesso aos serviços, o que facilitou esta atividade foi a implementação da arquitetura do Mobile Broker de forma modular, diminuindo o retrabalho.

A falta de conhecimento da ferramenta também dificultou a implementação do Home Broker, pois o tempo gasto para a geração das telas JSP foi acima do planejado.

Os padrões de criptografia para a conexão entre o dispositivo móvel e o Web Service encontrados no mercado não são compatíveis com as restrições impostas pelo ambiente J2ME, o que levou o grupo a optar por uma simulação desta criptografia em emuladores.

13 MUDANÇAS DE ESCOPO INICIAL

Diante das dificuldade citadas no capítulo anterior e da saída de um dos integrantes, no mês de novembro o grupo decidiu realizar uma reprogramação das atividades.

Foi realizada uma reunião com um especialista do mercado de ações do banco Santander que nos ajudou a definir as principais funcionalidades do sistema. Como resultado desta reavaliação, as funcionalidades de Cadastro e envio de notícias e recomendações foi retirada do escopo, assim como o envio de notificação da realização da operação. Esta última funcionalidade foi retirada devido à dificuldade encontrada para simular a realização ou não de uma operação na bolsa.

A princípio, foi imaginado que as simulações seriam realizadas em um dispositivo móvel fornecido pelo laboratório da Microsoft, porém diante da impossibilidade de executar o algoritmo de criptografia em dispositivos com menor capacidade, este teste ficará restrito a um emulador rodando em um microcomputador.

14 ESPECIFICAÇÃO TÉCNICA

Este capítulo visa fornecer informações a respeito do software desenvolvido no projeto, com o objetivo de documentá-lo para futura utilização.

Para a implementação, o sistema foi subdividido em três módulos: o web service, o mobile broker e o home broker conforme figura abaixo:

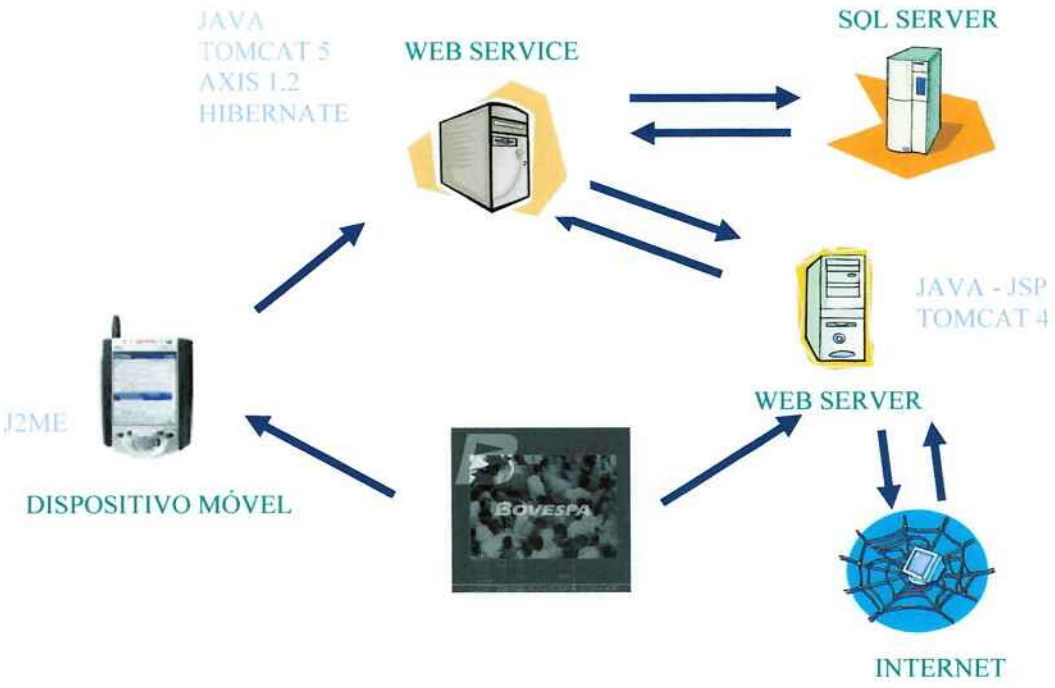

Figura 14.1 – Módulos do Sistema

14.1 WEB SERVICE

Para o Web Service era necessário prover uma arquitetura simples porém de fácil utilização e implementação. Visando tornar fácil a criação e o acesso à base de dados, foi utilizada a ferramenta HIBERNATE.

14.1.1 Serviços do Web Service

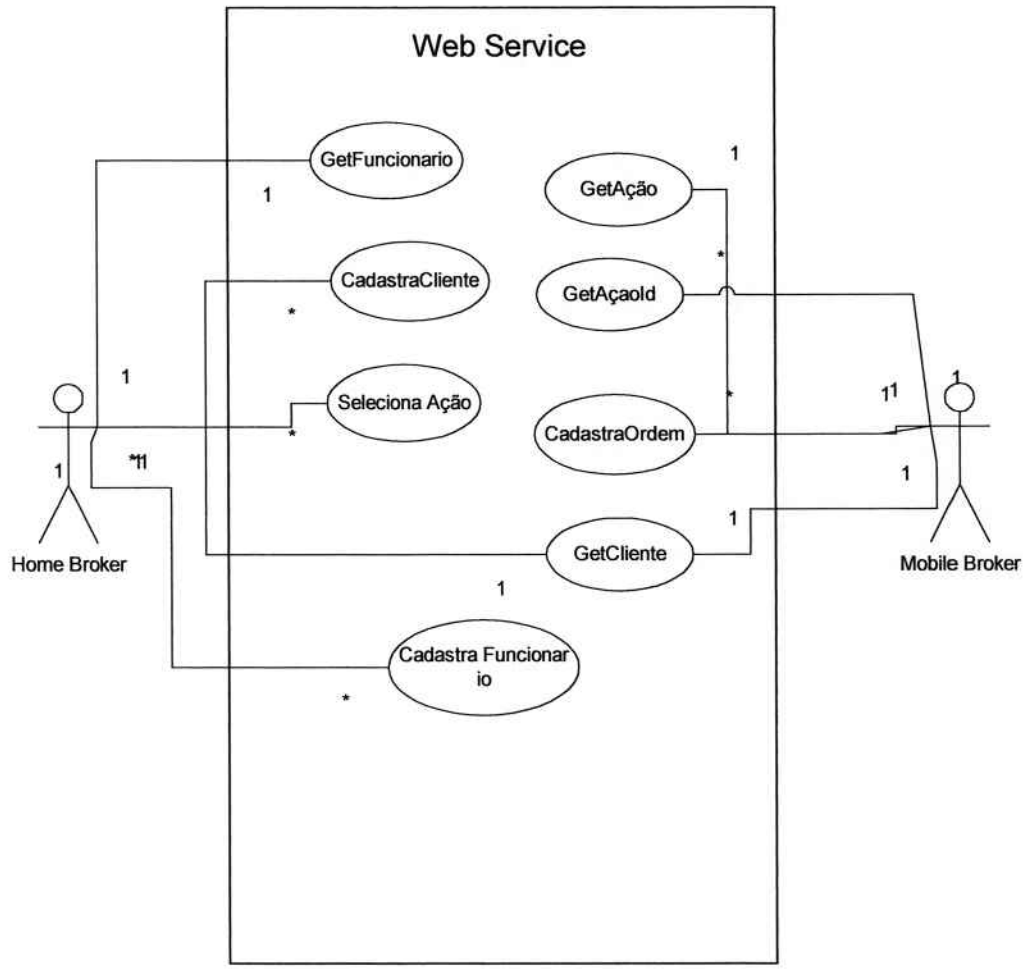

Figura 14.2 – Casos de Uso do Web Service

14.1.2 Diagrama de Classes Web Service

Abaixo pode-se ver o diagrama de classes com os principais pacotes do Web Service, que apóiam a classe a classe ServiceProvider responsável por publicar os serviços disponíveis.

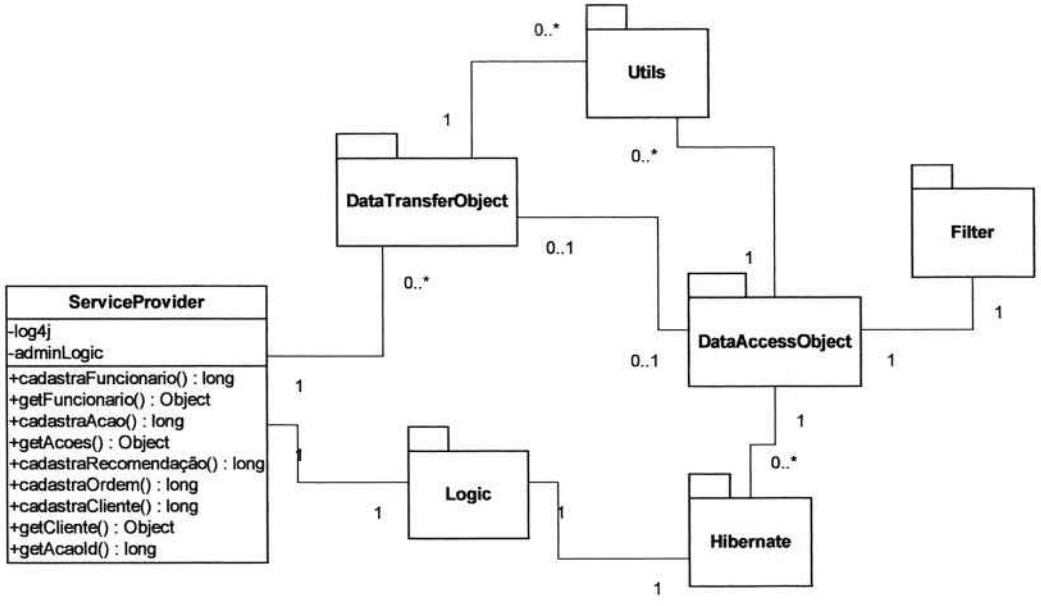

Figura 14.3 – Diagrama de Classes do Web Service

A seguir cada pacote será melhor estudado, conhecendo as suas classes, atributos e responsabilidades.

O pacote DataTransferObject armazena os objetos definidos na aplicação que serão transmitidos pela rede. Estas classes devem implementar a classe java.io.Serializable, presente na virtual machine JAVA, pois serão transmitidas pela rede. Por este motivo, estas classes também não podem instanciar classes que não tem esta propriedade. Os métodos destas classes são apenas os "getters" e "setters" dos atributos.

As classes responsáveis por converter objetos de um tipo para outro, por exemplo, de Long para Date e as classe responsáveis por obter a sessão de acesso à base de dados estão no pacote Utils.

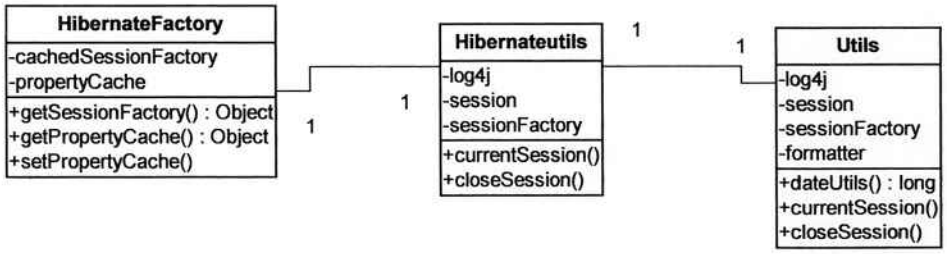

Figura 14.4 – Diagrama de Classes do Pacote Utils

No pacote DataAccessObjetc estão as classes que implementam métodos de busca na base de dados, auxiliada pelo pacote Filter que cria classes de filtro da busca.

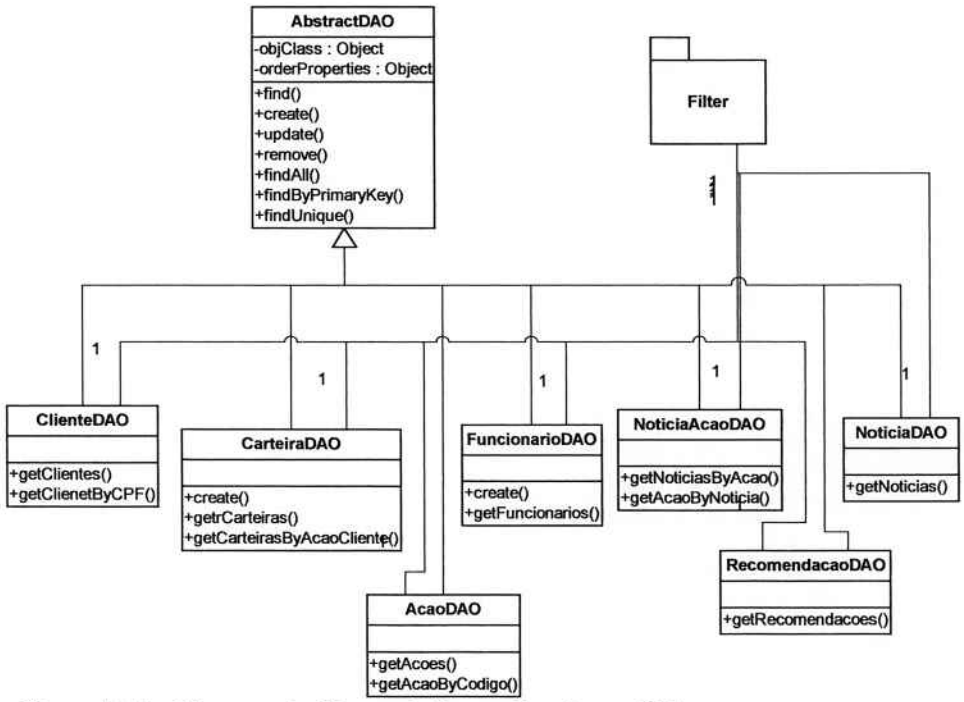

Figura 14.5 – Diagrama de Classes do Pacote DataAccessObject

No pacote Hibernate estão as classes persistentes, que se tornarão registros nas tabelas do banco de dados. Os métodos destas classes são apenas os "getters" e "setters", por isso não estão identificados na figura. Este diagrama também pode representar o modelo de dados do sistema.

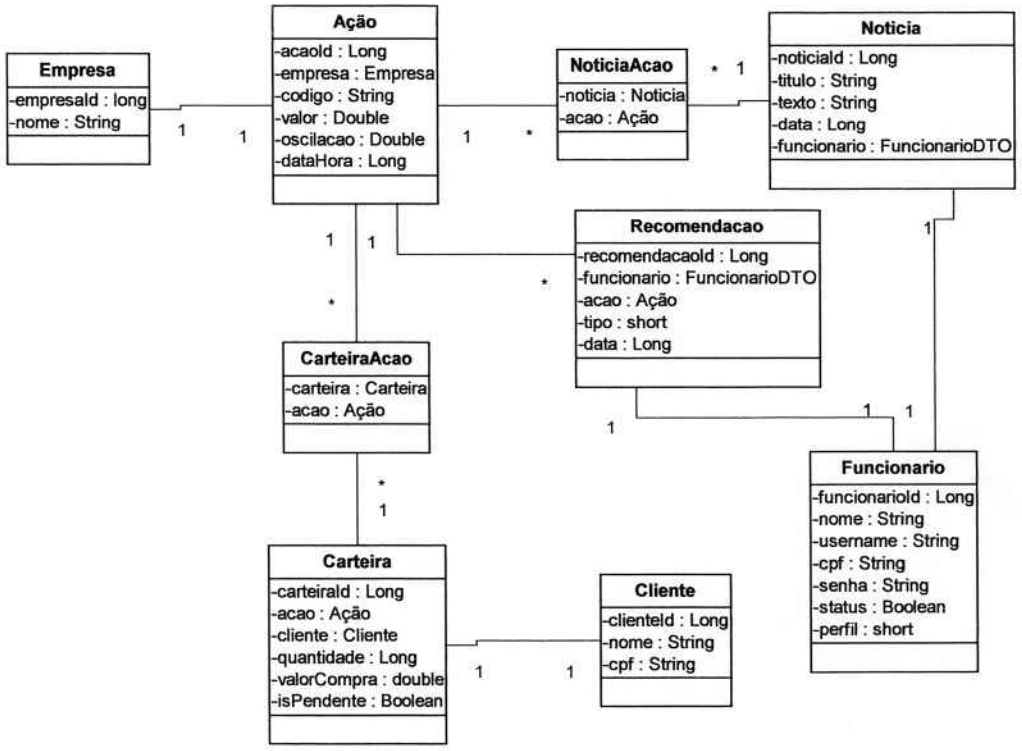

Figura 14.6 – Diagrama de Classes do Pacote Hibernate

A lógica do negócio está toda implementada dentro do pacote Logic, na classe AdminLogic. Para cada serviço do web service existe uma função correspondente nesta classe que executa os testes específicos.

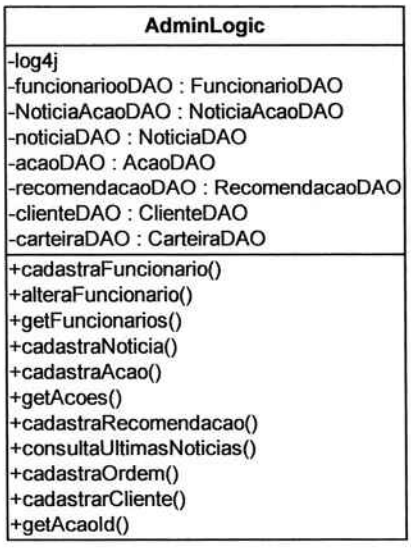

Figura 14.7 – Diagrama de Classes do Pacote Logic

14.1.3 Diagrama de Sequencia do Web Service

A seguir é apresentada uma ilustração sobre o funcionamento da requisição de cadastro de funcionário ao Web Service, o funcionamento para as demais requisições funcionam de maneira análoga.

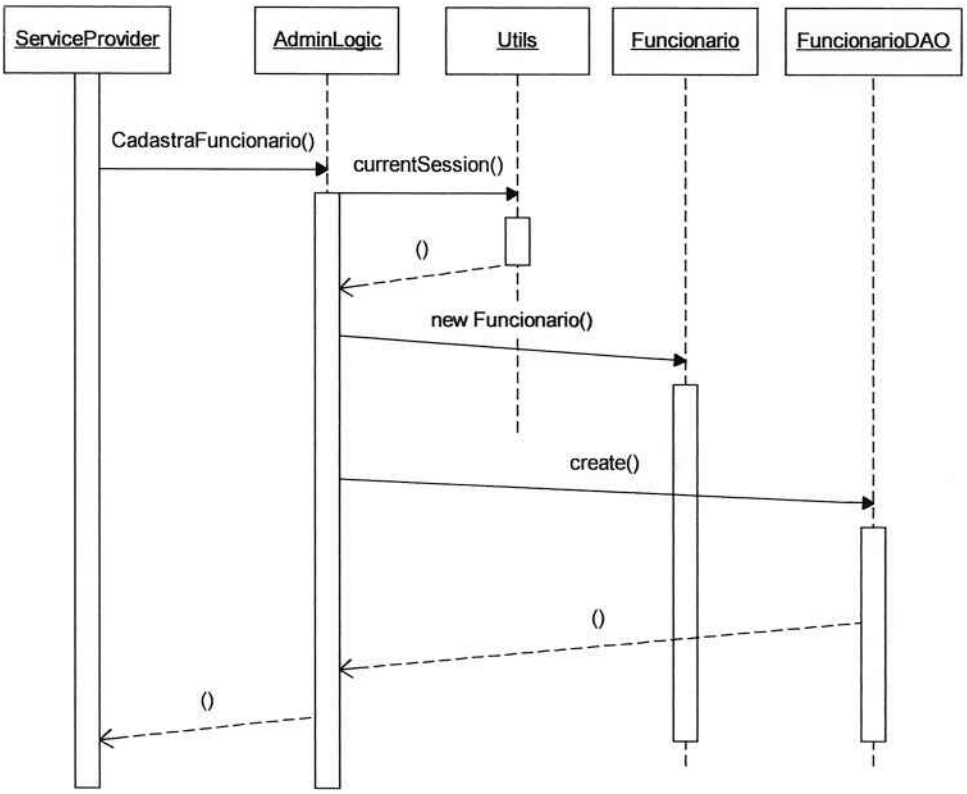

Figura 14.8 – Diagrama de Seqüência do Serviço CadastrarFuncionário

14.1.4 Requisitos de Banco de Dados

A escolha do banco de dados foi bastante flexível, porque o hibernate poderia construir a tabela e gerar as consultas independente do banco de dados que estiverem sendo utilizados, bastando este ser um banco de dados relacional. Através de um arquivo de configuração seria possível alterar a base de dados que estava sendo utilizada e atualizá-la com a ultima versão do modelo de dados automaticamente. Diante desta flexibilidade, optou-se por utilizar a base de dados SQL Server por ser

robusta, muito utilizada no mercado, de fácil obtenção no Laboratório Microsoft e de conhecimento dos integrantes do grupo.

14.1.5 Ferramentas de Desenvolvimento

Para desenvolvimento do web service utilizamos a IDE Eclipse, servidor Tomcat com web service Axis1.2 e banco de dados SQL Server 2000.

14.2 MOBILE BROKER

14.2.1 Funções do Mobile Broker

Inicialmente foram previstas as seguintes funções para o Mobile Broker:

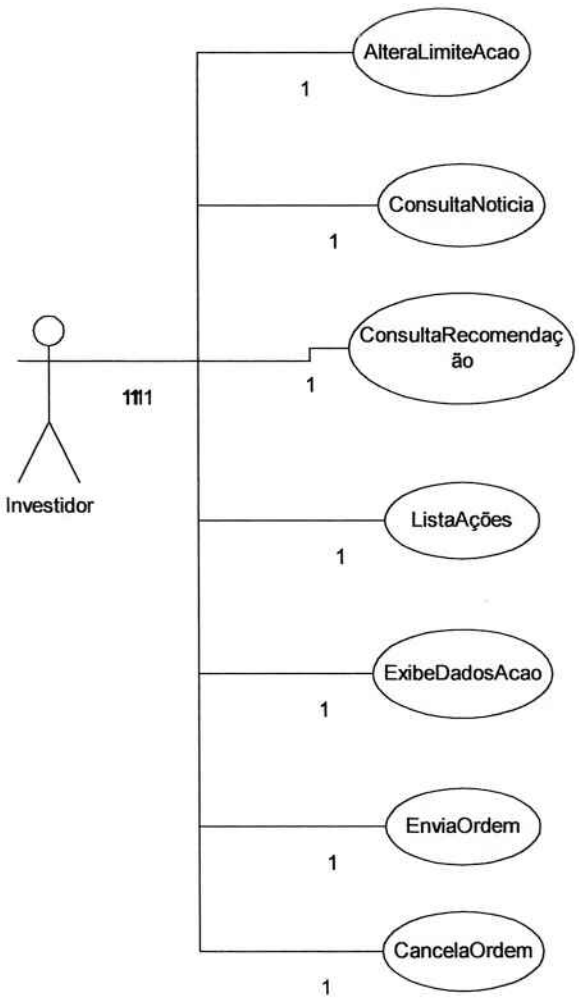

Figura 14.9 – Diagrama de Casos de Uso do Mobile Broker

Após a revisão das funcionalidades na segunda parte do projeto, verificou-se que, para o perfil de investidor que irá utilizar o Mobile Broker não era necessário colocar informações de notícias e recomendações. Portanto, estas funcionalidades, que apesar de já estarem com as telas desenvolvidas, não foram utilizadas.

14.2.2 Diagrama de Classes do Mobile Broker

Abaixo há uma descrição de como as classes do Mobile Broker estão divididas para atender a classe principal chamada MobileBrokerMIDlet, os pacotes e suas funcionalidades.

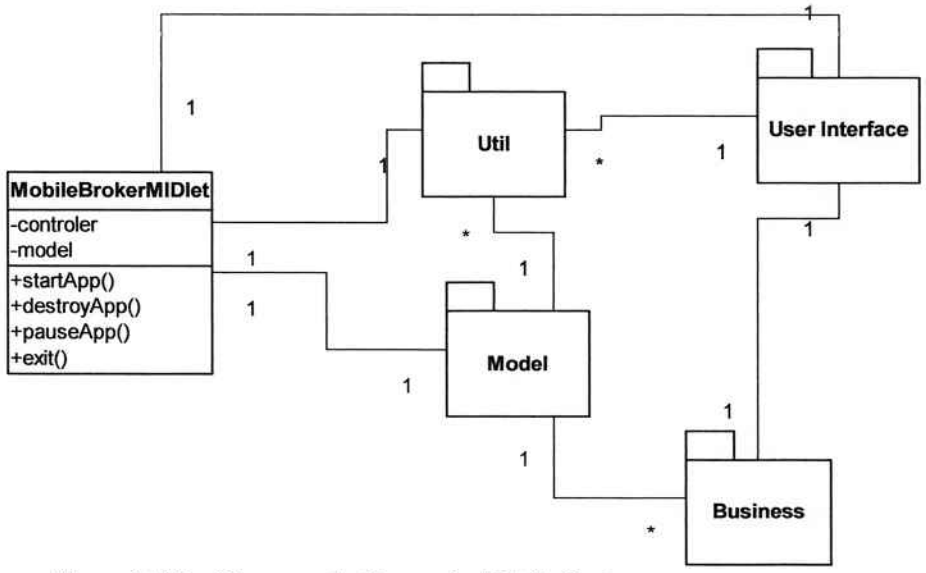

Figura 14.10 – Diagrama de Classes do Mobile Broker

A classe MobileBrokerMIDlet é a classe inicial do programa pois estende a classe MIDlet, que no J2ME é sempre a classe inicial, com os métodos startApp invocado no inicio da aplicação, destroyApp antes de sair da aplicação, pauseApp quando o usuário, por exemplo, recebe uma chamada quando está executando o programa e exit para sair da aplicação.

O pacote Util armazena duas classes utilizadas em muitos pontos da aplicação, uma responsável por tratar exceções (ApplicationException) e outra que mostra uma barra de progresso quando uma nova tela está sendo carregada (ProgressObserver).

No pacote Model está a classe ModelFacade, que é responsável por realizar a lógica de todas as requisições da aplicação. É nela que os serviços do Web Service são chamados e o retorno é enviado para a aplicação. Outro método importante é o getQuote que busca os dados das cotações das ações on-line no site http://finance.yahoo.com para atualização da tela. Optou-se por realizar todas as funções do Mobile Broker para tornar a aplicação modular, ou seja, o método de acesso ao servidor fica restrito a uma classe e passando-se a utilizar um outro método de acesso a outro servidor não sendo necessário alterar todas as telas da aplicação.

O pacote UserInterface, como o próprio nome diz, é onde ficam as telas do sistema. Foi dada especial atenção à tela de listagem de Ações (ListaAçõesUI) que é a tela principal para o investidor. É onde ele acompanhará a evolução do valor das ações, portanto ela deve ser atualizada a todo momento. Outra classe muito importante deste pacote é a UIControler que é a classe que controla todas as telas que estão sendo mostradas, gera as requisições para o ModelFacade e controla exceções.

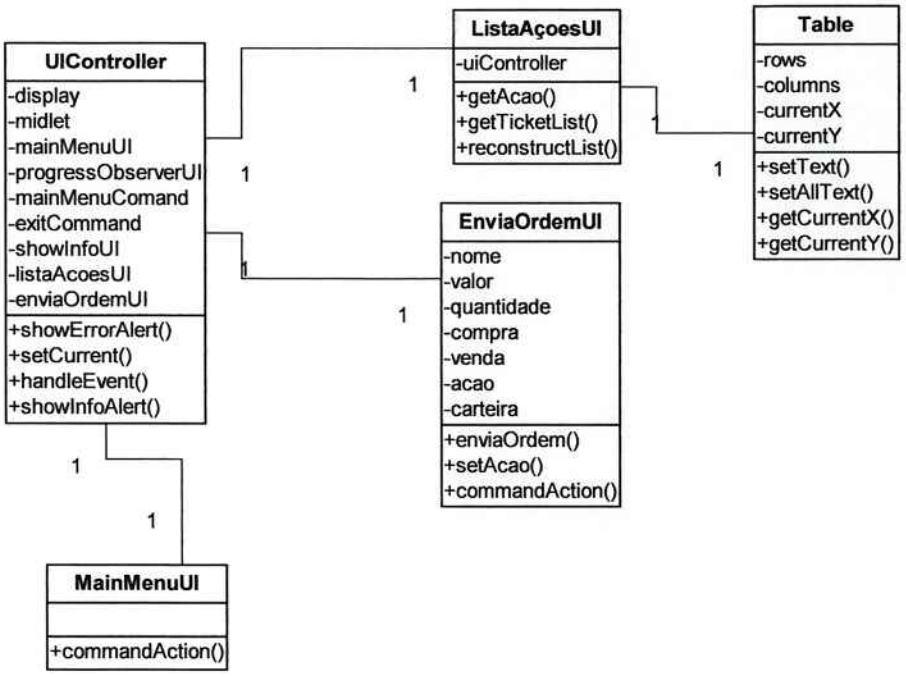

Figura 14.11 – Diagrama de Classes do pacote UserInterface

O pacote Business armazena todas as classes de envio para o web service, estas classes são as mesmas do pacote DataTransferObject do Web Service e foram geradas automaticamente com a ferramenta J2ME Wireless Tollkit. Esta ferramenta também cria automaticamente uma classe que estabelece a conexão com o Web service e realiza a chamada ao serviço (ServiceProvider_Stub).

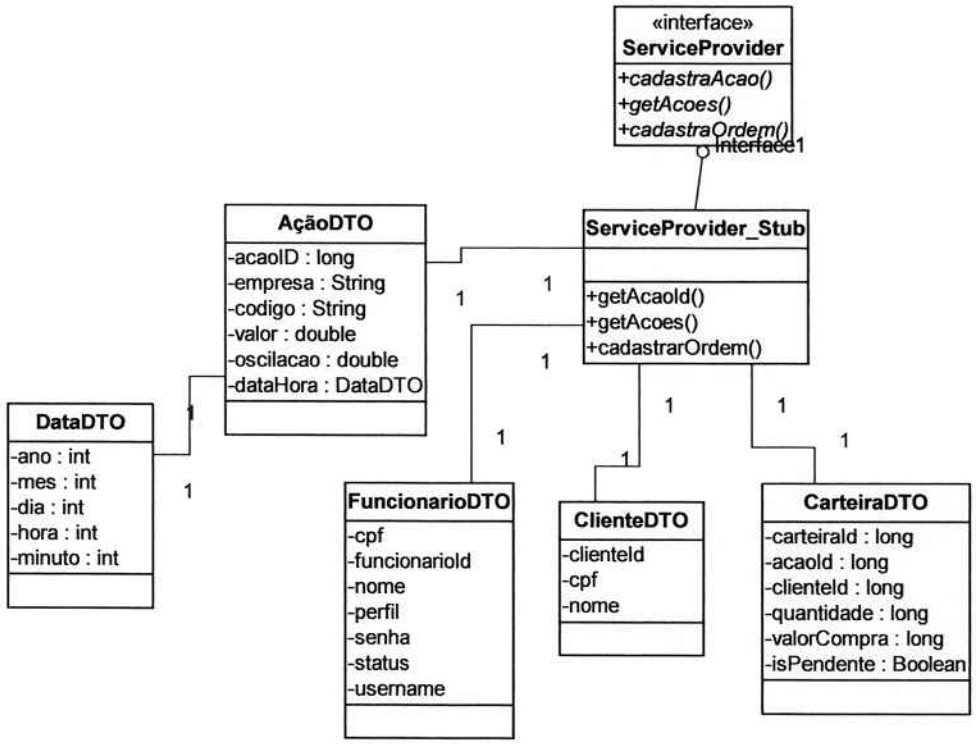

Figura 14.12 – Diagrama de Classes do Pacote Business

14.2.3 Diagrama de Seqüência do Mobile Broker

A seguir será apresentado um exemplo do funcionamento do Mobile Broker através do diagrama de seqüência da funcionalidade de envio de Ordem.

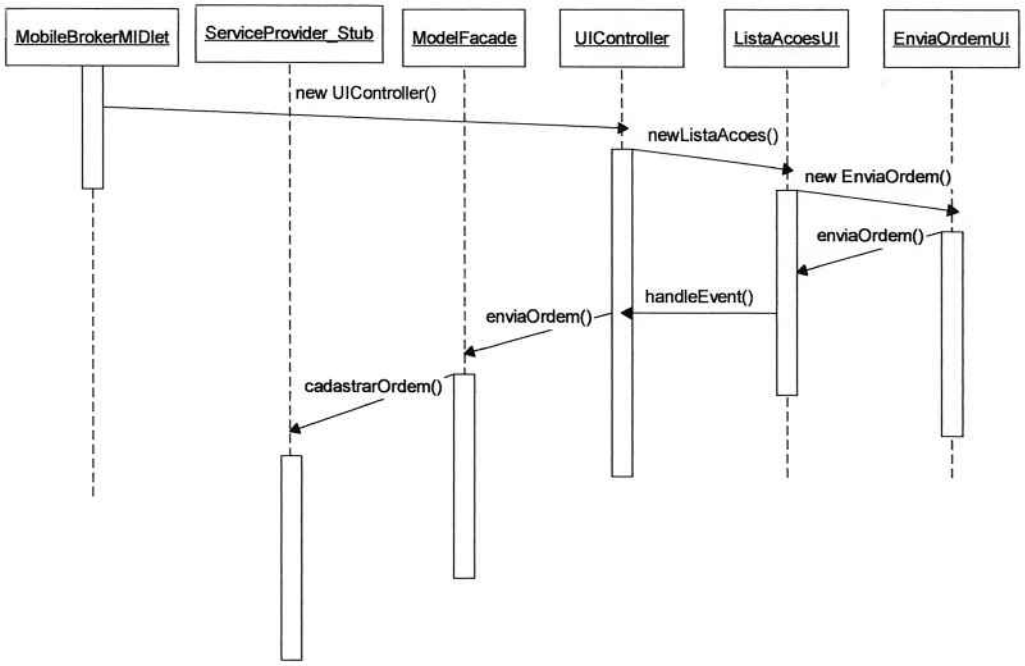

Figura 14.13 – Diagrama de Seqüência de Envio de Ordem

14.2.4 Ferramentas de Desenvolvimento

Para a implementação do Mobile Broker foi utilizada a IDE Eclipse, para rodar aplicativos J2ME no eclipse, utilizamos o plugin eclipseme 0.4.6. Além disso, utilizamos o J2ME Wireless Tollkit 2.2 para gerar as classes de acesso ao Web Service.

14.3 HOME BROKER

14.3.1 Funções do Home Broker

Inicialmente foram previstas as seguintes funções para o Home Broker:

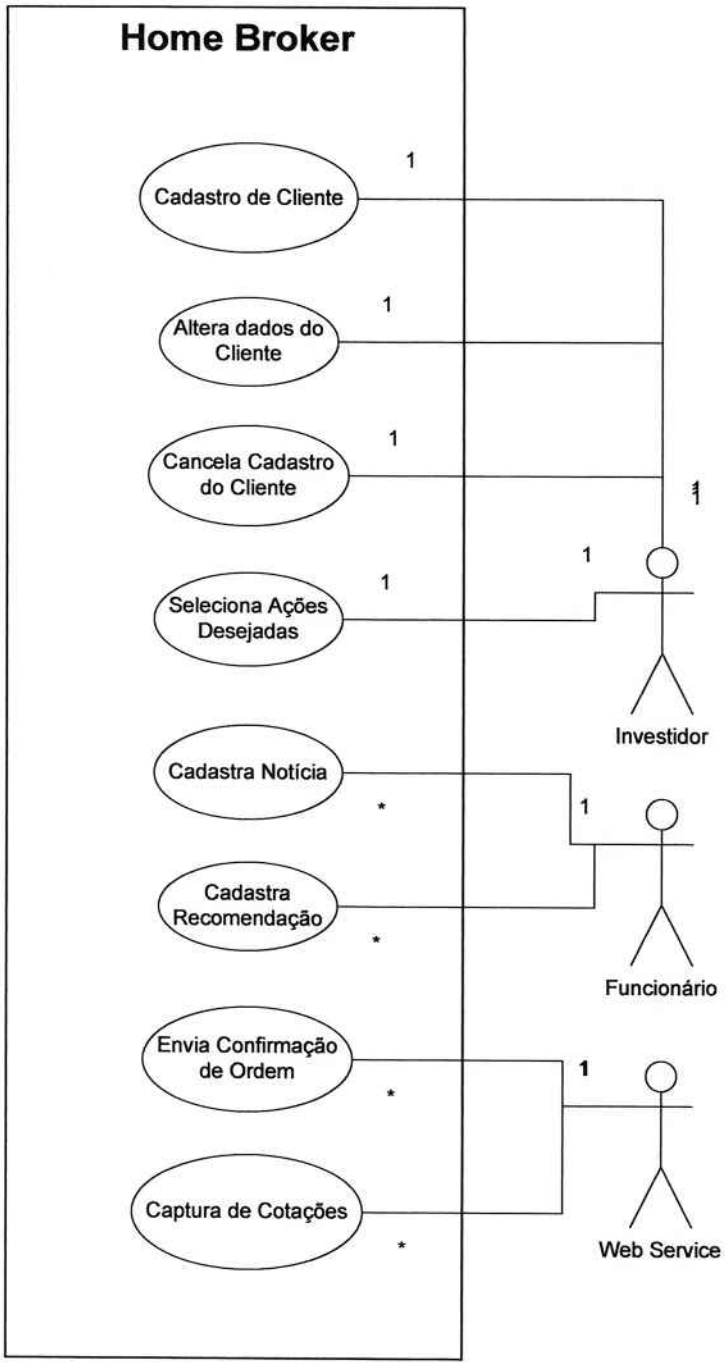

Figura 14.14 – Diagrama de Use Cases do Home Broker

Após a revisão das funcionalidades na segunda parte do projeto, verificou-se que, para o perfil de investidor que iria utilizar o Mobile Broker não era necessário colocar informações de notícias e recomendações. Portanto, o cadastro das mesmas não seria mais necessário, sendo retiradas do escopo inicial.

14.3.2 Fluxo do Home Broker

O Home Broker tem a finalidade de manter o cadastro de clientes, controlas logins, segregar acessos e disponibilizar as ações para seleção dos investidores, assim como disponibilizar suas cotações.

O fluxo abaixo mostra sucintamente a seqüência das telas utilizadas no Home Broker.

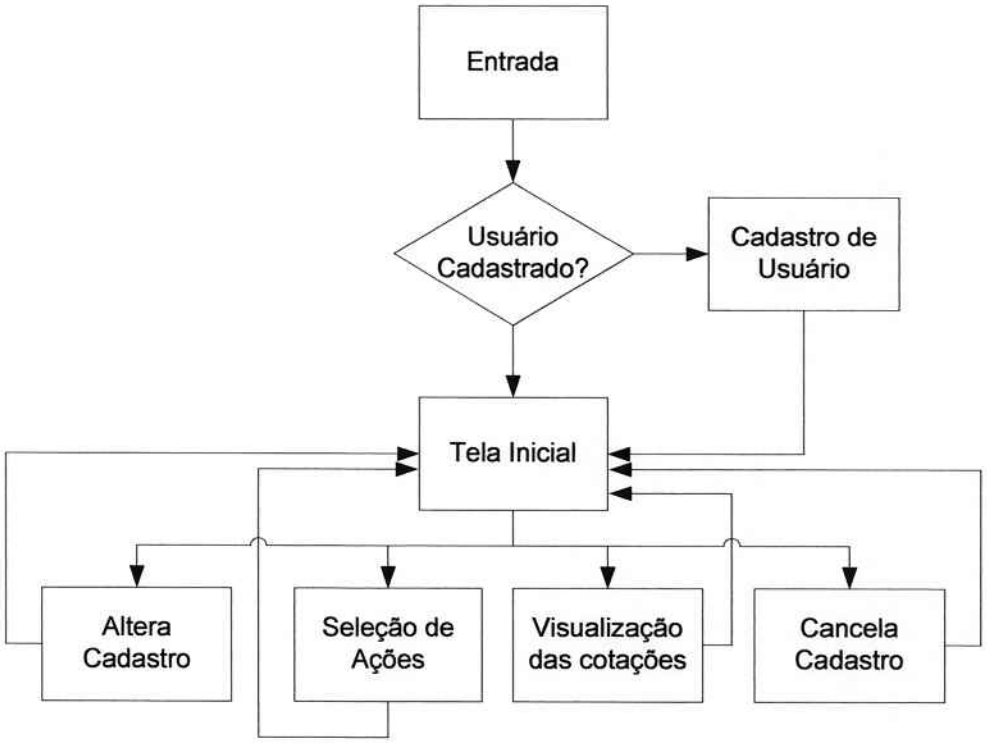

Figura 14.15 – Fluxo simplificado de Telas do Home Broker

Um usuário acessa o sistema, que verifica se ele está ou não cadastrado. Se estiver, é direcionado para a página inicial, onde tem as opções de alterar ou cancelar seu cadastro, selecionar as ações que lhe interessam e visualizar as cotações mais recentes.

A busca da cotação das ações é realizada online no site http://finance.yahoo.com.

14.3.3 Ferramentas de Desenvolvimento

Para a implementação do Home Broker foi utilizado o Notepad do Windows para desenvolvimento das páginas HTML e a IDE Eclipse, para criação das páginas JSP e testes de classes.

14.4 SEGURANÇA

A solução adotada para a comunicação em ambiente wireless entre o PDA do cliente e o servidor foi a implementação do protocolo SSL.

O protocolo SSL como dito anteriormente irá criar um canal seguro para a transmissão das informações sigilosas entre cliente-servidor.

Para isso, do lado do servidor, será exigido um par de chaves (uma chave privada e uma pública) e um certificado digital, contendo informações sobre sua chave pública, o tipo de criptografia assimétrica adotada que será utilizado pelo cliente para o envio da chave de sessão gerada no hand-shake do protocolo SSL. A chave privada será armazenada no keystore do servidor protegida por senha.

Para fins acadêmicos, não iremos solicitar um certificado em uma Autoridade Certificadora. Para gerar esse certificado que será utilizado pelo servidor, foi utilizada a ferramenta keytool presente no jdk (java development kit) disponibilizado pela Sun.

A partir dessa ferramenta foi gerado um certificado digital, sendo o formato escolhido para a chave privada RSA, o tamanho dessa chave de 1024 bits e o método para assinar o certificado, no caso MD5 com RSA.

Comando executado:

keytool -genkey -keyalg RSA -sigalg MD5withRSA

-keysize 1024 -alias MBroker -keystore MobileBroker.ks -storetype JKS

Esse certificado é auto-assinado, e portanto será detectado que o mesmo não foi gerado por uma Autoridade, e portanto o browser não confiará no mesmo. Como resultado, será exibida uma mensagem de alerta quando o mesmo for apresentado ao cliente, basta aceitar esse certificado para prosseguir.

Depois da geração desse certificado, o mesmo é armazenado no keystore do servidor, que é um repositório de chaves também especificado no jdk. Esse armazenamento é realizado também utilizando a ferramenta keytool.

No lado do cliente, o mesmo necessita importar para o keystore (repositório de chaves) de seu PDA a chave pública do servidor, presente no certificado do servidor.. Essa importação é realizada utilizando uma ferramenta MEKeyTool (Mobile Equipment Key Tool), similar à keytool, para dispositivos móveis, utilizando J2ME Wireless Toolkit.

Feito isso, os serviços poderão ser invocados através da conexão HTTPS, utilizando o canal SSL criado.

15 ESFORÇO PARA A REALIZAÇÃO DO TRABALHO

Após a definição do escopo inicial, foi realizado um esforço grande por parte dos integrantes para conhecer as tecnologias e iniciar o desenvolvimento, conforme descrito no capitulo 12. O desenvolvimento das soluções foi implementado enquanto um dos integrantes realizava pesquisas sobre conceitos de segurança e a integração destas soluções na implementação do projeto.

A tabela abaixo resume o esforço realizado para estudos e implementação do projeto.

INTEGRANTE	ESFORÇO (HS)
ANDRE	950
MURILO	930
PINHEIRO	900
TOTAL	2780
Custo do HH	R$ 20,00
Custo total do HH	R$ 55.600,00

Tabela VI – Esforço do Projeto

16 LISTA DE REFERÊNCIAS

- http://www.hibernate.org
- http://www.alphafintec.com.br
- http://www.bovespa.com.br
- http://inpresspni4.locaweb.com.br
- http://www.valoreconomico.com.br
- http://www.comunique-se.com.br
- http://www.mobileplanet.com
- http://computing.kelkoo.co.uk
- http://www.scriptsharks.com
- http://www.saugus.net
- http://www.digicom.co.nz
- http://www.objectlearn.com
- http://renaud91.free.fr
- http://www.sysdeo.com
- http://solareclipse.sf.net
- http://www.world.std.com
- http://www.peertech.org
- http://www.trl.ibm.com
- Little, M. – "Transaction and Web Service" – Communication of ACM, v46 n10 Outubro de 2003
- Stallings, William – "Network and Internetwork Security"
- Dournaee, Blake – "XML Security"
- Weill, Peter; Vitale, Michael – "Place to Space"
- Albuquerque, Ricardo – "Segurança no Desenvolvimento de Software"
- Pavlova, Anna – "Mapping a Contagious Global Economy"
- NIST (National Institute of Standarts and Technology) – "Wireless Network Security"
- Santana, André A. – "Proposta para otimização do desempenho do protocolo TCP em redes Wireless"
- Geus, Paulo Lício de; Nakamura, Emilio Tissato – "Segurança de Redes"

17 CONSIDERAÇÕES FINAIS

Apesar de todas as mudanças de escopo, às quais o projeto foi submetido, devido às dificuldades encontradas, pode-se dizer que o resultado final atingiu nossas expectativas.

Foi possível projetar e implementar um sistema com as funcionalidades principais que haviam sido planejadas, culminando em um projeto, a fim de que as funcionalidade retiradas do escopo possam ser adicionadas facilmente no futuro.

Além do aprimoramento técnico obtido com as tecnologias utilizadas, conseguiu-se também dar um enfoque do mercado com o qual a aplicação está relacionada, com o intuito de um futuro aprimoramento para implementação de um produto com bastante apelo comercial.