UNIVERSIDADE FEDERAL DE SANTA CATARINA
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

Raquel Aparecida Pegoraro

Segurança no Desenvolvimento de Sistemas de Comércio Eletrônico

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

Prof. Ricardo Felipe Custódio, Dr.
Orientador
custodio@inf.ufsc.br

Florianópolis, Agosto de 2002

Segurança no Desenvolvimento de Sistemas de Comércio Eletrônico

Raquel Aparecida Pegoraro

Esta Dissertação foi julgada adequada para a obtenção do título de Mestre em Ciência da Computação, área de concentração Sistemas de Computação e aprovada em sua forma final pelo Programa de Pós-Graduação em Ciência da Computação.

Prof. Fernando Ostuni Gauthier, Dr.

Coordenador do Curso

gauthier@inf.ufsc.br

Banca Examinadora

Prof. Ricardo Felipe Custódio, Dr.

Orientador

custodio@inf.ufsc.br

Prof. Aires José Rover Junior, Dr.

airesjr@ccj.ufsc.br

Prof. Carla Merkle Westphall, Dr.

carla@lrg.ufsc.br

Prof. Clerilei Aparecida Bier, Dr.

c2cab@udesc.br

Ofereço este trabalho aos meus pais João e Iria, e ao meu noivo Josenir.

Agradecimentos

Agradeço a Deus, o qual é o grande responsável por tudo isso.

Gostaria de agradecer ao meu orientador Ricardo Felipe Custódio, por toda sua atenção, esforço e amizade. Ele foi um verdadeiro mestre.

Ao meu noivo Josenir, pelo amor e paciência durante todo a minha luta.

Aos meus pais João e Iria, pela educação, apoio e amizade, os quais estão sempre presente me apoiando em todos os desafios da minha vida. Essa vitória também é deles.

Aos colegas de mestrado, grandes companheiros durante o período de estudo, que me apoiaram e ajudaram em todos o momentos.

Sumário

Lista de Figuras

Lista de Tabelas

Lista de Siglas

AA	Autoridade de Aviso
AC	Autoridade Certificadora
ACP	Autoridade de Chave Pública
AD	Autoridade de Datação
AR	Autoridade de Registro
CE	Comércio Eletrônico
DES	Data Encryption Algorithm
ICP	Infra-estrutura de Chaves Públicas
I2AC	Infra-estrutura de Auxílio a Análise de Crédito
LabSEC	Laboratório de Segurança
SAC	Serviço de Atendimento ao Cliente
SET	Secure Electronic Transactions
SSL	Secure Socket Layer
STT	Secure Transaction Technology
SEPT	Secure Electronic Payment Protocol
SETco	Secure Electronic Transaction Consortium
RSA	Padrão de cifragem assimétrica
TI	Tecnologia de Informação

Resumo

Atualmente, o comércio eletrônico está emergindo no mercado e, como conseqüência, surge uma grande oportunidade de novos e inovadores negócios. Nessa nova forma de negociação, surgem várias questões que necessitam ser resolvidas para que o comércio eletrônico possibilite um mercado global. Um dos pontos em questão nos últimos anos se refere a segurança. Nesta dissertação é fornecida uma avaliação sobre os assuntos de segurança que envolve o comércio eletrônico e suas aplicações. São discutidos os processos e requisitos de segurança em aplicações de comércio eletrônico, os quais geralmente vão além das exigências tradicionais de segurança de redes. Apresentada também uma visão geral dos projetos de pesquisa que tem sido feitos sobre segurança no comércio eletrônico. É proposto um programa de trabalho de pesquisa para segurança em aplicações de comércio eletrônico e uma metodologia para a agregação de segurança nos sistemas de comércio eletrônico.

Palavras-chave: Comércio eletrônico, segurança.

Abstract

Now a days, the electronic commerce is emerging in the market and, as consequence, a great opportunity appears of new and innovative business. In that new negotiation form, it appears several subjects that need to be resolved so that the electronic commerce could provide a global market. One of the points in subject in the last years refers the security. In this dissertation an evaluation is supplied on safety's subjects that it involves the electronic commerce and its applications, it is discussed the processes and requirements of security in applications of electronic commerce, which are generally going beyond of safety's of nets traditional demands. A general vision of the research projects that has been done on security in the electronic commerce.A program of research work is proposed for security in applications of electronic commerce and a methodology for aggregation of security in the systems of electronic commerce.

Capítulo 1

Introdução

A popularização da Internet abriu vários caminhos para sua utilização, deixando de ser utilizada apenas como meio de comunicação e passando a ser utilizada como um novo meio de fazer negócios, dando origem ao conceito de Comércio Eletrônico.

A idéia de Comércio Eletrônico não é nova já que a técnica de vender produtos utilizando novas mídias e meios de comunicação, existe desde os serviços de tele-vendas ou vendas pelo correio através de catálogos. A Internet é só mais um veículo que possibilita a comercialização de produtos de forma a atingir novos consumidores.

O comércio tradicional sempre foi realizado de forma local, centrado (do ponto de vista geográfico), restrito por fronteiras físicas e, por isso mesmo, cercado de restrições legais. A globalização da economia teve reforço substancial com o emprego da tecnologia de informação. Esse novo tipo de comércio, apoiado pela Internet e transações de cartões de crédito, trouxeram muitos benefícios às empresas que atuam neste área:

- Na Internet ninguém sabe qual o porte da sua empresa, pois a interface entre a empresa e o cliente é o seu sítio (site) e seus serviços;
- Os custos de criação e manutenção de uma loja virtual são extremamente menores dos de uma loja real;
- A Internet tem alcance mundial, possibilitando a expansão de mercados regionais e locais para nacionais e internacionais;

- Na Internet a cadeia de intermediários é menor. Os produtos negociados sem os atravessadores normalmente tem preços menores;

- A Internet funciona 24 horas por dia. Não há despesa com hora extra, com luz, e riscos de assaltos. Pedidos podem ser feitos a qualquer hora e para qualquer país, pois na Internet não há fusos horários;

- Na Internet o cliente está mais próximo da empresa. É interativa e permite saber exatamente quem é o cliente e o que ele quer;

- A Internet é um mercado orientado mas com o alcance de um mercado em massa. A Internet pode identificar o cliente permitindo que se possa oferecer anúncios e material orientado às suas necessidades, tudo isso em larga escala.

Se por um lado, as perspectivas para o crescimento do comércio na Internet são enormes, por outro, surgiram problemas associados a um comércio inovador, abrangente e sem fronteiras.

Um dos problemas relacionados ao comércio eletrônico é a questão da segurança, por exemplo, como assegurar a autenticidade das transações realizadas, ou seja, como garantir quem foi, realmente, o emissor de um determinado pedido de compras, e como garantir que a ordem foi emitida numa determinada data.

E também como lidar com fraudes e falsificações em um mundo digital? No mundo real, o comércio é estabelecido dentro de limitações que não existem no mundo digital, onde, apesar do enorme potencial para a fraude, tem disponível medidas tão efetivas que podem torná-lo relativamente confiável.

Quando se discute segurança da informação, em geral, associa-se quatro objetivos principais: confidencialidade, integridade, autenticidade e não-repudiação. A confidencialidade garante que informações relevantes não sejam acessadas por pessoas não autorizadas. A integridade objetiva a consistência dos dados, não tornando possível a alteração ou eliminação das informações transmitidas ou armazenadas. A autenticação prevê garantias da procedência das informações. Finalmente, a não-repudiação permite que não seja possível a rejeição da ocorrência de uma determinada ação, seja através da

negação do envio ou do recebimento de uma determinada informação. Esses objetivos são fundamentais à efetivação plena das transações comerciais, sejam as realizadas pelo método tradicional ou não.

1.1 Objetivos

1.1.1 Objetivo Geral

O objetivo geral deste trabalho é fazer uma avaliação sobre os assuntos de segurança que envolve o comércio eletrônico e suas aplicações, discutir os processos e os requisitos de segurança em aplicações do comércio eletrônico, os quais geralmente vão além das exigências tradicionais de segurança de redes, e propor uma metodologia para a agregação de segurança nos sistemas de comércio eletrônico.

1.1.2 Objetivos Específicos

- Apresentar um panorama geral sobre comércio eletrônico;
- Apresentar os conceitos essenciais sobre segurança da informação, e estudar os principais mecanismos de segurança utilizados no comércio eletrônico;
- Estudar os sistemas de comércio eletrônico e identificar os processos numa aplicação de comércio eletrônico;
- Estudar os aspectos de segurança relacionados ao comércio eletrônico;
- Fazer levantamento do estado da arte quanto a segurança no comércio eletrônico;
- Apresentar os projetos que estão sendo desenvolvidos pelo LabSEC (Laboratório de Segurança) da UFSC e de outros centros de pesquisa, quanto a segurança no comércio eletrônico;
- Propor um programa de trabalho de pesquisa para segurança no comércio eletrônico;

- Propor uma metodologia de desenvolvimento para os projetos a serem desenvolvidos;

- Identificar os requisitos globais de segurança no comércio eletrônico, os quais deverão ser observados no desenvolvimento dos projetos de pesquisa a serem desenvolvidos;

- Apresentar um software que sirva como ferramenta para auxilar a análise do desempenho de protocolos criptográficos.

1.2 Motivação

O meu interesse por soluções para Internet é antiga, mas a decisão de desenvolver a minha dissertação sobre segurança no comércio eletrônico surgiu a partir da disciplina do mestrado de Redes de Computadores, onde este assunto foi abordado.

Ao pesquisar sobre o assunto, me deparei com uma nova área e de pouca pesquisa no Brasil, onde as técnicas de segurança utilizadas desenvolvem soluções apenas para um processo específico no comércio eletrônico, como por exemplo o pagamento.

Assim pude definir a minha proposta, que é desenvolver uma solução para o comércio eletrônico, o qual deverá ser encarado como uma nova forma de fazer negócios, onde existem vários participantes (comerciantes, clientes, parceiros, bancos, etc.) que fazem parte de um sistema, e em determinado momento eles realizam transações (compra, venda, pagamento, entrega, etc.). Esta solução procura garantir a segurança tanto das transações eletrônicas utilizadas durante o processo, quanto aos interesses particulares das partes envolvidas.

1.3 Trabalhos Correlacionados

Este trabalho, devido a sua amplitude de aplicação, está correlacionado a vários trabalhos na área de segurança.

Serão utilizados nesta dissertação os trabalhos científicos desenvolvidos por pesquisadores em projetos do LabSEC, que são:

- Cartório Virtual [PAS 01];
- Análise Segura de Crédito [BRO 01];
- Sistema Seguro de Atendimento ao Cliente (SAC Seguro) [GHI 01];
- Auditoria de publicidade na web [GHI 02];
- Compras Seguro [PER 02].

Estes trabalhos serão apresentados no capítulo 5. Esta dissertação de mestrado também faz parte dos projetos do LabSEC.

Também estão correlacionados a este trabalho as pesquisas relacionadas a segurança no comércio eletrônico desenvolvidas por outros grupos de pesquisa, obtidos em artigos de revistas científicas e em congressos da área.

As linhas de pesquisa identificadas, e que estão relacionadas com este trabalhos são:

1. Segurança dos dados e sistemas de comércio eletrônico [MAN 00], [THU 01], [NGA 02], [OPP 99];
2. Segurança Individual [MAR 02], [NGA 02], [OPP 99];
3. A utilização de componentes que ajudam os usuários a resolver questões empresariais são muito discutidas, tais como a utilização de agentes móveis e o XML [WAN 02], [GUA 02], [COR 99];
4. Questões legais quanto a regulamentação do comércio eletrônico, assinatura digital, documentos eletrônicos [MUE 02], [TOR 01], [STA 01].

1.4 Materiais e Métodos

Esta dissertação está fundamentada na atualização de pesquisa bibliográfica, realizada principalmente em artigos e publicações recentes.

Para saber o estado da arte atual no Brasil, foram levantados os principais congressos de segurança no Brasil.

Para o levantamento bibliográfico também foram estudadas revistas científicas da área, tais como: ACM, ELSEVIER e IEEE.

Também foram estudados os projetos do LabSEC, do qual este projeto faz parte.

1.5 Conteúdo desde Documento

Este trabalho está estruturado da seguinte forma: o capítulo 2 apresenta um panorama geral sobre comércio eletrônico, suas as principais definições, etapas da comercialização, suas vantagens e desvantagens em relação ao comércio tradicional e questões relacionadas a legislação do comércio eletrônico. O capítulo 3 apresenta conceitos essenciais sobre segurança da informação, em que serão discutidas as suas características desejáveis, e os principais mecanismos de segurança utilizados no comércio eletrônico. O capítulo 4 estuda os sistemas de comércio eletrônico e identifica os processos numa aplicação de comércio eletrônico, apresenta os aspectos de segurança relacionados, e faz um levantamento dos estudos que estão sendo feitos atualmente quanto a segurança no comércio eletrônico. O capítulo 5 apresenta o levantamento feito sobre os projetos de pesquisa que estão sendo feitos sobre segurança no comércio eletrônico, pelo LabSEC e outros pesquisadores. No capítulo 6 é proposto um programa de trabalho de pesquisa sobre segurança no comércio eletrônico. O capítulo 7 propõe uma metodologia de desenvolvimento para os projetos a serem desenvolvidos, apresenta os requisitos globais de segurança identificados para o comércio eletrônico, e apresenta um software que serve como ferramenta para auxilar a análise do desempenho de protocolos criptográficos desenvolvidos. E finalmente, o capítulo 8 apresenta as considerações finais do

trabalho desenvolvido.

Capítulo 2

Comércio Eletrônico

2.1 Introdução

As organizações, tanto em nível mundial como nacional, tem passado por profundas mudanças nos últimos anos, as quais têm sido diretamente relacionada com a Tecnologia da Informação (TI). Essa relação engloba desde o surgimento de novas tecnologias, ou novas aplicações, para atender às necessidades do novo ambiente, até o aparecimento de novas oportunidades empresariais criadas pelas novas tecnologias ou novas formas de aplicação [ALB 99].

Atualmente, algumas das características do novo ambiente empresarial, tais como globalização, integração interna e externa das organizações, entre outras, têm confirmado as tendências da criação e utilização do comércio eletrônico, que já é considerado uma realidade.

O crescimento da Internet está provocando mudanças neste cenário de negócios, oferecendo às empresas um novo e poderoso canal de comunicação com o mercado e possibilitando o surgimento de comunidades virtuais. Esta nova tecnologia, inserida na realidade das empresas de forma cada vez mais atuante, tem possibilitado a atuação das empresas no comércio eletrônico.

O objetivo deste capítulo é apresentar um panorama geral sobre comércio eletrônico, e está estruturado da seguinte forma: a seção 2.2 apresenta as principais

definições sobre o comércio eletrônico. A seção 2.3 descreve as etapas da comercialização. A seção 2.4 destaca os objetivos do comércio eletrônico, e a seção 2.5 os casos em que pode-se aplicar o comércio eletrônico. Na seção 2.6 são apresentadas as modalidades de formas de pagamentos para a comércio eletrônico. Na seção 2.7 são destacadas as vantagens e desvantagens do comércio eletrônico em relação ao comércio tradicional.

2.2 Definição

O comércio eletrônico é a realização dos processos de negócio num ambiente eletrônico, por meio da aplicação intensa das tecnologias de comunicação e de informação, atendendo aos objetivos de negócio. Os processos podem ser realizados de forma completa ou parcial, incluindo as transações negócio-a-negócio, negócio-a-consumidor e intra-organizacional, numa infra-estrutura predominantemente pública de fácil e livre acesso e baixo custo [ALB 99].

A maioria das pessoas pensam que comércio eletrônico significa fazer compras *on-line*. Mas usar a Internet para fazer compras é só uma pequena parte do universo do comércio eletrônico. O termo também se refere a transações de estoque *on-line*, compra ou *download* de software sem a necessidade de ir a uma loja, entre outros . Além disso, comércio eletrônico inclui conexões negócio-a-negócio que tornam compras mais fáceis para grandes corporações.

Os modelos básicos de comércio eletrônico são:

Negócio-a-negócio: Neste modelo as partes são duas organizações que interligam-se, geralmente em uma relação de fornecedor ou usuário de produtos, serviços ou informação;

Negócio-a-consumidor: É a versão eletrônica da venda a varejo. Envolve uma organização e um consumidor e geralmente envolve estratégias de pagamento aceitas pelas partes. Este modelo teve grande crescimento, principalmente a partir de 1995 quando a Internet abriu-se para as empresas, assim como houve um crescimento concomitante dos provedores de acesso e informação;

Negócio-a-governo: Neste modelo as organizações se relacionam com as administrações federais, estaduais ou municipais dos governos. No Brasil observa-se o SIAFI (Sistema Integrado de Administração Financeira) ou SIAFEM (para os estados e municípios) e o sistema de compras do Ministério da Administração;

Consumidor-a-governo: O consumidor relaciona-se com o Estado para a obtenção de serviços, benefícios ou informações. São exemplos o acesso a informações sobre procedimentos a realizar para aquisição de direitos, andamento de processos (tribunais), declaração de imposto de renda e consulta de multas de trânsito;

Consumidor-a-consumidor: Transações entre consumidores finais. Sítios que funcionam como leilões virtuais permitindo aos consumidores a publicação e licitação de produtos;

Consumidor-a-negócio: Transações entre consumidores e empresas, por exemplo, passageiros que fazem lances por passagens aéreas, cabendo as empresas aéreas aceitar ou não.

2.3 Etapas da Comercialização

O conceito de comércio eletrônico é um pouco evasivo. Para tanto, deve-se ter atenção para as várias diferenças entre a comercialização convencional e a eletrônica. O ato de comercializar é mostrado aqui como uma relação de troca entre duas partes, nas quais uma entrega uma mercadoria ou serviço para a outra, mediante o recebimento de uma contrapartida, ou a promessa de pagamento futuro, normalmente de alguma forma monetária existente atualmente.

Segundo Roselino [ROS 00], normalmente as etapas de comercialização comum é feita em quatro etapas: visualização da mercadoria, negociação, pagamento e uma possível entrega.

A etapa inicial é a **apreciação da mercadoria** onde o potencial comprador busca agregar informações a respeito das especificações do produto e a conseqüente adequação deste as suas necessidades ou desejos iniciais. Em uma comercialização

convencional esta etapa pode incluir um exame detalhado do produto, questionamento de suas características ao vendedor, peculiaridades como: prazo de validade, qualidade do material utilizado, embalagem, garantias, etc. Porém podemos ressaltar que esta etapa guarda características próprias ao se tratar de produtos distintos. Poderíamos citar que na comercialização de um automóvel usado, esta etapa guarda importância e poderá ser realizada inclusive mediante consulta a uma terceira parte com conhecimentos específicos, como o mecânico de sua confiança, já no caso da venda de pães em uma padaria esta etapa se cumpre mediante questionamentos simples como a sua visualização ou a notação de outras condições, como por exemplo a higiene do local. Finalizada esta etapa e mantido o interesse do comprador em levar a mercadoria mediante o valor estipulado passa-se à etapa seguinte.

A **negociação** é a etapa seguinte onde o comprador deverá estabelecer com o vendedor condições para a realização da transação, a respeito das quais estariam em melhor acordo. Nesta fase normalmente inclui-se questões como: preços, quantidades, condições e prazos para o pagamento e a forma de entrega da mercadoria. Possui características específicas conforme o tipo de mercadoria que está sendo negociada. Esta etapa é finalizada geralmente com um acordo entre ambas as partes, em consonância com as condições estabelecidas para a transação.

O **pagamento** consiste em ceder um determinado valor (normalmente na sua forma monetária) por parte do comprador em favorecimento do vendedor, e deve realizar-se no ato, ou ainda através de uma promessa de pagamento futuro. Normalmente, nas transações mais comuns isso ocorre por meio da entrega de determinada quantia em moeda corrente, assinatura de um cheque, transferências eletrônica de valores, assinatura de uma nota promissória, etc.

A **entrega** (feita em alguns casos) realiza-se com o comprador recebendo a mercadoria em algum lugar determinado. Como foi dito, a forma como esta se efetiva dependerá das características físicas da mercadoria. Em transações comerciais de balcão a entrega ocorre normalmente no ato do pagamento. Em alguns casos, quando a mercadoria é dotada de características que dificultam seu transporte, a entrega pode se dar por meio da utilização de serviços especializados de transporte, como os Correios.

Em outros casos, como a aquisição de um imóvel este se dará mediante a oficialização da transação envolvendo transferência patrimonial em algum cartório.

Mas e o comércio eletrônico? Para entender como funciona este novo processo de comercialização é preciso entender como funciona o mais convencional e fazer algumas modificações peculiares da própria Internet, mas que, por se tratar de negócios virtuais alguns elementos seriam inviáveis de se comercializar no sistema eletrônico.

No comércio eletrônico a realização da negociação não enfrenta grandes dificuldades para se adaptar ao meio eletrônico, uma vez que a disposição de uma tabela de preços inicial em um sítio é facilmente realizável. Bem como a eventual realização de uma discussão a respeito de condições entre as partes pode ser efetuada por meio de *e-mails*, ou ainda de conversas através da rede.

Contudo, a efetivação do pagamento é problemática. Mas a evolução dos mecanismos de segurança na rede tem permitido a realização de transações envolvendo cartões de crédito, ou ainda movimentação entre contas bancárias através de boletos de pagamento.

Os principais ítens que impedem o avanço e popularização do comércio eletrônico se concentram na realização da apreciação da mercadoria e da entrega da mercadoria [ROS 00].

A apreciação da mercadoria tende a inviabilizar a realização de transações de produtos com características distintas e complexas, ou desconhecidas pelo potencial comprador. Produtos de marcas reconhecidas ou de padronização generalizada podem passar por esta etapa sem grandes dificuldades.

A entrega da mercadoria é que parece ser o grande impedimento para compreendermos o verdadeiro potencial transformador do comércio eletrônico via Internet. Na comercialização eletrônica deve-se incluir a realização da troca da mercadoria para sua completa efetivação. A verdadeira característica inovadora do comércio eletrônico estaria relacionado à possibilidade de se efetivar a entrega de determinadas mercadorias também por meio eletrônico, completando toda a transação comercial. Para isso a empresa deve estar com um sistema de logística bem apurado e consistente e não

deixar-se levar por uma eventual demanda, que é muito comum numa rede que é mundial.

2.4 Objetivos do Comércio Eletrônico

Cada empresa que busca soluções de comércio eletrônico possui uma meta muito individual. O objetivo de uma empresa pode ser filiar-se a um centro comercial, pode ser apenas abrir uma loja virtual e vender alguns de seus produtos, ou ainda pode querer associar-se a fornecedores e vender vários produtos diretamente deles. De uma maneira geral, os objetivos principais do comércio eletrônico são [CON 00]:

- Promover uma apresentação eletrônica de bens e serviços;
- Aumentar a proporção de vendas dos produtos bem como a divulgação e marketing dos mesmos;
- Fornecer um ambiente de comércio que seja atrativo ao cliente, e que seja de fácil navegação[1];
- Oferecer formas de pagamento e transporte que sejam acessíveis ao público-alvo, melhorando assim o tempo e a qualidade dos serviços prestados;
- Automatizar transações entre fornecedores e empresas de modo a minimizar custos e agilizar processos.

Podem existir outros objetivos secundários, dependendo do objetivo final da empresa que deseje implementar uma solução de comércio eletrônico.

2.5 Casos que Podemos Aplicar o Comércio Eletrônico

Alguns produtos, devido a sua natureza, não se adaptam facilmente à forma de comercialização eletrônica.

[1]Navegar significa movimentar-se entre as páginas de um sítio.

Alguns exemplos destas formas de comercialização eletrônica incompletas são o atendimento de pedidos de pizzas. Outro exemplo é a venda de automóveis usados, onde a apreciação da mercadoria é de uma importância sem igual, por isso dificilmente teriam condições de se adaptar à comercialização eletrônica.

Mas alguns produtos podem adaptar-se plenamente a este novo canal de comercialização, e para estes as oportunidades são enormes, trazendo novas e importantes perspectivas.

Estes produtos seriam aqueles dotados de características que permitem inclusive a realização da entrega por meio eletrônico, e dotadas de dois atributos, sendo que o primeiro diz respeito a possibilidade de digitalização do produto, e o segundo com respeito a possibilidade de transmití-lo por meio eletrônico.

Os produtos que se enquadram nesta categoria são de dois tipos: aqueles já originariamente pertencentes à este meio, como os programas de computador, e aqueles que são adaptáveis à este, como por exemplo jornais e revistas impressas que podem ser digitalizados e disponibilizados para acesso nos meios eletrônicos.

Ainda tem-se os outros produtos que estão relacionados à indústria de audiovisual, uma vez que o aprimoramento das tecnologias de multimídia tem permitido a transferência destes produtos para o mundo da informática. Entre esses produtos está a telefonia, cujas experiências deixam de ser apenas curiosidade para aficcionados e passam a despertar interesses comerciais, uma vez que a digitalização, compactação e transmissão da voz humana em tempo real, com qualidade satisfatória se coloca como um serviço tecnicamente possível, adequando-a ao segundo atributo que é a possibilidade da transmissão para a realização da comercialização eletrônica completa e segura.

2.6 Formas de Pagamento

O objetivo fundamental das tecnologias criadas para possibilitar a realização de transações comerciais de forma eletrônica reside em garantir a segurança do processo [ROC 99]. Diversas modalidades de pagamento têm sido propostas, com diferentes níveis de segurança, algumas de cunho genérico, e outras de cunho específico, mas todas

elas podem ser classificadas, segundo Bernstein [BER 97], em três grupos: os sistemas de pagamento baseados de **débito/crédito**, aqueles baseados em **moedas eletrônicas** e aqueles que permitem transações *on-line* com **cartões de crédito**. Para fins comparativos, são apresentados aqui os conceitos fundamentais de cada uma destas abordagens.

2.6.1 Pagamento Baseados em Sistemas de Débito/Crédito

Os sistemas de débito/crédito, já existentes na Internet desde 1994, permitem aos usuários a efetivação de compra e venda de produtos e serviços utilizando por exemplo o correio eletrônico. Considerando esta abordagem, é necessário aos usuários a criação de contas de correio eletrônico na entidade provedora de sistema, cuja assinatura é realizada através do envio de uma requisição ao servidor de correio eletrônico do provedor dos serviços, e a principal vantagem identificada nesta solução é que não há a necessidade do envio de informações sensíveis de pagamento pela rede.

O procedimento de cadastramento é normalmente executado baseado no protocolo FTP ou Telnet. A entidade provedora responde através de correio eletrônico, enviando uma mensagem com o número da requisição, e um número telefônico, geralmente gratuito, para o qual o usuário deve ligar a fim de fornecer o número do cartão de crédito e confirmar as informações enviadas. Há ainda um procedimento adicional relativo à senha, a fim de garantir o sigilo dos futuros processamentos, e posteriormente a entidade provedora do serviço envia outra mensagem de correio eletrônico confirmando a criação da conta do usuário. A transação típica desta modalidade de pagamento é ilustrada na figura 2.1.

Um ponto fundamental para a garantia da segurança da transação nesta modalidade de pagamento, consiste no envio da confirmação do usuário (passo 3 e 4), que é exigida para a concretização da transação. Além desta característica, o modelo em questão opta por não trafegar os números de cartões de crédito na Internet.

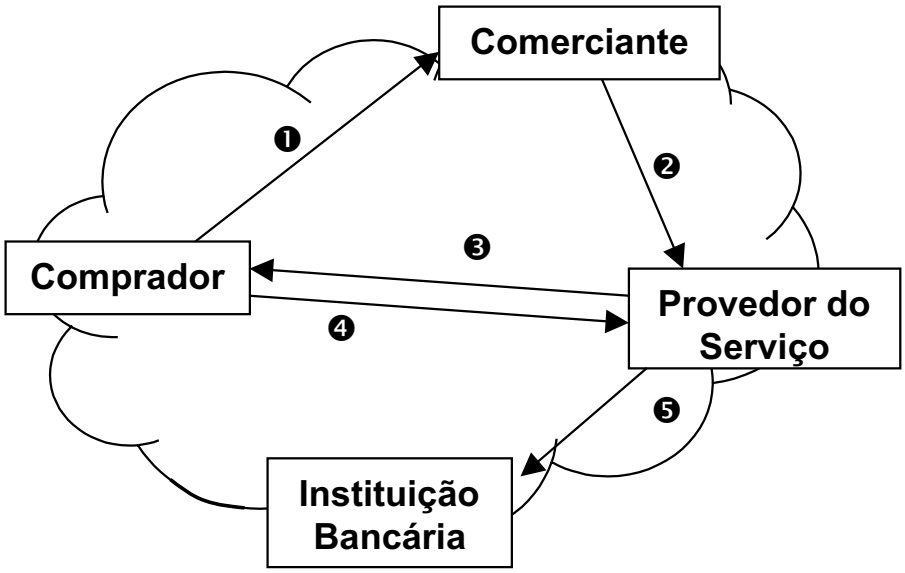

Figura 2.1: Fluxo de transação baseada em sistemas de débito/crédito: Após ter realizado o processo de navegação na Internet, o comprador monta o seu pedido de compra, fornecendo o número da sua conta ao Comerciante (passo 1). Para proceder a autorização de compra, o Comerciante envia a solicitação da transação para o provedor de serviço (passo 2), sendo que este passo é normalmente executado através do envio de uma mensagem de correio eletrônico, ou através de Telnet. O provedor de serviço envia uma mensagem de correio eletrônico para o Comprador (passo 3), solicitando que este confirme a validade da transação em questão e o seu compromisso de pagamento. O Comprador responde à solicitação de confirmação, também através de correio eletrônico (passo 4). Depois de realizado o pagamento à Administradora de Cartões de Crédito, o provedor do serviço efetua o depósito do dinheiro na conta corrente do Comerciante, na instituição bancária pré-determinada (passo 5).

2.6.2 Pagamentos Baseados em Moedas Eletrônicas

Esta modalidade de sistema de pagamento baseia-se no conceito de dinheiro digital, uma espécie de moeda virtual, que permite a compradores, comerciantes e bancos, efetivarem transações comerciais através da Internet, e tem seu principal exemplo no sistema conhecido como DigiCash, desenvolvido pela empresa DigiCash Inc. [EC 01]. Neste modelo, o dinheiro digital pode ser armazenado em carteiras eletrônicas, na memória do computador, ou carregado em cartões inteligentes.

Uma das características fundamentais desta tecnologia é garantir o ano-

nimato do comprador/pagador através de protocolos criptográficos. O mecanismo desenvolvido por este modelo, garante que a identidade do iniciador da transação permanecerá desconhecida. A identificação e o não-repúdio de cada transação eletrônica são garantidas através do uso do algoritmos de criptografia assimétrica [ROC 99].

Para tornar o modelo viável em um sistema interbancário, é necessário que o banco do Comerciante possua as chaves públicas de todos os bancos usados por seus clientes, a fim de que os requisitos de segurança possam ser verificados. A implementação deste modelo na prática, no entanto, têm se mostrado relativamente complexa, em função exatamente desta característica. A figura 2.2 apresenta o fluxo de informações do modelo em questão.

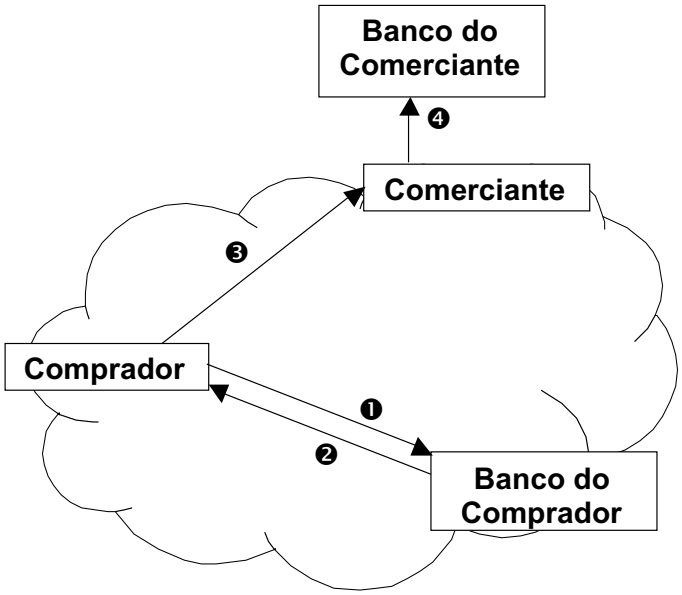

Figura 2.2: Fluxo de transação baseada em moeda eletrônica: A primeira etapa do processamento consiste no *download* de dinheiro digital da conta bancária do comprador para o computador. Após a criptografia, é criado um envelope, que é enviado até o banco do comprador, onde as moedas são validadas e recebem valores (passo 1). Uma vez processada a validação das moedas, e feito o débito na conta do correntista (comprador), o banco assina digitalmente as moedas, e as envia de volta para o correntista (passo 2). Quando desejar efetuar uma compra, o comprador paga ao comerciante com as moedas (passo 3), efetivando uma transação anônima, uma vez que o comerciante não tem acesso à identidade do comprador. Após realizado o pagamento, o comerciante envia então as moedas para o seu banco, a fim de que seja feita a validação, através da verificação de veracidade da assinatura digital do banco emissor da referida moeda (passo 4).

2.6.3 Pagamento Baseados em Transações On-Line com Cartões de Crédito

Esta modalidade é considerada a mais abrangente no atendimento aos requisitos de segurança para sistemas de pagamento eletrônico na Internet, em virtude do amplo conjunto de procedimentos necessários para efetivação das transações.

A recomendação atual é o SET - Secure Electronic Transactions, desenvolvido por um consórcio de empresas lideradas pela Visa e Mastercard, e descrito em maiores detalhes na seção 3.4.8, página 36 do capítulo 3.

2.7 Comércio Tradicional x Comércio Eletrônico

2.7.1 Vantagens do Comércio Eletrônico

Um sistema de comércio eletrônico bem planejado e implementado é capaz de trazer inúmeras vantagens em comparação com o comércio tradicional [CON 00]. Eis algumas delas:

- Os sistemas de comércio eletrônico possuem como uma das principais vantagens o aumento considerável na negociação de bens e serviços;
- Existe o aprimoramento das relações com os clientes, devido à interação com os mesmos através de linhas diretas (correio eletrônico, telefone) ou através de propaganda e marketing no próprio sítio. Isto causa maior interesse e confiança por parte do cliente, que percebe o esforço que a empresa está empregando para melhor serví-lo;
- O custo para convencer e conquistar um cliente é inferior ao custo que seria gasto em um comércio tradicional. E conquistar a confiança do cliente é crucial para o sucesso do comércio;
- O tempo que envolve todo o processo de compra, venda e entrega do produto é otimizado. Através da racionalização dos processos e de pessoal;

- Existe a redução de despesas com o transporte, armazenamento, distribuição, bem como a redução de despesas com estoque através da automação e redução dos tempos de processamento;

- Maior competitividade com outras empresas e expansão do mercado. O planejamento de um bom sistema de marketing e propaganda pode migrar o mercado de atuação de locais e regionais para nacionais e internacionais, com requisitos mínimos de capital, estoque e pessoal;

- A comunicação e coordenação dentro das empresas tendem a melhorar, em função do aumento do uso da informação tecnológica, dos sistemas de integração e da própria rede. As tarefas são divididas de um modo mais otimizado, e as áreas profissionais tendem a ser mais definidas. Como um exemplo, suponha uma empresa que possua um sistema de comércio eletrônico que venda CDs. As funções de cada profissional são bem definidas: um profissional cuida da parte da confecção do catálogo de CDs (*compact disk*), inserindo, retirando e modificando detalhes dos produtos; outro profissional cuida da comunicação com os fornecedores; um profissional cuida da parte de propaganda e marketing do produto; existem profissionais da área de informática e tecnológica para suporte, e assim por diante. Todos estes profissionais estão em constante comunicação, mas nenhum interfere na atividade do outro;

- Surge um contato mais direto com os fornecedores, podendo ser feito até mesmo através de sistemas interligados, eliminando a necessidade de representantes e inventários, e aumentando a disponibilidade de produtos para os clientes.

2.7.2 Desvantagens do Comércio Eletrônico

A implantação de um sistema de comércio eletrônico necessita de alguns requisitos que não são necessários no comércio tradicional. O objetivo desta seção é ilustrar as desvantagens que, apesar de existirem, possuem soluções que podem ser implementadas ou que no momento estão sendo estudadas [CON 00]. Eis algumas delas:

- Muitas vezes as empresas que buscam as soluções de comércio eletrônico não se dão conta do planejamento de pessoal e de estrutura que são necessários. Ao implantar uma solução de comércio eletrônico é preciso definir claramente quem são as pessoas e quais as funções de cada um no processo de venda. Uma pessoa que controla a interação com fornecedores não deve controlar ao mesmo tempo a liberação de boletos bancários ou de pagamento de produtos; isto poderia causar confusão e problemas. Esta desvantagem pode ser contornada com uma boa fase de planejamento, incluindo divisão de tarefas e orçamento;

- Atualmente, os sistemas de comércio eletrônico não permitem uma comunicação direta e livre com os vendedores. Existem mecanismos como Agentes Inteligentes - um sistema que possui a capacidade de tomada de decisões, as quais podem aumentar a automatização das tarefas - que estão sendo desenvolvidos para melhorar a interação entre o cliente e o vendedor [GUA 02];

- Apesar de todo esforço voltado para a segurança, existem ainda problemas em torno desta questão. Criptografia, certificação digital e autenticação são alguns recursos que estão sendo utilizados para garantir maior segurança em compras *on-line*. Vale lembrar que é mais fácil um cartão de crédito ser roubado ou clonado em um estabelecimento comercial (um restaurante, por exemplo) do que seu número ser conseguido através de uma compra *on-line* ou de sistemas de comércio eletrônico;

- Os sistemas de comércio eletrônico possuem uma boa automatização, porém ela está um pouco distante de ser a ideal. A parte do processo contábil e da transferência efetiva de fundos são prejudicadas, pois durante o processo da venda de um produto são as que requerem mais tempo. Existem projetos de sistemas que permitem um maior controle de fluxo de caixa, estocagem, comunicação com fornecedores e controle de recursos, mas ainda não existe nenhuma forma de integração total e real [CON 00];

- A lista de requisitos do hardware e comunicação não é muito extensa, porém é um pouco rígida. Estas definições rígidas devem ser determinadas com relação à

estrutura e dados estabelecidos, e com isso pode-se criar barreiras em função desta rigidez devido ao tempo e custo resultantes para a disseminação dos sistemas de comércio eletrônico;

- Embora existam atualmente várias tecnologias que possam auxiliar o sistema de comércio eletrônico, muitas delas ainda não estão disponíveis o mercado brasileiro. Um exemplo é o processamento e cobrança *on-line* de pagamentos com cartão de crédito, que nos Estados Unidos já está em funcionamento há algum tempo, e no Brasil só existe em grandes empreendimentos ligados a bancos, como por exemplo VisaMall e o E-card Unibanco.

2.8 Conclusão

É seguro afirmar que a tecnologia de informação contribui com mudanças significativas nos setores de comércio e serviços, e que a Internet mudou a maneira de se fazer comércio e promete também inovações na área de serviços. O comércio eletrônico via Internet permite que empresas de pequeno porte possam competir com grandes empresas, além de estreitar laços entre cliente e fornecedor, ampliando a abrangência da empresa.

Apesar das inúmeras vantagens do comércio eletrônico, um dos principais pontos que limita o crescimento e aceitação ampla do comércio eletrônico é a falta de segurança.

Garantindo a segurança, a tendência é que o comércio eletrônico cative cada vez mais um maior número de usuários devido a comodidade e personalização dos produtos.

Capítulo 3

Tecnologias de Segurança da Informação

3.1 Introdução

Para que o comércio eletrônico se torne uma realidade e para que exista maior aceitação e confiança nas transações entre as empresas e consumidores - participantes da negociação, o aspecto relacionado a segurança precisa ser resolvido.

Este capítulo apresenta conceitos essenciais sobre segurança da informação, em que serão discutidas as suas características desejáveis, e os principais mecanismos de segurança utilizados no comércio eletrônico. O capítulo está dividido da seguinte forma: a seção 3.2 descreve os conceitos fundamentais sobre segurança de informação; a seção 3.3 descreve sobre política de segurança; e a seção 3.4 aborda os mecanismos de segurança, descrevendo os que são utilizados no comércio eletrônico.

3.2 Conceitos Fundamentais

Segundo Garfinkel [GAR 99], um computador é seguro se você pode ter certeza que ele e seu software vão se comportar de maneira que você espera. Usando esta definição, a segurança na Internet é representada por um conjunto de procedimentos,

práticas e tecnologias usadas para proteger os servidores, usuários e suas empresas. A segurança protege os envolvidos de comportamentos inesperados.

Quando se discute segurança da informação, em geral associam-se quatro objetivos principais:

- **Confidenciabilidade:** garante que informações relevantes não sejam acessadas por pessoas não-autorizadas;
- **Integridade:** objetiva a consistência dos dados, não tornando possível a alteração das informações transmitidas ou armazenadas por uma organização;
- **Autenticidade:** provê garantias de procedência das informações;
- **Não-repudiação:** permite que não seja possível a uma pessoa ou organização a rejeição da ocorrência de uma determinada ação, seja através da negação do envio ou do recebimento de uma determinada informação.

Estes objetivos são fundamentais à efetivação plena das transações comerciais, sejam as realizadas pelos métodos tradicionais ou não. Ao assinarmos um cheque ou um recibo, por exemplo, estamos dando garantias de autenticidade. Os timbres, marcas d'água, selos de cartórios públicos, dentre outras identificações, são formas alternativas de autenticação de documentos. A integridade pode ser conferida pela grafia do autor, por exemplo. As cartas enviadas pelos correios tradicionais têm a confidencialidade garantida por amparo legal. O envio de correspondência registrada, com notificação de recebimento, constitui um exemplo típico de garantia de não-repudiação. Os métodos tradicionais terão correspondentes aos digitais numa infra-estrutura para o comércio eletrônico.

Alguns conceitos fundamentais para segurança da informação, tais como: ameaça, proteção, vulnerabilidade, ataque e risco, são apresentados a seguir de acordo com [WAN 00]:

Uma **ameaça** para um sistema de computadores pode ser definida ou identificada como qualquer circunstância ou evento que forneça algum potencial de vio-

lação de segurança, comprometendo a integridade, a confidencialidade, a disponibilidade da informação ou a disponibilidade de recursos.

Proteção (do inglês, safeguard) são controles físicos, mecanismos, políticas e procedimentos que protegem as informações e os recursos contra ameaças.

Vulnerabilidade são fraquezas nos meios de proteção, ou a falta destes.

Ataque é uma ação tomada por um intruso não autorizado que envolve a exploração de certas vulnerabilidades, visando violações de segurança. Os ataques são classificados como: passivos, os que ameaçam somente a confidencialidade dos dados; e ativos, que envolvem a modificação não autorizada e a negação de serviço, afetando a integridade e a disponibilidade das informações.

Risco é uma medida do custo de uma vulnerabilidade que incorpora a probabilidade de um ataque ocorrer com sucesso.

Na prática, a concepção de sistemas em que essas violações são totalmente evitadas é muito difícil. Todo o sistema em que a concepção está baseada no compartilhamento de recursos apresenta possibilidades sutis e não esperadas para a transferência de informação não autorizada entre duas entidades. Pode-se gastar uma quantidade ilimitada de tempo, dinheiro e esforço para buscar segurança, mas nunca se obtém uma total imunidade de problemas.

3.3 Políticas de Segurança

Manter as características desejáveis de segurança em um sistema e também assegurar a maneira como são garantidas as características desejáveis, estão fortemente vinculadas à definição de políticas de segurança do sistema, principalmente no comércio eletrônico onde o contexto geral do sistema é muito complexo [AND 00].

Segundo [WES 00], *"A política de segurança de um sistema é o conjunto de regras e práticas que determinam a maneira pela qual as informações e os outros recursos são gestionados, protegidos e distribuídos no interior de um sistema específico"*.

No mundo dos negócios, os especialistas afirmam a importância da elaboração de uma política de segurança corporativa, formalizando procedimentos para

o manuseio adequado das informações estratégicas.

A noção de política de segurança, descrita por Wangham [WAN 00], pode ser destacada em três ramos distintos: as **políticas de segurança física**, **políticas de segurança administrativa** e **políticas de segurança lógica**. A políticas de segurança física se ocupa com tudo que se refere à situação física do sistema a proteger. Neste ramo, em particular, são definidas as medidas contra a violação de segurança por incêndio, catástrofes naturais, etc.

A política administrativa trata de tudo que resulta da segurança sob o ponto de vista organizacional no seio da empresa, como a seleção do pessoal responsável pela segurança dos sistemas informatizados que fazem parte dessas políticas. Já a política de segurança lógica se interessa pelo conteúdo do sistema de informação. Esta política é encarregada de realizar todos os controles de acessos lógicos, especificando quem tem acesso a que e em quais circunstâncias. A política de segurança lógica pode ser decomposta da seguinte maneira: cada indivíduo que utiliza um sistema seguro deve se identificar e deve poder provar que ele realmente é a pessoa que pretende acessar um recurso ou informação do sistema. Estas duas idéias são definidas como política de identificação e política de autorização. Quando um usuário é identificado e autenticado, a política de autorização deve especificar quais são as operações que este usuário particular pode realizar no sistema.

A política de autorização é definida em parte por um conjunto de propriedades de segurança que devem ser satisfeitas e, além disso, por um esquema de autorização, que apresenta regras (chamadas regras de transição) que permitem modificar o estado de proteção do sistema. Por exemplo, uma propriedade de segurança poderá ser: “uma informação classificada que não deve ser transmitida a um usuário não habilitado a conhecê-la”, enquanto que uma regra do esquema de autorização poderá ser “o proprietário de uma informação que pode conceder um direito de acesso para esta informação a qualquer usuário” [WAN 00].

Todo sistema de comércio eletrônico tem que ter um documento que descreve a sua política de segurança. E todas as pessoas que operam o sistema de comércio eletrônico devem conhecer o conteúdo deste documento.

Para que seja possível projetar e monitorar a segurança de forma inteligente no sistema de comércio eletrônico, é necessário que se esclarer o que é permitido e a quem.

3.4 Mecanismos de Segurança

Os mecanismos de segurança concretizam a política de segurança, e para o comércio eletrônico estão baseados no uso das técnicas de: criptografia, assinatura digital, certificado digital e protocolos criptográficos.

3.4.1 Criptografia de Dados

A criptografia compreende a prática e o estudo da cifração e da decifração, ou seja, a cifragem de dados de forma que somente possam ser decodificados por uma entidade autorizada [oC 01]. Um sistema que realiza a cifração e a decifração é chamado de sistema de criptografia. Estes sistemas, em geral, envolvem um algoritmo específico que embaralha os dados utilizando de uma chave de conhecimento exclusivo do emissor e receptor dos dados. O resultado da cifração é chamado de texto cifrado. Um bom sistema de criptografia produzirá textos cifrados aparentemente randômicos, o que os tornam imunes a estudos estatísticos ou outros métodos de análise criptográfica para a obtenção do texto original sem o conhecimento da chave. A segurança de um sistema criptográfico depende do segredo das chaves utilizadas, podendo o algoritmo aplicado na geração do texto cifrado ser de conhecimento público. Quanto maior o universo de chaves possíveis, maior a dificuldade em se decifrar os dados cifrados através da tentativa de todas as possíveis chaves, conhecido como espaço de chaves.

A criptografia é usada para:

- Proteger a informação armazenada em trânsito;
- Deter alterações de dados;
- Identificar pessoas.

Porém, com a criptografia não é possível:

- Impedir que um intruso apague ou danifique os dados de uma instituição, estando eles criptografados ou não;
- Que um intruso modifique o programa de cifração. Desse modo o receptor não conseguirá decifrar com a sua chave.

A criptografia pode ser classificada em duas categorias, como sistema de criptografia simétrica, que tem como principais padrões o DES (Data Encryption Algorithm) e o AES (Advanced Encryption Standard), e o sistema de chave assimétrica (ou chave pública), e que tem como principal representante o RSA [BRO 01]

3.4.1.1 Criptografia Simétrica

A criptografia simétrica é caracterizada pelo uso da mesma chave nos processos de cifração e decifração [BAU 97]. A figura 3.1 ilustra um sistema de criptografia simétrico. Os parceiros da comunicação, A e B na figura, são os únicos conhecedores da chave k, o que faz este sistema ser conhecido também por criptografia com segredo compartilhado.

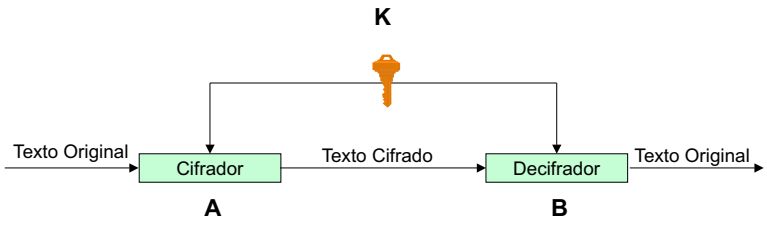

Figura 3.1: Sistema de criptografia simétrico: Utiliza criptografia simétrica para a troca de mensagens entre duas entidades (A e B). Utiliza um algoritmo criptográfico para cifrar a mensagem com uma chave k, a qual, também é utilizada para decifrar.

O uso de chaves privadas em sistemas de criptografia permite a garantia da confidencialidade na comunicação. Embora simples de implementar, o compartilhamento de chave tem a desvantagem de não permitir precisar, em determinado momento,

qual das partes originou uma mensagem, não sendo possível garantir a não-repudiação. Um sistema simétrico depende da confiança mútua entre as partes envolvidas na comunicação.

3.4.1.2 Criptografia Assimétrica

Proposto em 1976 por Whitfield Diffie e Martin Hellman, o sistema de criptografia assimétrico utiliza um par de chaves matematicamente relacionadas, uma para cifração e outra para decifração [BAU 97]. Cada chave é utilizada por uma das entidades envolvidas na comunicação, sendo a chave privada sempre mantida em segredo por um dos referidos sistemas. A chave pública, por sua vez, pode ser distribuída livremente. São dois os modos de uso da criptografia assimétrica ou por chave pública, como estes sistemas são também conhecidos: o de cifração e o de autenticação. No modo de cifração, ilustrado na figura 3.2, a chave pública é utilizada na cifragem da mensagem original.

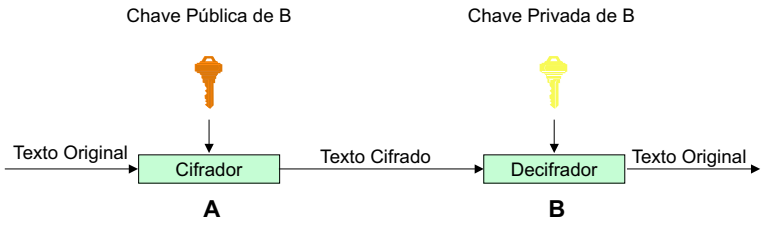

Figura 3.2: Sistema de criptografia por chave pública: modo de cifração. Neste caso A utiliza a chave pública de B para cifrar o texto, e esta mensagem só poderá ser decifrada por B com a sua chave privada.

Somente a entidade detentora da chave privada correspondente poderá decifrar a mensagem. O modo de cifração garante a confidencialidade e a integridade, da mesma forma que a criptografia simétrica, com a vantagem adicional do uso de apenas um par de chaves para todas as comunicações que tenham como destino o sistema detentor da chave privada.

No modo de autenticação, ao contrário do modo de cifração, a codificação é realizada utilizando-se a chave privada conforme ilustra a figura 3.3. Qual-

quer sistema que tenha conhecimento da chave pública correspondente pode decifrar a mensagem transmitida, não sendo possível garantir a confidencialidade. Por outro lado, como apenas o transmissor detém o conhecimento da chave privada, este modo é utilizado como forma de autenticação, além de garantir a integridade da mensagem. Uma outra vantagem é a garantia de não-repudiação, uma vez que somente o transmissor detém o conhecimento da chave utilizada na cifragem. Um sistema de criptografia capaz de operar nos modos de cifração e de autenticação é chamado de sistema reversível. Por outro lado, um sistema que implementa apenas um dos modos é chamado de sistema irreversível.

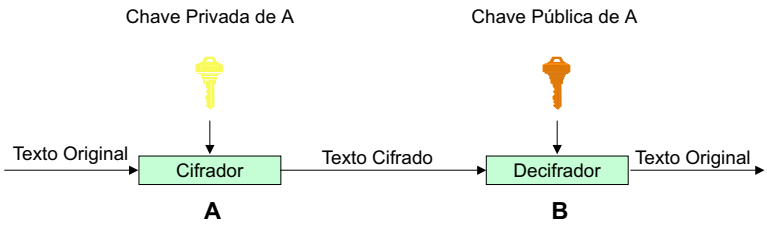

Figura 3.3: Sistema de criptografia por chave pública: modo de autenticação. Neste caso A utiliza sua chave privada para cifrar o texto, e esta mensagem poderá ser decifrada por B com a chave pública de A.

3.4.2 Função Resumo de Mensagem ou Hash

A idéia básica desta função é que um valor resumo serve como uma imagem representativa compacta (às vezes chamada de impressão digital ou "message digest") da cadeia de bits da entrada, e pode ser usada com se fosse unicamente identificável com aquela entrada. As funções resumo funcionam semelhante ao dígito verificador do CPF. Por exemplo, se um número qualquer do CPF for modificado, o dígito verificador também sofrerá a alteração. As funções resumo são usadas para garantir a integridade de dados [BRO 01].

Algumas das propriedades desta função:

- Deve ser computacionalmente inviável fazer a operação inversa, ou seja, dado um

resumo deve ser inviável obter uma mensagem original;

- Duas mensagens semelhantes devem produzir um mesmo resumo completamente diferente;

- Deve ser fácil e rápido produzir o resumo.

Uma boa função resumo tem uma característica chamada efeito avalanche. Isto significa que uma pequena mudança no arquivo de entrada acarreta uma grande e imprevisível mudança na saída.

A função resumo pode ser utilizada para garantir a integridade de uma mensagem. Isso pode ser feito enviando-se para Beto a mensagem e o resumo da mensagem cifrados com a chave privada de Alice. Beto decifra o resumo com a chave pública de Alice, calcula um novo resumo com base na mensagem recebida e compara os dois valores. Se forem iguais, a mensagem não foi alterada, garantindo-se dessa forma a sua integridade. A figura 3.4 ilustra este processo.

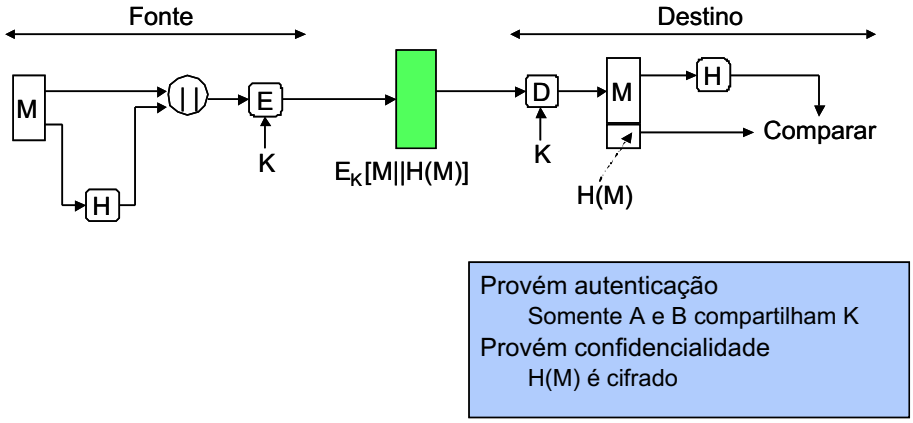

Figura 3.4: Função de condensação (HASH). A autenticação e confidencialidade é garantida através da aplicação da função HASH à mensagem *M* que é sucessivamente concatenada a *M*. Neste produto é aplicada a criptografia simétrica com uma chave *K*, e enviado para o destino. Para verificar a mensagem é feito o processo inverso. Utilizando-se da chave *K* o destino a decriptografa. A verificação da integridade da mensagem é realizada através da aplicação da função HASH à mensagem *M*, e comparando este resultado com o HASH recebido. Se o resultado for idêntico, a mensagem é autêntica, do contrário ela foi alterada.

3.4.3 Assinatura Digital

A assinatura digital é um algoritmo criptográfico com as seguintes características [SCH 96]:

Identificação: a assinatura garante a identificação do remetente que deliberadamente assinou a mensagem;

Não-Falsificação: a assinatura garante que o remetente, e ninguém mais, assine a mensagem;

Unicidade: a assinatura é parte de uma mensagem, e não pode ser utilizada em uma mensagem diferente;

Integridade: depois de uma mensagem ter sido assinada, ela não pode ser alterada;

Não-repúdio: a assinatura não permite que o remetente alegue não ter assinado a mensagem.

Uma assinatura pode ser obtida por meio de criptografia de um resumo da mensagem com a chave privada da entidade que está assinando a mensagem.

Métodos de assinatura direta, em que estão apenas envolvidos o emissor e o receptor na comunicação, possuem uma fraqueza: como a validade da assinatura depende da chave privada do emissor (aquele que assina), ele pode enviar um documento e mais tarde afirmar que a sua chave privada foi de alguma forma comprometida. Para resolver este impasse, existem protocolos para assinatura digital arbitrada, em que uma terceira parte, o árbitro, é responsável para garantir a validade da assinatura [STA 99].

Uma assinatura digital caracteriza-se por ser: fácil de se produzir, fácil de se reconhecer, e difícil de se falsificar. Assim, a assinatura digital imita a regra das assinaturas convencionais. Há, portanto, uma comprovação perante terceiros (que desempenham o papel de cartório) de que uma mensagem é uma cópia inalterada de uma produzida por um agente específico.

A capacidade de proporcionar assinaturas digitais depende de haver algo que o emissor original possa fazer que outros não possam. Isto pode ser obtido, por

exemplo, solicitando-se a uma terceira pessoa confiável, que tem prova da identidade do emissor original, para cifrar uma mensagem ou, então, uma forma reduzida da mensagem, denominada resumo.

3.4.4 Certificados Digitais

Um certificado digital é uma coleção de informações sobre a qual uma assinatura foi afixada por uma organização que goza da confiança de uma comunidade de usuários [BAU 97]. Esta organização é normalmente chamada de Autoridade Certificadora.

A Autoridade Certificadora assina o certificado de chave pública. Quem desejar confirmar a autencidade do certificado, basta pegar a chave pública da AC e verificar a assinatura do certificado.

No comércio eletrônico, certificados de vários tipos podem servir a vários propósitos. Um dos tipos de certificados mais importantes é o de chave pública, onde uma chave pública é seguramente associada a uma pessoa ou a um sistema em particular.

3.4.4.1 Certificados de Chave-Pública

Embora as chaves públicas sejam de livre distribuição, um usuário da mesma deve ter a certeza que está de posse da chave correta. Um certificado de chave pública, como o mostrado na figura 3.5, permite o fornecimento desta garantia.

Conforme pode ser observado na figura 3.5, um certificado de chave pública deve possuir uma identificação única, uma validade e a chave pública propriamente dita. A validade de um certificado é requerida como uma forma de diminuir as chances da chave privada correspondente à chave pública certificada ser descoberta. O uso de chaves temporárias aumenta consideravelmente a segurança do sistema como um todo. Acrescenta-se a estas informações o nome da Autoridade Certificadora, sendo este conjunto autenticado pela sua chave privada.

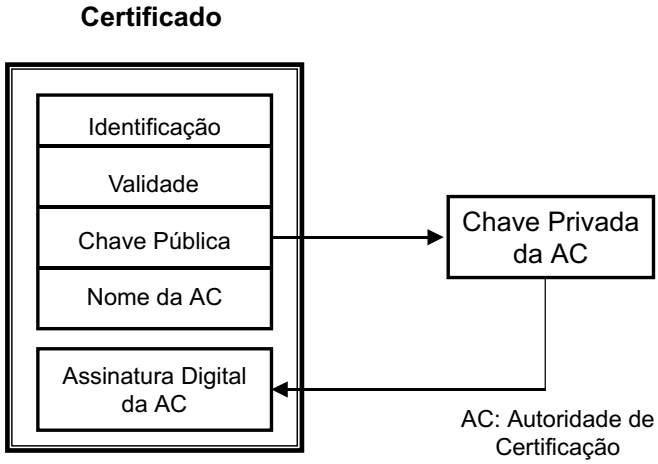

Figura 3.5: Certificado de chave-pública. O certificado de chave pública deverá possuir uma identificação única, uma validade, a chave pública e o nome da Autoridade Certificadora. Todo esse conjunto é autenticado pela sua chave privada.

3.4.5 Infra-estrutura de Chaves Públicas

Uma Infra-estrutura de Chaves Públicas - ICP, é um conjunto de ferramentas e processos para a implementação e a operação de um sistema de emissão de certificados digitais baseado em criptografia de Chaves Públicas [FEG 99]. Engloba também os detalhes do sistema de credenciamento e as práticas e políticas que fundamentam a emissão de certificados e outros serviços relacionados.

De forma genérica, para a emissão de um certificado digital há a necessidade de três módulos. O primeiro é o módulo público, o segundo módulo é a Autoridade de Registro e o terceiro é o módulo de Autoridade Certificadora. O módulo público é onde ocorre a requisição de um certificado, bem como a geração do par de chaves. O módulo de registro envia a requisição, assinada por ele, para a Autoridade Certificadora. A Autoridade Certificadora emite um certificado digital, disponibiliza-o em um diretório público e o transmite para a Autoridade de Registro.

Dependendo da política de certificação adotada em uma ICP, o grau de confiabilidade, definido pela classe, de um certificado pode variar. Por exemplo, um

certificado pode ter três tipos de classe:

Certificados Classe 1 - Não são utilizados para garantir a identidade do assinante. Elas representam uma simples verificação do e-mail do requisitante. Elas não servem para uso comercial quando forem exigidas provas de identidade e não se deve basear neles para esse tipo de uso.

Certificados Classe 2 - Podem oferecer garantias razoáveis, porém não a prova de erros, da identidade de um assinante com base em um processo *on-line* automatizado que compara o nome, endereço e outras informações pessoais do candidato contidas na solicitação do certificado com informações contidas em bancos de dados amplamente consultados. A confirmação baseia-se em critérios de propriedade de correspondência entre bancos de dados de terceiros e as informações contidas na solicitação.

Certificados Classe 3 - Para certificados Classe 3 é necessário o comparecimento, munido de documentos, do solicitante perante uma autoridade de registro para ser feito a identificação. A autoridade de registro confere os dados e identifica o solicitante fisicamente. Esta classe garante maior grau de confiabilidade na identificação do usuário constante no certificado.

3.4.6 Protocolos Criptográficos

Protocolo é um conjunto de passos durante a comunicação entre duas ou mais entidades, de forma a atingir um determinado objetivo [SCH 96]. Um protocolo criptográfico é um protocolo que utiliza criptografia, e tem como requisito a condição de que nenhuma entidade deve conseguir fazer mais ou saber mais do que está especificado no protocolo. Protocolos criptográficos, com base em mecanismos como criptografia simétrica ou assimétrica, funções resumo e assinaturas digitais, fornecem a infra-estrutura necessária para o desenvolvimento de aplicações seguras.

3.4.6.1 Características

Os protocolos criptográficos desenvolvidos devem ter as seguintes características [SCH 96]:

- Todas as entidades envolvidas no processo devem estar cientes, com antecedência, do protocolo como um todo e concordarem quanto ao seu uso;
- O protocolo nunca pode ser ambíguo;
- O protocolo deve ser completo, isto é, deve prever todas as situações possíveis, dentro do problema proposto.

3.4.7 SSL

Em julho de 1994, surge o padrão SSL (*Secure Sockets Layer* ou Camada de Socket Seguro). Trata-se de um protocolo de uso geral que através de técnicas de cifração garante autenticação dos sítios, cifração dos dados nas transmissões entre o navegador e o sítios e a verificação de integridade das informações transmitidas.

Desenvolvido pela Netscape, o SSL se tornou popular inicialmente devido ao seu navegador bastante difundido e pelo servidor Web da Netscape que propriciava este mecanismo de confidencialidade e autenticação. A idéia era estimular a venda dos servidores capacitados para criptografia, distribuindo um cliente gratuito que implementava os mesmos protocolos criptográficos. Desde então, o SSL foi incorporado a muitos outros servidores e navegadores, de forma que sua utilização já não é mais uma vantagem competitiva, mas uma necessidade [GAR 99].

Desde o início de 1996, os navegadores automaticamente cifram as informações, quando estão em uma sessão com um sítio comercial que está configurado para usar este protocolo. A maioria dos sítios utilizam este processo quando lidam com informações sigilosas ou sensíveis de seus clientes, como números de cartões de crédito e dados pessoais. Esta comunicação cifrada é chamada de ”conexão segura”. Isto é obtido com a utilização do SSL, criando uma conexão segura ao servidor, protegendo a informação que trafega na Internet. O SSL usa chave pública. No navegador Netscape

Navigator, quando está no modo seguro, ocorre o aparecimento de uma chave no canto esquerdo inferior da janela do Browser. O navegador da Microsoft Internet Explorer exibe um cadeado no canto direito inferior da tela. Outro modo para identificar que um sítio da Rede é assegurado por SSL é quando o URL começa com ”https” em vez de ”http”.

O SSL pode ser usado para quaisquer tipos de transmissões em que se queira segurança, não só as referentes a comércio eletrônico.

O padrão SSL resolve as questões referentes a segurança e privacidade na Internet, porém não resolve por exemplo o problema de autorização de pagamento e padrões de comunicação entre sítios e operadoras de cartão de crédito. Além disso, a idéia de o cliente informar seu número de cartão de crédito em todo sítios onde compra não é desejável.

3.4.8 Transações eletrônicas seguras - SET

Paralelamente ao surgimento das primeiras aplicações de comércio eletrônico, no começo dos anos 90, vieram à tona as primeiras pressões no sentido de desenvolver uma recomendação internacional para o processamento de transações eletrônicas sobre a rede. Os bancos se recusavam a aceitar processos de solicitação de pagamento originados na Web, e os comerciantes eram obrigados a utilizar sistemas *batch*, ou baseados em autorização por telefone. Assim, estas entidades pressionaram a indústria de software para que fosse desenvolvido uma tecnologia que atendesse aos diversos requisitos necessários para que essas transações fossem realizadas de forma segura.

Duas iniciativas independentes precederam o SET. A primeira, denominada STT (Secure Transaction Technology), foi lançada pelas empresas Visa e Microsoft em 1995. A Segunda, conhecida como SEPT (Secure Electronic Payment Protocol), foi desenvolvida pela Mastercard e seus aliados: Netscape, IBM, CyberCash e GTE. As duas iniciativas tinham objetivos idênticos, e suas implementações eram bastante similares, mas não o suficiente para lhes garantir compatibilidade [ROC 99].

A necessidade de criar uma recomendação para ser utilizado como padrão único, aberto, e que atendesse a todos os requisitos para a realização de transações

eletrônicas seguras na Internet, foi a motivação que levou as administradoras de cartão de crédito Visa International e Mastercard International a anunciar, em 1996, o início do desenvolvimento do SET - Secure Electronic Transaction. O acordo liderado por estas duas empresas envolve também outras grandes empresas, tais como GTE, IBM, Microsoft, Netscape, RSA, SAIC, Terisa e VeriSign. A especificação SET é coordenada pelo Secure Electronic Transaction Consortium (SETco), que foi desenvolvida pela Visa e Mastercard em 1997, para este fim.

A criação e o suporte do SET como uma tecnologia aberta inclui em seus objetivos oferecer informações detalhadas sobre o protocolo, de forma que os vários sistemas possam trabalhar em conjunto, a nível global, utilizando sempre que possível os padrões já existentes. Outro objetivo é o de assegurar a compatibilidade com quaisquer combinações de hardware e software. O SET visa conseguir a aceitação global através da facilidade de implementação, da integração com as aplicações clientes já existentes, da minimização nas mudanças no relacionamento entre compradores, comerciantes e administradoras de cartão, e por último pela eficiência do protocolo para as instituições financeiras.

De acordo com [VIS 97a],[VIS 97b], os objetivos do SET estão concentrados em atender aos seguintes requisitos:

I. Oferecer confidencialidade sobre as informações relacionadas a pagamentos e pedidos de compra

O atendimento a este requisito é particularmente importante no sentido de garantir que as informações sejam transmitidas de forma segura sem estar acessível a terceiros não autorizados. A possibilidade de um intruso interceptar o tráfego sendo realizado e filtrar informações tais como o número do cartão ou a data de validade do mesmo é encarado como uma fraude potencial caso este ponto não seja atendido.

II. Assegurar a integridade das informações trafegadas

O protocolo de pagamento deve assegurar que o conteúdo da mensagem não seja alterado durante a transmissão entre o originador e o destinatário. As

informações de pagamento sendo enviadas, contém dados pessoais do proprietário do cartão, informações sobre a compra sendo realizada e instruções sobre o pagamento propriamente dito. O SET deve fornecer mecanismos que assegurem que o conteúdo da mensagem esteja protegido de quaisquer modificações.

III. Oferecer a autenticação de que o proprietário de cartão é um usuário legítimo de uma conta em uma administradora de cartões

O protocolo de pagamento deve oferecer meios que assegure ao comerciante que o usuário com quem ele está estabelecendo a transação é de fato um usuário legítimo. Isso significa que o proprietário do cartão deve ser autenticado como sendo proprietário de uma conta de cartão de crédito válida.

IV. Oferecer a autenticação de que o comerciante está habilitado para aceitar pagamentos da administradora de cartões em questão, através do seu relacionamento com uma instituição financeira

Além de autenticar o proprietário do cartão de crédito, é de fundamental importância para a segurança das transações, que também o comerciante possa ser autenticado perante o comprador. Este deve ter acesso a um mecanismo que lhe permita confirmar que o comerciante com quem ele está estabelecendo a transação é de fato autorizado por uma determinada instituição financeira para realizar transações eletrônicas baseadas na especificação.

V. Assegurar o uso das melhores práticas de segurança e técnicas de projeto de sistemas, a fim de proteger todas as partes envolvidas na transação de compra eletrônica

Para o sucesso do modelo, não basta que todas as informações trafeguem adequadamente cifradas e todos os usuários sejam autenticados através de esquemas de certificação digital. Para que a implementação do SET atenda de fato, aos requisitos de segurança estabelecidos para o comércio eletrônico na Internet, é necessário a utilização de métodos e ferramentas adicionais que visem garantir a viabilidade do modelo como

um todo. O exemplo típico da fragilidade da proposta pura e simples do SET reside na questão do armazenamento dos certificados digitais, necessários a cada uma das entidades envolvidas, que caso não seja realizada de forma adequada, irá comprometer a segurança de todo o processo.

VI. Criar um protocolo que não dependa de mecanismos de segurança no nível de transporte

Para que o SET seja de fato uma tecnologia aberta, e realmente escalável, é de fundamental importância que ele não esteja vinculado a determinados algoritmos ou técnicas de criptografia, no nível de transporte, pois estão sujeitas a futuras modificações que inviabilizam sua utilização na especificação proposta para o SET. Por outro lado, é também importante, que o protocolo seja de tal forma flexível, que ele possibilite a utilização, caso necessária, de determinados mecanismos de segurança, pelo nível de transporte.

VII. Facilitar e encorajar a interoperabilidade entre provedores de software e serviços de rede

Os protocolos de pagamento devem oferecer a capacidade de operarem em diferentes plataformas de hardware e software, sem determinar preferência por nenhuma em particular. Além disso é fundamental que a interoperabilidade entre diferentes plataformas seja garantida através do uso de protocolos e formatos de mensagem específicos.

A implementação do SET, através de um conjunto de pedidos e respostas, simula através da Internet o funcionamento de um sistema tradicional de autorização de transações de compras com cartão de crédito, acrescentando algumas características mais complexas, destinadas a assegurar os requisitos de segurança exigidos. Os pares de mensagens que trafegam são encapsulados em blocos criptográficos antes de serem transmitidos através de rede, a fim de que garanta o sigilo e a integridade das mesmas. Diferentemente das abordagens desenvolvidas por tecnologias utilizadas anteriormente, o SET utiliza o conceito de que certificados digitais devem ser utilizados por todos os

envolvidos no processo, a fim de garantir a autenticidade dos envolvidos. No SET, não apenas os usuários, que estão no início do processo, devem possuir certificados digitais, mas também todas as demais entidades, como por exemplo os comerciantes e os *Gateways* de pagamento, responsáveis pela aprovação das transações.

Se por um lado, essa tecnologia oferece soluções para todos os requisitos de segurança apresentados, por outro, a complexidade inerente ao processo de desenvolvimento de aplicações compatíveis com o SET, têm dificultado a sua aceitação como um padrão de fato.

Além da questão relativa à complexidade do desenvolvimento de aplicações baseadas no SET, outro problema que emerge quando se trata de analisar a robustez do SET como um todo, está relacionada à fragilidade dos sistemas propostos para o gerenciamento das chaves. O SET não tem como objetivo tratar este tópico, que continua sem tratamento, e que compromete a garantia de segurança do modelo. Um aspecto importante a ser lembrado, relacionado à segurança, é que define que a utilização de mecanismos complexos de segurança em determinadas partes do sistema é ineficaz se em outro ponto não houve pelo menos o mesmo nível de segurança. Em outras palavras: um sistema é tão vulnerável quanto o seu ponto mais frágil. Considerando que a maioria dos usuário-alvo das aplicações de comércio eletrônico são usuários de Computadores Pessoais, a segurança no modelo estará comprometida se a implementação levar o usuário a armazenar suas chaves criptográficas no sistema de arquivos dos mesmos, pois de uma forma geral, nesta plataforma de equipamentos não há garantias em relação à privacidade dos dados [ROC 99].

Para tratar este item, há diversas propostas atualmente em análise pela comunidade de desenvolvimento. Uma delas, e talvez a mais promissora, é a da utilização de *smartcards* (cartões inteligentes), que nada mais são que cartões com formato semelhante aos cartões de crédito comuns, mas que incorporam circuitos integrados que permitem armazenar, entre outras coisas, as chaves criptográficas necessárias para a implementação de mecanismos de segurança mais complexos.

A figura 3.6 ilustra o funcionamento do cartão *smartcard* para assinar um documento digitalmente.

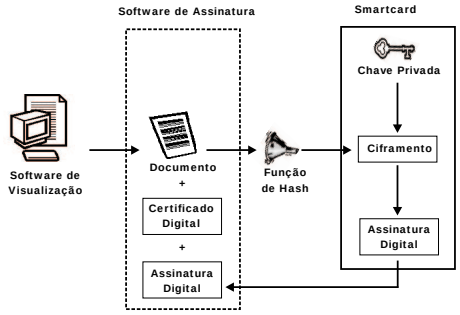

Figura 3.6: Smartcard - O software envia o resumo do documento para ser assinado, o cartão cifra o resumo que fará parte da assinatura e envia para o software [BOR 02].

3.4.8.1 Participantes do Sistema de Pagamento

A tabela 3.1 mostra os participantes do sistemas de pagamento SET.

Tabela 3.1: Participantes do Sistema de Pagamento SET

Participante	**Descrição**
Comprador	O proprietário do cartão.
Emissor	A instituição financeira ligada ao proprietário do cartão. O emissor de cartão bancário, o banco que fornece ao cardholder uma conta e um cartão bancário.O issuer garante o pagamento para transações autorizadas usando o cartão bancário de acordo com as regulamentações da associação e a regulamentação local.
Comerciante	O negociante de produtos, serviços e ou informações que aceita em troca o pagamento eletrônico.
Banco	A instituição financeira ligada ao comerciante, e que suporta comerciantes fornecendo serviços para o processamento de transações baseadas em cartões de crédito.
Gateway Pagamento	Dispositivo operado por um Acquirer ou terceiro, que processa as mensagens de pagamento dos comerciantes.
Marca	Administradora de cartões. Instituições financeiras tem fundado associações que protegem e divulgam a marca, estabelece e fortifica regras para o uso e aceitação de cartões bancários, e fornecem redes para interconexão das instituições financeiras.
Autoridade Certificadora	Um agente de uma ou mais associações de cartão bancário que provê a criação e distribuição de certificados eletrônicos para merchants, acquirers e cardholders.

3.4.8.2 Gerenciamento de Certificados Digitais no SET

A fim de verificar a autenticidade dos envolvidos nas transações, a especificação criada para o SET engloba a utilização de certificados digitais, que devem ser

utilizados por todos os envolvidos no processo, quer sejam eles instituições financeiras, comerciantes ou consumidores.

O SET incorpora uma nova forma de utilização de assinaturas digitais, conhecida como assinaturas duais. Esta assinatura aparece dentro das mensagens trafegadas, como por exemplo, para que o comerciante não tenha acesso às informações relativas a pagamento, originadas pelo consumidor.

O processo de validação de certificados digitais no SET, se dá através de um conjunto de operadores. Após ter completado a seleção dos ítens que deseja comprar, o proprietário do cartão seleciona o sistema de pagamento desejado, que deve ser compatível com o SET. Neste momento, o módulo SET do comerciante envia uma mensagem que aciona o módulo de software utilizado para estabelecer a comunicação com as demais entidades, e emitir as requisições definidas pelo conjunto de protocolos, mais conhecido como ”carteira eletrônica”. São enviados, então pelo módulo SET do comerciante, os certificados necessários (do comerciante e do *gateway* de pagamento).

Encerrada a etapa inicial de envio dos certificados, a carteira eletrônica realiza o processo de verificação da autenticidade das chaves, e caso este processo seja concluído de forma bem sucedida, a carteira eletrônica envia uma cópia do seu certificado, para utilização na cifragem das mensagens a serem retornadas para ela. Uma vez concluída a etapa de intercâmbio dos certificados, e todas as entidades estando adequadamente certificadas, o processamento poderá ser iniciado de forma apropriada. A partir deste momento, a integridade e a confidencialidade das mensagens podem ser asseguradas.

As mensagens geradas pela carteira eletrônica (utilizada pelo proprietário do cartão), que tem como destino o comerciante (mensagens contendo informações sobre a compra, por exemplo), são cifradas e assinadas utilizando a chave pública do comerciante. Isso significa que somente o comerciante pode abrir e decifrá-las. Já as mensagens geradas pela carteira eletrônica que tenha como destino o *gateway* de pagamento (mensagens contendo informações relativas à forma de pagamento, por exemplo), são cifradas e assinadas utilizando a chave pública do *gateway* de pagamento. Isto garante, que mesmo sendo enviadas para o comerciante, elas somente poderão ser decifradas e in-

terpretadas quando este as repassar para o *gateway* de pagamento, que terá então acesso às mesmas.

As mensagens geradas pelo comerciante, que tenham como destino o proprietário do cartão, são assinadas utilizando a chave pública deste, e que garante que somente ele terá acesso. De forma semelhante, as mensagens geradas pelo comerciante (autorização e captura de pagamentos, por exemplo), são cifradas e assinadas utilizando a chave pública do *gateway* de pagamento, garantindo também o sigilo e a integridade das informações trafegadas.

Todo o complexo processamento de criptografia realizado pelo SET visa garantir os requisitos de segurança já discutidos no início deste trabalho. O SET, de fato, constitui um dos mais complexos sistemas já desenvolvidos para garantir a segurança do processamento de pagamento eletrônico.

Apesar de toda a complexidade criptográfica definida pelo SET, a questão da segurança está ligada diretamente à arquitetura definida para o gerenciamento dos certificados digitais emitidos para todas as entidades envolvidas, sem a qual os requisitos em questão não podem ser plenamente atendidos.

A figura 3.7 mostra o fluxo de dados do SET.

3.4.8.3 O Caso Bradesco

A primeira iniciativa nacional de implementação do protocolo SET para pagamento em compras eletrônicas foi a do Bradesco através da inauguração do shopping virtual Bradesco Net.

O Bradesco Net foi inaugurado no dia 24 de março de 1998 no endereço eletrônico http://www.bradesco.com.br/comercio. A principal característica desse shopping é a utilização da carteira eletrônica, um conceito novo introduzido na especificação do protocolo SET. O sistema cobre os pontos mais críticos do comércio eletrônico: sigilo, autenticação, através dos certificados digitais, integridade, autenticidade das informações e não repúdio.

O shopping foi construído no período de um ano, teve um custo de 700

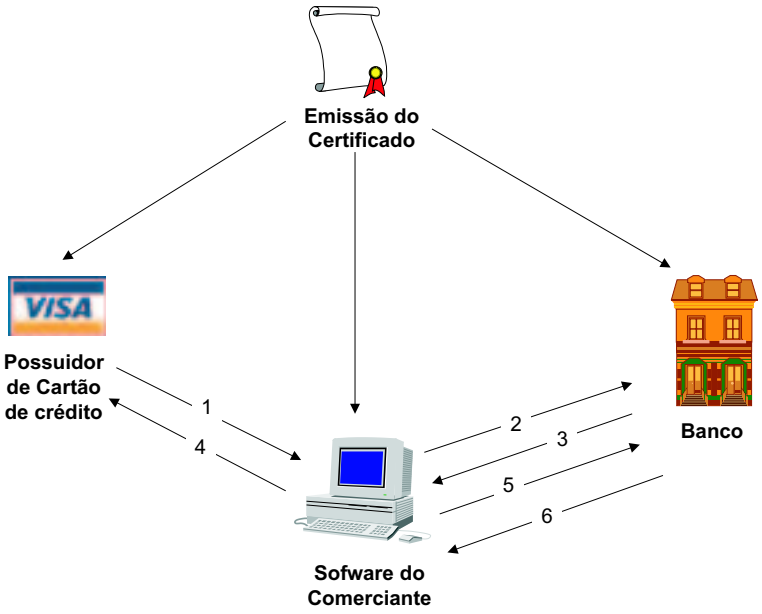

Figura 3.7: Fluxo de dados do SET. Análise do funcionamento do fluxo de dados da recomendação SET: (Passo 1) O dono do cartão de crédito inicia a compra. (Passo 2)O comerciante verifica o cartão de crédito. (Passo 3) A compra é autorizada. (Passo 4) A ordem de pagamento é confirmada. (Passo 5) O comerciante requisita o pagamento. (Passo 6) O pagamento é efetuado.

mil dólares e nasceu com 13 lojas conveniadas.

O sítio do Bradesco é um hospedeiro de lojas que queiram realizar vendas pela Web. O Bradesco não oferece produtos, ele fornece a infra-estrutura de um sistema de pagamentos pela Internet. As lojas interessadas assinam um convênio com o Bradesco Net e assim podem receber pagamentos eletrônicos efetuados com os cartões de crédito, débito e/ou de poupança do banco.

3.4.9 Autoridade de Aviso

Num sistema de atendimento ao cliente disponível através da Internet, poderá ocorrer problemas de comunicação e indisponibilidade de serviços, e pode ocorrer que eventualmente um participante esteja interessado na interrupção dessa comunicação. Para isso elege-se uma autoridade de aviso.

A autoridade de aviso (AA), primeiramente descrita em [BRO 01], é

uma entidade participante de um protocolo que tem como objetivo principal garantir a comunicação e o não repúdio de mensagens pelos participantes de uma transação. Seu papel consiste em notificar um destinatário, a pedido de uma outra entidade, através de diversos meios de comunicação. Os meios de comunicação empregados pela autoridade de aviso, podem variar desde métodos eletrônicos como *e-mail*, *fax*, telefone ou mensagens para aparelhos celulares, até os mais tradicionais como correspondência simples ou registrada e anúncios em jornais.

A participação da autoridade de aviso em um protocolo, sendo ela considerada uma entidade confiável para o mesmo, faz com que os outros integrantes tenham garantias de comunicação com seus destinatários ou, na pior das hipóteses, a prova de que tentaram fazê-la.

A figura 3.8 mostra o funcionamento da Autoridade de Aviso.

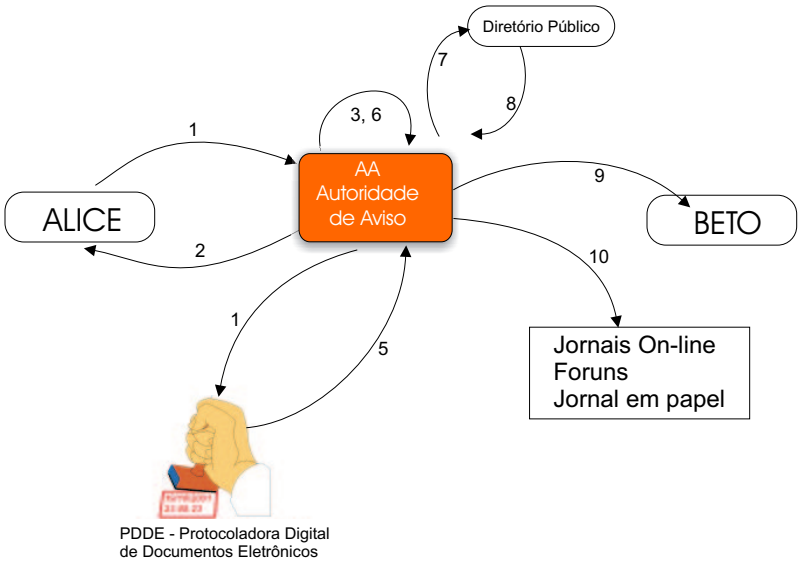

Figura 3.8: Procedimentos de funcionamento da Autoridade de Aviso. A Autoridade de Aviso funciona da seguinte maneira: (1) O remetente envia o documento a ser entregue para a Autoridade de Aviso; (2) A Autoridade de Aviso confere e emite um recibo de entrega para o remetente; (3) A Autoridade de Aviso gera um aviso para ser entregue; (4) A Autoridade de Aviso solicita um protocolo com data/hora da PDDE; (5) A AA monta o aviso; (6) A AA envia para o Diretório Público o aviso; (7) O Diretório Público devolve um recibo sobre a inclusão; (8) A AA de aviso envia o aviso, para o destinatário, primeiramente via e-mail. (9) A AA espera um determinado período e, se o destinatário não respondê-la, ela procede a publicação do aviso em outros locais, como por exemplo, jornais on-line, fóruns e, se for o caso, em jornais de papel.

3.4.10 Protocoladora Digital de Documentos Eletrônicos

A função da protocoladora digital de documentos eletrônicos - PDDE é de protocolizar as mensagens que recebe dos participantes, adicionando a elas um carimbo de tempo (data e hora) com a finalidade de dar uma referência temporal para as transações do protocolo.

Segundo [PAS 01], uma autoridade de datação pode ser utilizada também, por exemplo, para verificar se uma assinatura digital foi aplicada em uma mensagem antes que o seu certificado digital correspondente tenha sido revogado. Esta é uma condição fundamental para o bom funcionamento de toda a infra-estrutura de chaves públicas.

Requisitos que uma autoridade de datação deve satisfazer para ser considerada por seus usuários como segura e confiável [ADA 01, PAS 01]:

- Utilizar uma fonte de tempo precisa e confiável;
- Incluir uma marcação de tempo correta e honesta em todas as mensagens protocoladas;
- Incluir uma identificação única para cada mensagem protocolada;
- Aplicar a marcação de tempo somente num resumo (*hash*) da mensagem;
- Não incluir nenhuma identificação da entidade requisitante na mensagem datada;
- Assinar digitalmente cada mensagem protocolada com uma chave gerada especificamente para esse objetivo.

Existem 3 empresas que podemos destacar quanto a solução de PDDE, que são: a empresa Bry do Brasil, a empresa Surety dos EUA e a empresa Timeproof da Alemanha.

3.5 Conclusão

O aspecto principal que precisa ser controlado num sistema de comércio eletrônico é a segurança. Para que isso ocorra, as aplicações de comércio eletrônico deverão atender aos requisitos de segurança exigidos que são: confidencialidade, integridade, autenticidade e não-repúdio.

No momento da criação da política de segurança deve-se levar em consideração estas questões, e utilizar os mecanismos de segurança que atendem a esses requisitos. Para o comércio eletrônico, os mecanismos de segurança utilizados são a criptografia de dados, a assinatura digital, a utilização de certificado digital para documentos eletrônicos os protocolos criptográficos para transmissão de dados pela Internet e implementação de soluções específicas.

Capítulo 4

Segurança no Comércio Eletrônico

4.1 Introdução

O baixo custo e a larga disponibilidade da Internet para as empresas e clientes causaram uma revolução no comércio eletrônico e suas aplicações. Em resumo, uma aplicação de comércio eletrônico pode ser a etapa de uma ou várias fases de uma transação típica empresarial, e existem várias possibilidades para modelar estas fases. Por exemplo, uma possibilidade deve distinguir quatro fases de uma transação de negócio. Na fase 1, o comerciante faz uma oferta para bens específicos ou serviços. De acordo com esta oferta, o cliente pode fazer um pedido na fase 2. Na fase 3 o cliente faz um pagamento. Na fase 4 o comerciante entrega os bens ou serviços ao cliente. A manipulação do pagamento pode envolver terceiros, como bancos [OPP 99].

Este é apenas um modelo que pode ser usado, onde foram identificadas fases de uma transação de negócio, mas outros modelos podem ser usados e poderão ser parcialmente ou inteiramente diferentes.

Muitas empresas já estão explorando as oportunidades oferecidas pelo comércio eletrônico pela Internet, e é esperado que muitas outras empresas também explorem. Exemplos de aplicações incluem compras *on-line*, Internet Banking, educação a distância, jogos *on-line*, e outros. Mas apesar dos casos de sucessos existentes, como por exemplo a Amazon, muitas empresas e clientes ainda são cautelosos sobre participar do

comércio eletrônico, e as preocupações com segurança são citadas freqüentemente como sendo a barreira mais importante.

Considerando que o comércio eletrônico é uma forma de fazer negócios, é preciso considerar todas as mudanças necessárias no desenvolvimento dos sistemas de comércio eletrônico, englobando os processos que o compõem e o papel dos participantes do sistema.

A figura 4.1 mostra as etapas e processos que ocorrem num sistema de comércio eletrônico.

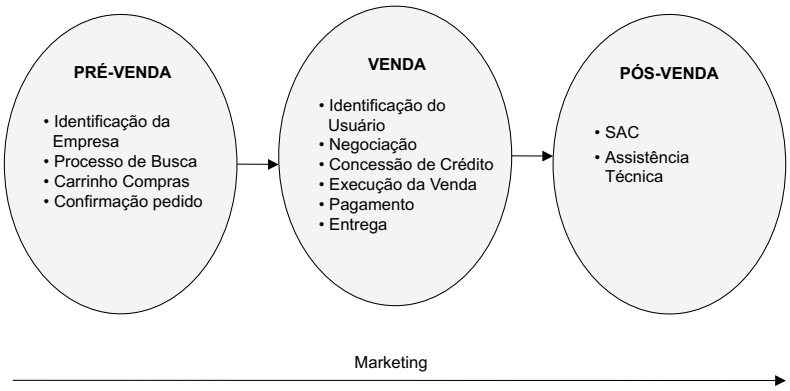

Figura 4.1: Sistema de comércio eletrônico - Na fase de pré-venda ocorrem os processos de Identificação da Empresa, Busca dos Produtos, Carrinho de Compras e Confirmação do Pedido. Na fase de venda ocorrem os processos de Identificação do Usuário, Negociação, Concessão de Crédito, Execução da Venda, Pagamento e Entrega. Na fase de pós-venda ocorre os processos de SAC - Serviço de Atendimento ao Consumidor e Assistência Técnica. Paralelamente aos eventos de pré-venda, venda e pós-venda ocorre o processo de Marketing.

O objetivo deste capítulo é apresentar uma nova abordagem sobre as aplicações de comércio eletrônico e suas etapas de comercialização, e fazer uma avaliação geral de seus aspectos segurança. Está estruturado da seguinte forma: a seção 4.2 identifica os processos de negócio numa aplicação de comércio eletrônico, a seção 4.3 apresenta os aspectos de segurança relacionados ao comércio eletrônico e a seção 4.4 refere-se a legislação para o comércio eletrônico.

4.2 Processos de negócio

O comércio eletrônico é uma área bastante nova se comparada aos outros tipos de comércio. No mundo real, para o comércio existir, há a necessidade de elementos de vários tipos: organizações, comerciantes e consumidores. Estes estão sempre visando alguns objetivos em seus negócios, cujos principais são: diminuir custos, melhorar a qualidade dos produtos e serviços e aumentar a velocidade de distribuição dos produtos/serviços [RIZ 01].

O processo de comercialização, sob a perspectiva do negócio, é apresentado em três situações típicas: pré-venda, venda e pós-venda, conforme apresentado na figura 4.2.

Figura 4.2: Processo de comercialização - O processo de comercialização, sob a perspectiva do negócio, é apresentado em três situações típicas: pré-venda, venda e pós-venda.

4.2.1 Pré-Venda

Durante a pré-venda, são fornecidas ao cliente todas as informações necessárias sobre os produtos e serviços disponíveis. Nesta situação, o cliente tem algumas necessidades por um produto ou serviço e o comerciante deve fornecer todas as informações sobre o que ele pode oferecer. Hoje isto é realizado na *Web* através de catálogos eletrônicos e consultas a bases de dados de produtos. Eles proporcionam a navegação dentro do catálogo através de índices ou pesquisas de existência. O índice apresenta uma hierarquia de características descritivas dos produtos no catálogo e dá suporte ao usuário durante a pesquisa.

A única parte ativa neste processo é o cliente, em contraste com o mundo real dos negócios, onde todos os tipos de técnicas de marketing são utilizadas. Na *web*

o cliente necessita buscar todas as informações por si mesmo.

O segundo tipo de abordagem é a navegação baseada nas necessidades onde o usuário entra com suas necessidades em relação a um produto e a base de dados é pesquisada para obtenção do produto mais adequado a estas necessidades.

A pré-venda é freqüentemente uma comunicação em um passo ou até em sentido único, até que o cliente fique interessado em comprar um produto. De qualquer forma, a fronteira entre a pré-venda e a venda é bastante tênue. O cliente primeiro decide se um produto é o que ele precisa e depois de uma decisão positiva ele envia o pedido, que é um processo que pertence a situação de vendas.

A fase da pré-venda é caracterizada por:

Identificação da empresa: comprovação de que a empresa realmente existe e é de confiança;

Processo de busca dos produtos: busca do cliente pelo produto ou serviço desejado;

Carrinho de compras: o cliente seleciona os produtos ou serviços;

Confirmação do pedido: solicitação de compra por parte do cliente. Este pedido poderá ser aceito ou não.

4.2.2 Venda

Durante a venda, um cliente e a empresa negociam os produtos e serviços e também os custos destes para o cliente. A principal tarefa é identificar as reais necessidades do cliente e encontrar um serviço ou produto apropriado para o mesmo. Comparada à pré-venda, a qual freqüentemente acontece a comunicação em uma via (cliente - vendedor), a fase de venda constitui-se de um processo complexo com muitas interações entre o cliente e a empresa.

Esta é a fase em que será literalmente realizada a venda, permitindo que a escolha feita pelo cliente na fase de pré-venda se caracterize na venda real do produto/serviço. Comparada à pré-venda, a qual freqüentemente acontece a comunicação

em uma via (cliente-fornecedor), a fase de venda constitui-se de um processo complexo com muitas interações entre a empresa e o cliente. O processo de venda é concluído após o cliente confirmar a compra, realizar o pagamento e a empresa entregar o produto/serviço adquirido pelo cliente.

Portanto, a fase da venda é caracterizada por:

Identificação do usuário: Cliente se identifica para a empresa;

Negociação: Acordo que deverá existir entre as partes quanto ao valor, condição de pagamento, forma e valor de entrega;

Concessão de crédito: Após o cliente decidir pela compra, a loja verifica sua situação quanto a disponibilidade de crédito para autorizar a sua compra;

Execução da venda: Esta etapa inclui emissão da nota fiscal, redução do produto do estoque e expedição da mercadoria;

Pagamento: Cliente deverá cumprir com o acordo feito na negociação e efetuar o pagamento combinado com a empresa;

Entrega: Ocorre após o cliente receber a mercadoria ou serviço, deverá haver controle de comprovação da entrega.

4.2.3 Pós-Venda

A etapa de pós-venda acontece na situação onde os clientes já adquiriram seus produtos ou serviços de uma companhia e eles necessitam de suporte adicional durante a utilização dos produtos comprados, ou por motivos de troca, devolução, reclamação e outros.

A fase da pós-venda é caracterizada por:

Serviço de SAC - Serviço de Atendimento ao Cliente: Departamento responsável pelo atendimento ao cliente. Posiciona-se como interface entre o cliente e a empresa, e é responsável pelos processos de:

- Esclarecimento de dúvidas;
- Atendimento das reclamações, fazendo os encaminhamentos necessários;
- Trocas e devoluções de mercadorias.

Assistência Técnica: Atendimento a dúvidas de utilização, manutenção e concerto.

4.3 Aspectos de Segurança Relacionados ao Comércio Eletrônico

No que diz respeito à segurança do comércio eletrônico e suas aplicações, é útil distinguir entre assuntos de segurança do lado do cliente, e assuntos de segurança do lado do servidor, e assuntos de segurança das transações. Além disso, há alguns assuntos de segurança organizacional e legal que deveriam ser considerados com cuidado [OPP 99].

4.3.1 Segurança no lado do cliente

Do ponto de vista do usuário, a segurança é normalmente a preocupação principal. Em geral, segurança do lado do cliente requer o uso de tecnologias de segurança tradicionais, como autenticação e autorização do usuário formal, controle de acesso, e proteção através de anti-vírus. Com respeito a serviços de comunicação, o cliente pode adicionalmente requerer autenticação do servidor e não repúdio do recebimento. Além disso, algumas aplicações podem requerer anonimato (por exemplo, navegar anonimamente pela rede).

4.3.2 Segurança no lado do servidor

A segurança do lado do servidor é a preocupação principal do ponto de vista dos provedores de serviço. Segurança do lado do servidor requer autenticação e autorização formal do cliente, não repúdio da origem, anonimato de remetente (por

exemplo, publicação anônima na Web), auditoria para rastreamento e responsabilização, como também confiabilidade e disponibilidade [OPP 99].

4.3.3 Transações seguras

A segurança da transação é igualmente importante tanto para o cliente e quanto para o servidor. A segurança de transação requer vários serviços de segurança, como autenticação de dados, controle de acesso, confidencialidade dos dados, integridade dos dados, e não repúdio dos serviços. Além disso, certas aplicações também podem requerer garantias de anonimato da transação [OPP 99].

4.3.4 Segurança organizacional e legal

Além dos mecanismos técnicos de segurança para dirigir-se ao lado cliente e ao lado servidor como também segurança nas transações, também há alguns assuntos de segurança organizacionais e legais que devem ser considerados com cuidado.

Um problema freqüente nas organizações são as pessoas, por isso não pode-se negligenciar esta situação, senão a organização estará com sérios problemas.

Uma analogia para ilustrar a insuficiência de técnicas de mecanismos de segurança é o serviço de entrega postal. Note que a técnica de segurança deste serviço é fornecida pelos meios de assinatura escrita a mão (para fornecer autenticidade dos dados) e envelopes de carta (para fornecer a confidência de dados). Ambos os mecanismos são relativamente simples e fáceis de falsificar. Então, foram desenvolvidos mecanismos de segurança adicionais e foram aplicados no lado organizacional e legal. Por exemplo, cartas são distribuídas por carteiros, e abrir ilegitimamente ou esconder uma carta é um ato criminal [OPP 99].

4.4 Legislação para o comércio eletrônico

Uma questão que não pode ser esquecida é a questão legal referente ao comércio eletrônico.

No Brasil ainda não existe uma lei que regulamente especificamente o comércio eletrônico, mas há trabalhos legislativos no Congresso Nacional que vêm sendo desenvolvidos nesta área. Atualmente, há três projetos de lei em tramitação, sendo um no Senado e dois na Câmara dos Deputados. No senado está em tramitaçãos o Projeto de Lei número 672 de 1999, e na câmara os Projetos de Lei número 1.489 de 1999 e número 1.589 de 1999.

Por não existir uma lei específica para o comércio eletrônico, o código de defesa do consumidor que foi criado com o objetivo tornar as relações comerciais transparentes entre as empresas e seus clientes, é o princípio básico para assegurar os direitos do cliente.

4.4.1 Projeto de Lei 672, de 1999, do Senado Federal

Este projeto de autoria do senador Lúcio Alcântara, é o que está mais adianto quanto ao comércio eletrônico. Foi baseado no modelo da UNCITRAL (Comissão das Nações Unidas para leis de comércio internacional), e busca a uniformização internacional da legislação sobre o tema.

4.4.2 Projeto de Lei 1.489, de 1999, do Câmara dos Deputados

Institui a fatura eletrônica digital, nas transações de comércio eletrônico. Este projeto possui apenas dois artigos e a certificação por órgão público.

Art. 1 - Fica instituída a fatura eletrônica assim como a assinatura digital, nas transações comerciais eletrônicas realizadas em todo o território nacional.

Art. 2 - A assinatura digital terá sua autenticação e reconhecimento certificado por órgão público que será regulamentado para este fim.

Parágrafo único. Toda documentação eletrônica, bem como o cadastro de assinaturas digitais, deverão estar com seus registros disponíveis para avaliação e fiscalização dos órgãos federais responsáveis.

4.4.3 Projeto de Lei 1.589, de 1999, do Câmara dos Deputados

Dispõe sobre o comércio eletrônico, a validade jurídica do documento eletrônico e a assinatura digital, e dá a outras providências. Este projeto foi elaborado a partir de um anteprojeto da Comissão de Informática Jurídica da OAB/SP. Prevê a adoção do sistema de criptografia assimétrico como base para a assinatura digital e ainda, estabelece que os cartórios poderão ser autoridades certificadoras. Este Projeto de Lei num. $1589/99$ foi apensado ao Projeto de Lei num. $1.483/99$ e encontram-se sob a apreciação de uma comissão parlamentar especial na Câmara dos Deputados. No mês de junho de 2001, o Relator do Projeto de Lei num. $1483/99$ (e do Projeto de Lei num. $1.589/99$ - apensado) apresentou Substitutivo aos referidos projetos, consolidando propostas e agregando aperfeiçoamentos. O trabalho apresentado pelo relator é resultado de discussões internas e audiências públicas da Comissão Especial. Destaque-se que ele prevê a assinatura digital baseada no sistema de criptografia assimétrico, e fixa que somente a assinatura digital certificada por entidade credenciada pelo Poder Público presume-se autêntica perante terceiros. Em setembro de 2001, a Comissão Especial da Câmara dos Deputados aprovou o Substitutivo do Relator [BOR 02],[STA 01].

4.5 Conclusão

Através da análise realizada pelo levantamento dos processos de negócio e do estudo dos sistemas de comércio eletrônico foi possível identificar os processos que fazem parte deste sistema. O processo de comercialização apresenta-se em três situações típicas: a pré-venda, a venda e a pós-venda. Em todas essas etapas deve-se garantir a integridade do processo e a segurança dos seus participantes. Ou seja, para o comércio eletrônico ser aceito largamente é necessário atender a todos os requisitos de segurança e assegurar o interesse de todas as partes envolvidas no processo.

Os estudos atuais envolvendo segurança no comércio eletrônico e suas aplicações foram apresentados aqui e enfocam soluções para atender a segurança do lado do cliente, do lado do servidor, nas transações e aspectos legais.

Capítulo 5

Projetos de Pesquisa

5.1 Introdução

O objetivo deste capítulo é dar uma visão geral dos projetos de pesquisa que tem sido feitos sobre segurança no comércio eletrônico, desenvolvido a partir do levantamento dos projetos de pesquisa de segurança no comércio eletrônico que está sendo realizado no Brasil.

Para atender a esses objetivo este capítulo está estruturado da seguinte forma: a seção 5.2 trata dos projetos de pesquisa desenvolvidos pelo LabSEC - Laboratório de Segurança em Computação. A seção 5.3 refere-se aos congressos da área de segurança realizados no Brasil. A seção 5.4 refere-se as soluções desenvolvidas por empresas na área de segurança no comércio eletrônico. A seção 5.5 apresenta um levantamento de pesquisa realizadas através do levantamento de artigos científicos publicados em revistas na área, e a seção 5.6 apresenta a visão geral do capítulo.

5.2 LabSEC

O LabSEC foi fundado em abril 2000 e faz parte do INE - Departamento de Informática e de Estatística da UFSC - Universidade Federal de Santa Catarina. O laboratório tem por objetivo estudar, pesquisar, avaliar e implementar soluções na área de

segurança em computação.

Atualmente, existe um grande projeto que está sendo desenvolvido, o projeto de Segurança no Comércio Eletrônico que está sub-dividido nos projetos Cartório Virtual, Análise Segura de Crédito, Sistema Seguro de Atendimento ao Cliente (SAC Seguro), Auditoria de publicidade na web e Compras Seguras.

O projeto de Cartório Virtual está subdividido nos projetos de Infraestrutura Digital de Documentos Eletrônicos (IDDE), Infraestrutura de Chave Pública (ICP), Autoridade Certificadora e a Autoridade de Registro.

Esta dissertação de mestrado faz parte do projeto de Segurança no Comércio Eletrônico do LabSEC e que apresenta como um estudo geral englobando todos os demais projetos relacionados, conforme está demonstrado na figura 5.1.

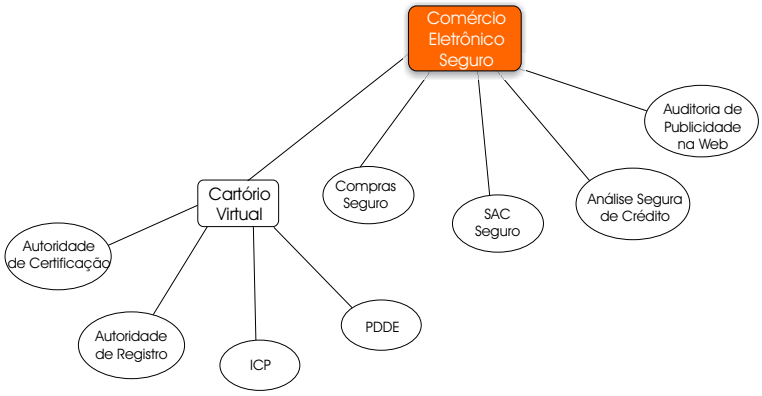

Figura 5.1: Existe um grande projeto que está sendo desenvolvido, o projeto de Segurança no Comércio Eletrônico que está sub-dividido nos projetos Cartório Virtual, Análise Segura de Crédito, Sistema Seguro de Atendimento ao Cliente (SAC Seguro), Auditoria de publicidade na web e Compras Seguro.

5.2.1 Análise Segura de Crédito

O tema central deste projeto está situado nas relações existentes em transações comerciais entre Estabelecimentos, Clientes e Sistemas de Crédito. Este último justificando sua existência devido a inadimplência dos Clientes. Os Sistemas de Crédito prestam serviços de análise ao crédito sobre os Clientes. Mas os Sistemas de Crédito

existentes possuem *falhas* de segurança e um déficit em abrangência, ao mesmo tempo que são vulneráveis a ataques e roubo de informações. Portanto, a comunicação entre os Estabelecimentos, Clientes e Sistema de Crédito deve oferecer segurança, bem como rapidez, privacidade e veracidade das informações [BRO 01].

O trabalho propõe um protocolo criptográfico para dar segurança às transações eletrônicas utilizadas para o fornecimento de crédito, e que atende aos seguintes requisitos de segurança:

1. **Confidencialidade ou sigilo:** Garantia de que somente as pessoas ou organizações envolvidas na comunicação possam ler e utilizar as informações transmitidas de forma eletrônica pela rede.

   (a) **Confidencialidade da Ficha Cadastral do Cliente** - Propriedade de que certas informações não possam ser disponibilizadas ou divulgadas sem autorização do Cliente.

   (b) **Confidencialidade das Informação de Crédito** - É a garantia de que os dados sobre os créditos concedidos sejam acessíveis somente para o Cliente e para o Sistema de Crédito. Não poderá ser possível relacionar uma determinada concessão de crédito a um Estabelecimento.

   (c) **Garantir a confidencialidade na comunicação** - A condição na qual os dados transmitidos são protegidos contra modificações não autorizadas.

   (d) **Confidencialidade em uma consulta** - Garantia de que uma consulta seja visível somente para o Estabelecimento.

2. **Integridade:** Garantia de que o conteúdo de uma mensagem ou resultado de uma consulta não será alterado durante seu tráfego ou no período em que ficou armazenada.

3. **Autenticação:** Garantia da identificação das pessoas ou organizações envolvidas na comunicação.

4. **Não-repúdio:** É a garantia de que uma informação produzida em um determinado tempo *t* não possa ser negada em $t + t_1$, $t_1 > 0$.

5. **Unicidade:** Os fraudadores costumam ter identidades falsas. Para isso, o sistema deve garantir que exista somente um único certificado válido por usuário. E quando da expedição de um novo certificado, deve haver uma verificação da existência de certificado revogado ou suspenso.

6. **Garantia de aspectos constantes na legislação:** Um ponto importante na legislação refere-se à garantia de sigilo de informações confidenciais dos Clientes e Estabelecimentos. Somente podem ter acesso às informações, as pessoas autorizadas pelos respectivos donos e os usuários do sistema. Equivale a dizer que a ficha cadastral do Cliente só pode ser visualizada após a autorização do respectivo Cliente; da mesma forma o acesso às informações do Estabelecimento e do Sistema de Crédito.

O protocolo deve garantir qual foi o usuário responsável pelos dados cadastrados, bem como os usuários que realizaram as consultas. Garantindo assim, por exemplo, a identificação de quem procedeu uma inclusão de determinado cliente no cadastro de inadimplementes. A figura 5.2 mostra o protocolo criptográfico I2AC.

5.2.2 Sistema Seguro de Atendimento ao Cliente - SAC Seguro

Este projeto estuda os modelos atuais de atendimento à clientes, abordando as dificuldades de garantia de qualidade nos serviços e na preservação dos direitos do consumidor previstos em lei, e com a intenção de resolver este problema e garantir um nível aceitável de atendimento aos clientes, propõe um protocolo criptográfico com base em tecnologias de segurança e criptografia [GHI 01].

A adoção do protocolo proposto é identificada no sítio da empresa por um selo, que também determina o comprometimento da mesma com a qualidade no atendimento ao cliente.

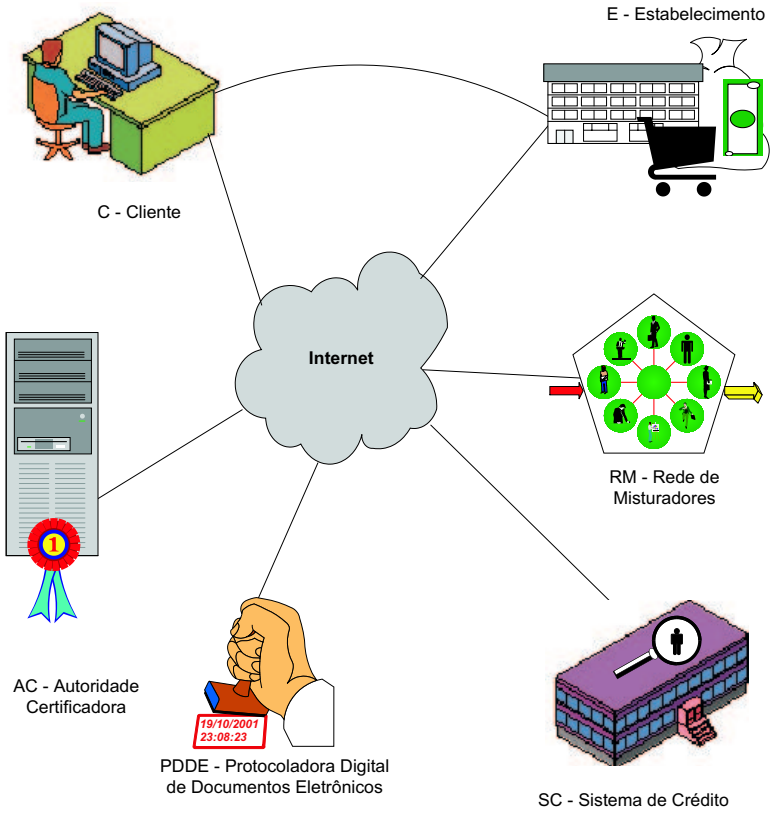

Figura 5.2: Protocolo criptográfico I2AC. A comunicação entre os participantes é através da internet, porém, a comunicação entre Cliente e Estabelecimento pode ocorrer presencialmente [BRO 01].

O protocolo proposto, elege uma autoridade fiscalizadora que pode acompanhar e intervir no processo de atendimento ao cliente, caso seus direitos sejam ameaçados. Tal autoridade fiscalizadora pode ser o próprio setor de garantia da qualidade da empresa, ou um órgão do governo que deseje monitorar as atividades de uma concessão de serviço público.

O atendimento ao cliente é dividido em 3 etapas: requisição, atendimento e fechamento da requisição.

A requisição de atendimento é o ponto de partida do início do processo em questão, e cliente pode solicitar pelo motivo de reclamação ou para contratação de serviço. Possui os seguintes requisitos de segurança:

- Comprovar a origem e autoria da requisição;
- Comprovação que a requisição foi aceita.

O atendimento é a fase em que a requisição do cliente passa a ser tratada pela empresa com a abertura de uma ordem de serviço. Após concluído o atendimento da requisição, a empresa emite um comunicado de conclusão da ordem de serviço para o cliente.

A fase de atendimento possui os seguintes requisitos de segurança:

- Comprovar o atendimento ao cliente;
- Comprovar a realização e o prazo que ocorreu cada evento do processo de atendimento.

O fechamento da requisição ocorre quando é realizado o fechamento de uma transação entre o cliente e a empresa, e possui os seguintes requisitos de segurança:

- Comprovar a realização da notificação ao cliente quanto ao fechamento da requisição.

Observando a figura 5.3 que mostra o funcionamento deste protocolo , temos:

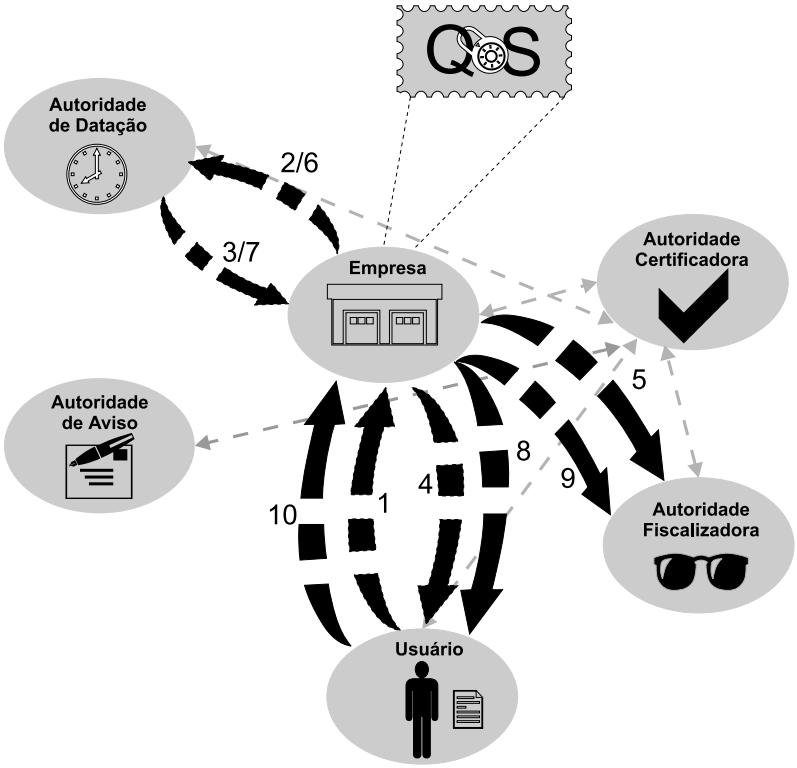

Figura 5.3: Protocolo Proposto. 1. **CL** faz a requisição; 2. **EM** envia em recibo da requisição para **AD**; 3. **AD** protocola o recibo e devolve-o para **EM**; 4. **EM** envia o recibo de requisição para **CL**; 5. **EM** envia uma cópia do recibo de requisição para **AF**; 6. Após concluir a **OS** gerada com a requisição do **CL**, **EM** gera um documento para o fechamento da **OS** e envia para **AD**; 7. **AD** protocola o documento para o fechamento da **OS** e envia para **EM**; 8. **EM** envia uma solicitação de fechamento da **OS** para **CL**; 9. **EM** envia uma cópia da solicitação de fechamento da **OS** para **AF**; 10. **CL** analisa a solicitação e responde fechando o ciclo da transação [GHI 01].

1. O cliente é o ponto de partida do protocolo, quando através de uma visita ao sítio da empresa contrata um serviço ou solicita um atendimento, através de uma requisição assinada digitalmente por ele de forma a garantir a sua identidade. A requisição tem o seguinte formato:

   REQ = E_{KR_CL}[requisição]

2. A empresa recebe a requisição, gera um resumo da mensagem com um algoritmo de *hash*, assina digitalmente e o encaminha para a autoridade de datação:

   RESUMO_REQ = E_{KR_E}[*Hash*(REQ)]

3. A autoridade de datação recebe o resumo da mensagem enviada pela empresa, protocola acrescentando data e hora locais e devolve para a empresa tudo assinado digitalmente. Com isso, é gerado o protocolo que comprova a requisição feita pelo cliente:

   PROTOCOLO_REQ = $E_{KR_{AD}}$[RESUMO_REQ || DATA || HORA]

4. A empresa recebe o protocolo solicitado à AD e gera o recibo da requisição para o cliente, dando-lhe com isso, a garantia para o atendimento. Esse recibo é composto pela requisição do cliente concatenada com o protocolo emitido pela AD e tem o seguinte formato:

   RR = [REQ || PROTOCOLO_REQ]

   Paralelamente, uma ordem de serviço (OS) é aberta na empresa para atender a requisição do cliente;

5. Uma cópia do recibo, também é remetida para a autoridade fiscalizadora, que o armazena em seu banco de dados para eventuais auditorias ou até mesmo litígio entre os participantes. Neste passo, a fase de requisição se encerra.

6. A empresa, após atender e concluir a ordem de serviço referente a requisição do cliente, efetua o fechamento da mesma, gera um resumo (*hash*) e o envia para a autoridade de datação:

   RESUMO_FEC = E_{KR_E}[*Hash*(OS)]

7. A AD protocola o resumo de fechamento da OS e devolve para a empresa. O fato de se protocolar esse fechamento, dá a empresa a comprovação do atendimento ao cliente naquele determinado prazo. O formato dessa mensagem é o seguinte:

   PROTOCOLO_FEC = $E_{KR_{AD}}$[RESUMO_FEC || DATA || HORA]

8. A empresa recebe o protocolo de fechamento da OS e gera o comprovante de fechamento (FEC), despachando-o juntamente com uma mensagem para o cliente. Essa mensagem, solicita ao cliente o encerramento da transação iniciada por ele junto à empresa. Essa mensagem tem o seguinte formato:

FEC = [OS || PROTOCOLO_FEC]

9. Uma cópia do FEC é enviada também para a autoridade fiscalizadora, o que permite a confrontação com o recibo de requisição (RR) para se verificar o prazo no atendimento. A AF, poderá fazer isso a qualquer momento, seja a título de auditoria ou reclamação;

10. O cliente, após verificar o atendimento recebido, encerra a transação com a sua assinatura na mensagem de fechamento recebida da empresa. Com essa operação, tem-se o recibo de fechamento que é a garantia da empresa junto ao protocolo:

    RF = $E_{KR_{CL}}$[FEC]

    Dessa forma, conclui-se idealmente uma transação prevista no protocolo.

5.2.3 Auditoria de Publicidade na Web

Este projeto aborda os principais problemas relacionados à publicidade na *Internet* destacando-se a questão da medição da efetividade e a garantia da publicação de anúncios em um sítio de acordo com um contrato pré-determinado entre as partes.

Propõe uma proposta de um protocolo que garanta que estes problemas sejam resolvidos, tendo em vista especialmente as questões ligadas à segurança. Para isso, utiliza-se de técnicas de criptografia, assinatura digital, protocolo digital de tempo entre outras ferramentas que visam a segurança em transações na *Internet* [GHI 02].

Num contrato de publicidade ocorrido com uma **empresa** que deseja expor produtos/serviços através da Web existem algumas características desejáveis do ponto de vista de segurança.

As principais destas características são:

1. A **empresa** precisa saber se os anúncios publicados atingem os objetivos de divulgação revertendo-se em vendas e/ou contratações de seus produtos/serviços;

2. O **sítio anunciante** também precisa saber o grau de efetividade dos anúncios publicados de modo a poder medir o quanto pode cobrar pelo seu espaço de anúncio em contratos futuros de publicidade;

3. Do ponto de vista do **cliente** (que é o alvo de um sistema de publicidade), o objetivo é encontrar os produtos/serviços que lhe ofereçam as melhores vantagens;

4. Outra característica importante do ponto de vista da **empresa**, e também da **agência de publicidade**, é a garantia de que o contrato com o **sítio anunciante** está sendo cumprido, ou seja, se o anúncio está sendo publicado com a freqüência e durante o tempo que foi contratado;

A figura 5.4 mostra os principais passos envolvidos no sistema aqui proposto.

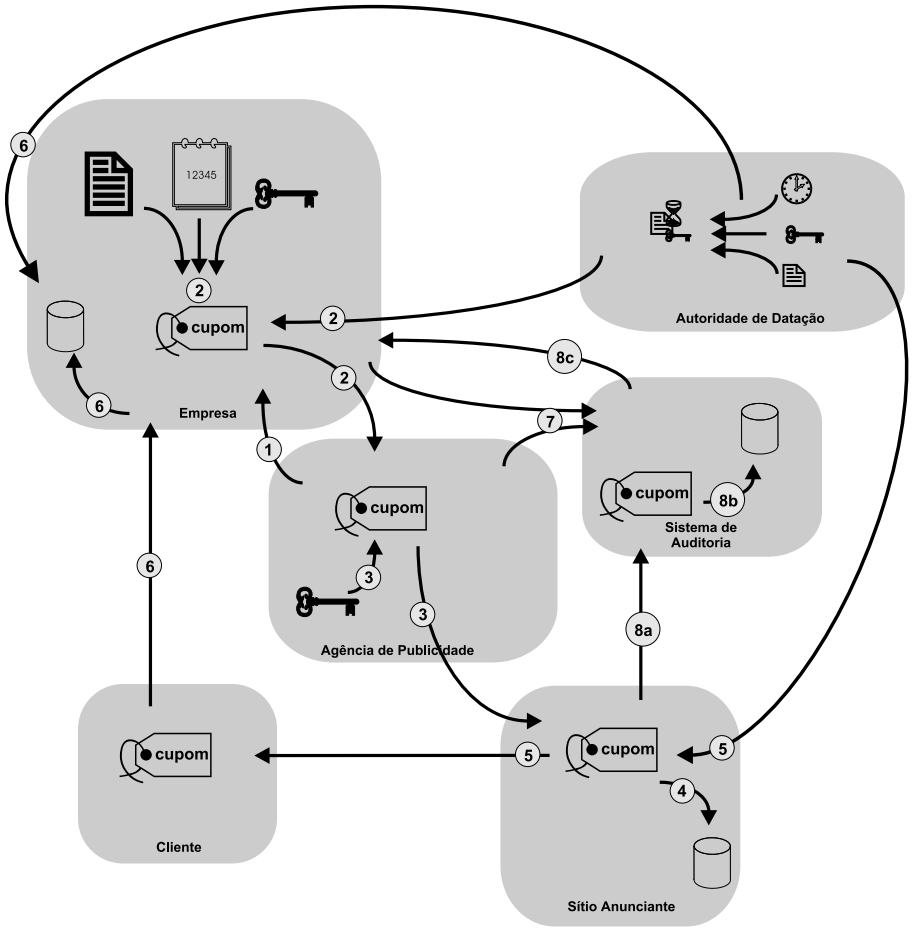

Figura 5.4: O protocolo proposto neste trabalho é composto de quatro participantes (empresa, agência de publicidade, sítio anunciante e cliente) e envolve ainda um **Sistema de Auditoria**; além disso, utiliza Autoridade Certificadora e Autoridade de Datação [GHI 02].

O processo é iniciado após ser firmado um contrato de publicação de anúncios baseado no uso de cupons eletrônicos entre a **empresa** e a **agência de publicidade** e funciona da seguinte forma:

1. A **agência de publicidade** escolhe um **sítio anunciante** (com o qual também firma um contrato) para publicar o anúncio e, a seguir, solicita à **empresa** que crie um cupom eletrônico para este **sítio anunciante**.

2. A **empresa**, atendendo a solicitação da **agência de publicidade**, cria o cupom eletrônico contendo um texto descritivo da promoção que está sendo realizada e mais um código identificador do **sítio anunciante**. Este cupom eletrônico é assinado digitalmente com a chave privada da **empresa**, recebe o "carimbo de tempo" de uma autoridade de datação e é enviado à **agência de publicidade** que o solicitou.

3. A **agência de publicidade** recebe o cupom, assina-o também com sua chave privada e repassa-o ao **sítio anunciante**. Esta assinatura poderá, mais tarde, comprovar que o **sítio anunciante** foi recomendado por ela, e não por outra agência concorrente que pode ter sido, eventualmente, contratada para auxiliar na publicação do mesmo anúncio e mesmo cupom.

4. O **sítio anunciante**, ao receber o cupom eletrônico, armazena-o em sua base de dados para que seja distribuído aos **clientes** que visitarem sua página.

5. O **cliente**, ao visitar o **sítio anunciante**, vê o anúncio publicado e, caso aceite, recebe o cupom eletrônico que lhe dará direito a algum benefício posteriormente; no momento da entrega ao **cliente**, o cupom recebe um novo "carimbo de tempo", registrando assim o instante exato em que o **cliente** recebeu este documento eletrônico.

6. O **cliente**, opcionalmente, pode resgatar o cupom enviando-o para a **empresa** de modo a trocá-lo por algum benefício. Neste momento, a **empresa** terá condições de checar a validade[1] do cupom e, com isso, oferecer o benefício ao **cliente**. O

[1] A validade do cupom que pode ser verificada pela **empresa** diz respeito tanto à checagem da data de

cupom resgatado poderá ser armazenado num banco de dados da **empresa** para garantir que ele, caso o **cliente** tente utilizá-lo novamente, seja rejeitado. Neste momento em que é gravado no banco de dados, o cupom recebe novo "carimbo de tempo" que comprova o momento de seu resgate.

7. A **agência de publicidade** ou a **empresa** podem, opcionalmente, solicitar ao **Sistema de Auditoria** informações referentes à publicação dos anúncios para saber se eles foram publicados pelo **sítio anunciante** conforme combinado previamente no contrato.

8. O **Sistema de Auditoria**, a pedido da **agência de publicidade** ou por solicitação direta da **empresa**, fiscaliza a publicação dos anúncios pelo **sítio anunciante**; esta fiscalização é feita com o auxílio de uma **Autoridade de Datação** da seguinte forma:

   (a) O **Sistema de Auditoria** acessa[2] o **sítio anunciante** e obtém cupons eletrônicos como se fosse um **cliente**;

   (b) Os cupons obtidos são armazenados em uma base de dados para serem posteriormente remetidos à **empresa**; o cupom recebido pelo **Sistema de Auditoria** é datado com um "carimbo de tempo", tal como ocorre quando um cupom é remetido a um **cliente**;

   (c) Com base nos acessos feitos ao **sítio anunciante**, o **Sistema de Auditoria** envia os resultados da medição de publicação indicando se o contrato foi corretamente cumprido pelo **sítio anunciante** em termos de freqüência e horários pré-estabelecidos.

prazo (que pode ter sido opcionalmente estipulado pela empresa) quanto às assinaturas digitais contidas no cupom.

[2]O acesso ao **sítio anunciante** pode ser feito em momentos pré-determinados ou esporadicamente, conforme contrato de fiscalização feito com a **empresa** que o contratou

5.2.4 Compras Seguro

Este projeto tem como objetivo propor e implementar um sistemas de compras seguras [PER 02].

O processo de compras poderá ser para empresas privadas, para compras diretas ou leilões, e para empresas públicas, em concorrências, concursos, leilões, carta convite e tomadas de preço.

Os requisitos de segurança necessários para este protocolo são:

- Não deve ser possível o Comprador ser malicioso ou beneficiar-se de alguma forma do processo de compra;
- Fornecedor não pode provar qual foi sua oferta, ou mesmo se ofertou, antes da data de abertura das ofertas;
- O Comprador não pode verificar a identidade do Fornecedor antes da: abertura das propostas ou divulgação do resultado;
- O conteúdo das propostas deve ser confidencial até o momento da abertura das propostas;
- Nenhuma proposta pode ser entregue após o término do prazo de entrega das propostas;
- Todas as propostas entregues devem poder ser abertas após a data fixada para a abertura das propostas;
- Todo o processo de compra deve poder ser verificável por terceiros previamente estabelecidos.

Os requisitos de implementação do protocolo são:

- Alta disponibilidade;
- Escalável;

- Robusto;
- Customizável;
- Tolerante a falhas;
- Fácil de usar;
- Flexível (legislação, normas e procedimentos)
- Possibilidade de auditoria interna e externa.

A figura 5.5 mostra o protocolo proposto.

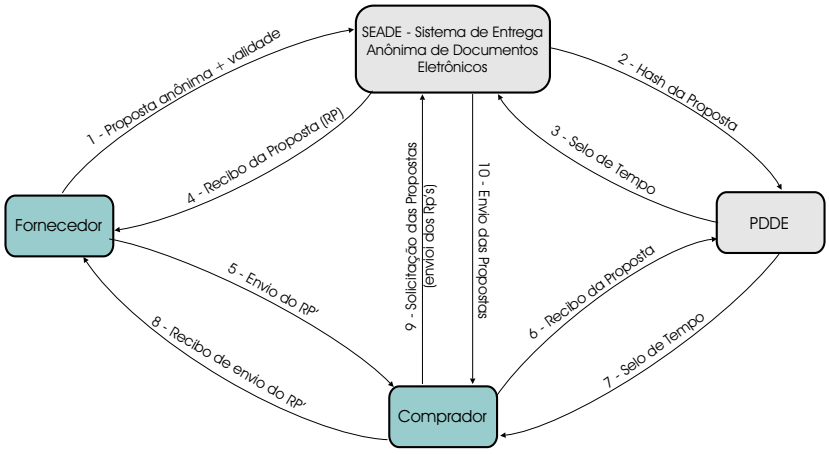

Figura 5.5: Protocolo Proposto Compras Seguro - O protocolo proposto neste trabalho é composto pelo Fornecedor, pelo Comprador, pela SEAD (Sistema de Entrega Anônima de Documentos Eletrônicos) e pela IDDE (Infra-Estrutura Digital de Documentos Eletrônicos).

5.3 Congressos da Área de Segurança de Computação

No Brasil temos dois principais congressos ligados a segurança, um é o SSI - Simpósio de Segurança de Informática - o evento é realizado pelo Centro Técnico Aeroespacial (CTA), o Instituto Tecnológico de Aeronáutica (ITA), através de sua Divisão

de Ciência da Computação (IEC) em parceria operacional com o Centro de Computação da Aeronáutica (CCA/SJ). O objetivo do SSI é divulgar e discutir os diversos aspectos relacionados com Segurança em Informática.

Os tópicos abordados no congresso são:

- Administração da Segurança;
- Aspectos Legais da Segurança;
- Auditoria e Análise de Segurança;
- Certificação de Sistemas e de Software;
- Confiança no Funcionamento (*Dependability*);
- Criptografia e Certificação Digital;
- Estratégias de Tolerância à Falhas;
- *Firewalls* e Ferramentas de Segurança de Sistemas;
- Forense Computacional;
- Medidas e Sistemas de Contingência Face a Desastres;
- Novos Paradigmas em Segurança;
- Padronização e Normalização;
- Pirataria de Software;
- Políticas de Segurança;
- Programação Segura;
- Redes Virtuais Privadas;
- Segurança Contra Intrusões (*Security*);
- Segurança Contra Riscos (*Safety*);

- Segurança de Sistemas Operacionais;
- Segurança em Computação Móvel;
- Segurança em Redes;
- Segurança em Sistemas Distribuídos;
- Segurança na Internet/Web;
- Segurança no Comércio Eletrônico;
- Segurança no Voto Eletrônico;
- Sistemas de Identificação e Controle de Acesso;
- Vírus e Outros Programas Nocivos.

O segundo congresso é o WSeg - Workshop em Segurança em Sistemas Computacionais - organizado pelo Programa de Pós-Graduação em Informática Aplicada da Pontifícia Universidade Católica do Paraná (PUCPR) sob coordenação do Prof. Carlos Maziero, com o objetivo de atuar como espaço para apresentação de pesquisas e atividades relevantes na área de segurança de sistemas de informação, integrando a comunidade brasileira de pesquisadores e profissionais atuantes nessa área [WSE 02]. O tema central do evento é a segurança de sistemas computacionais. Nesse contexto, destacamos os seguintes tópicos:

- Segurança em redes;
- Segurança em sistemas distribuídos;
- Segurança em sistemas operacionais;
- Técnicas de autenticação;
- Modelos de controle de acesso;
- Confidencialidade e integridade da informação;

- Técnicas criptográficas;
- Detecção de intrusão;
- Vulnerabilidades e ataques;
- Vírus, worms e outros códigos nocivos;
- Protocolos de segurança;
- Firewalls e filtragem de pacotes;
- VPNs e extranets;
- Políticas de segurança;
- Auditoria em sistemas;
- Avaliação da segurança;
- Gestão integrada da segurança;
- Segurança em aplicações Web;
- Segurança em comércio eletrônico.

Analisando os artigos aceitos para o evento observou-se que nenhum artigo aceito em 2002 tratou do tema segurança no comércio eletrônico [MAZ 02], e em 2001 apenas um artigo que tratava da segurança no comércio eletrônico foi aceito [MAZ 01] cujo tema trata da Segurança em Aplicações de Comércio Eletrônico Baseadas em Agentes Móveis.

5.4 Empresas desenvolvedoras de soluções

Existem produtos desenvolvidos por empresas para resolver a questão de segurança, entre este podemos citar o e-mail seguro no Outlook Express desenvolvido

pela Microsoft, que já tem agregado a característica e a infra-estrutura necessária para assinar e-mails digitalmente.

A maior parte dos produtos para trabalhar com workflow e e-mail já vem com a característica de assinar o documento com o certificado digital.

A questão de segurança do e-mail é muito importante pois a maioria das empresas fazem uso da Internet para o comércio eletrônico utilizando o e-mail como meio de comunicação, compra, para passar informações importantes e confidenciais aos clientes e parceiros de negócio.

5.5 Pesquisas relacionadas à segurança no comércio eletrônico

O comércio eletrônico é uma área excitante para pesquisa, por causa de suas novidades relativa ao crescimento explosivo.

Nesta seção apresentaremos o levantamento realizado sobre pesquisas que estão sendo realizadas sobre segurança no comércio eletrônico.

Os artigos analisados foram retirados das revistas científicas IEEE, LOUVASIER e NEC. Estes periódicos foram selecionados porque são possíveis meios de publicação sobre a área de segurança no comércio eletrônico.

Após o levantamento geral das referências bibliográficas, pode-se identificar as seguintes linhas de pesquisa:

1. Segurança dos dados e sistemas de comércio eletrônico;

2. Segurança Individual;

3. A utilização de componentes que ajudam os usuários a resolver questões empresariais são muito discutidas, tais como a utilização de agentes móveis e o XML;

4. Questões legais quanto a regulamentação do comércio eletrônico, assinatura digital, documentos eletrônicos.

5.5.1 Segurança dos dados e sistemas de comércio eletrônico

Muitos estudos estão sendo feitos relacionados à segurança dos dados e do sistema de comércio eletrônico. Na segurança de dados, as publicações recentes estão relacionados aos métodos de criptografia, tais como criptografia de chave pública ou privada. Além disso, modelos seguros [MAN 00], aplicações seguras [THU 01], a utilização dos protocolos SSL e SET são outras tecnologias populares disponíveis para ajudar proteger e garantir a privacidade e a segurança *on-line* [NGA 02] [OPP 99].

5.5.2 Segurança Individual

A segurança individual pode incluir senhas, controles de acesso ou assinaturas digitais. Além disso, os firewalls, os servidores de proxy, e rede VPN (*virtual private networking* - redes virtuais privadas) podem assegurar a proteção e segurança dos sistemas contra aos ataques externos e internos, tais como *hackers*, vírus, cavalo de tróia [MAR 02]. Conseqüentemente, estas tecnologias podem impedir a perda dos dados a fim preservar os serviços internos e externos [NGA 02] [OPP 99].

5.5.3 Utilização de Componentes

A utilização de componentes que ajudam os usuários a resolver questões empresariais são muito discutidas, tais como a utilização de agentes móveis e o XML.

O paradigma de agente móvel foi proposto como sendo uma solução promissora para facilitar a distribuição computacional em redes heterogêneas e abertas. Mobilidade, autonomia, e inteligência são identificados como características chaves dos sistemas de agentes móveis e disponíveis para a próxima geração de um comércio eletrônico inteligente na Internet.

Porém, existem problemas relacionados a segurança, especialmente proteção e integridade na tecnologia de agente móvel, os quais dificultam o uso difundido de agentes móveis.

Existem estudos que estão sendo realizados neste sentido, para garantir

a integridade do agente móvel contra ataques de agentes maliciosos, com o uso agentes dinâmicos e esquemas de verificação [WAN 02]. Também existe proposta de criação de um projeto de uma arquitetura segura de agentes para o comércio eletrônico, onde é proposto um protocolo de transporte de agentes [GUA 02], além de [COR 99] que propõe para um ambiente aberto e seguro para o uso de agentes móveis em aplicações de comércio eletrônico, para se proteger dos agentes maliciosos ele faz uso de dois agentes. O primeiro faz uso de uma terceira parte confiável para certificação, a segunda não assume uma entidade confiança e trata da distribuição, sendo que as duas são integradas. Onde o desempenho deste modelo é discutido.

Procurando avançar com os recursos de segurança em torno da linguagem XML, o Worldwide Web Consortium (W3C) recomendou a especificação XML Signature como um padrão da indústria. A especificação foi criada a partir de uma parceria entre o W3C e o Internet Engineering Task Force (IETF) visando capacitar a assinar de documentos e garantir a autenticidade dos mesmos [W3C 02].

A XML Signature, XML Encryption e XML Key Management, são as três especificações relacionadas à XML em desenvolvimento no W3C que contribuirão para a segurança dos serviços Web em geral.

5.6 Conclusão

A segurança de redes e da informação é uma questão atual, e um grande número de projetos de pesquisa estão sendo desenvolvidos dirigindo-se para esta área.

Os projetos desenvolvidos pelo LabSEC buscam estudar, pesquisar, avaliar e implementar soluções na área de segurança em computação.

No LabSEC está sendo desenvolvido um projeto direcionado para a pesquisa de segurança no comércio eletrônico. Devido a sua complexidade e grandeza da área de aplicação, este projeto foi dividido em vários sub-projetos, do qual esta dissertação faz parte. Neste capítulo foram apresentados os sub-projetos que completam este projeto em desenvolvimento.

Vários outros grupos de pesquisa estão buscando desenvolver soluções

a respeito de segurança de informação e de comércio eletrônico.

Capítulo 6

Programa de Pesquisa

6.1 Introdução

Analisando-se o contexto das aplicações de comércio eletrônico voltadas para a transação de negócios apresentadas no capítulo 4 seção 4.2, procurou-se observar as falhas de segurança nestas aplicações.

O objetivo deste capítulo é propor um programa de trabalho de pesquisa para segurança no comércio eletrônico, a fim tentar resolver os problemas de segurança observados, e tornar este ambiente seguro.

Este capítulo está estruturado de forma a apresentar as propostas de trabalho de pesquisa: a seção 6.2 apresenta uma proposta para resolver a questão da administração da confiança no comércio eletrônico. A seção 6.3 apresente para resolver a questão da negociação. A seção 6.4 apresenta uma proposta para entrega segura. A seção 6.5 da proteção da propriedade intelectual e a seção 6.6 para certificação dos softwares de comércio eletrônico.

6.2 Administração da Confiança

A administração de confiança pode ser definida como a atividade de fazer avaliações da confiança coletando, classificando, analisando e apresentando evidência

pertinente à segurança, com a finalidade de fazer avaliações e decisões. Atualmente não há nenhuma maneira sistemática e confiável de obter evidência sobre o sistema e das transações entre participantes em um ambiente de comércio eletrônico [JOS 00].

A identificação e integridade das partes através de interface de um sistema são importantes, pois é a prova a ser apresentada em última instância, e é a partir daí que a confiança é adquirida.

6.2.1 Projeto a ser Desenvolvido

Um projeto deverá ser desenvolvido, com o objetivo de garantir o controle da qualidade das transações entre os participantes de uma transação.

Primeiramente será eleito um órgão para fiscalizar e controlar as atividades. Este órgão fornecerá selos de qualidade para as empresas que atenderem aos requisitos recomendados. Segundo, deverá ser especificado para cada participante quais os processos que exigem controle no sentido de garantir a confiança dos participantes (clientes, empresas e fornecedores).

As empresas possuem processos distintos e particularidades próprias a serem controladas. Conforme descrito na seção 4.1 do capítulo 4, isso ocorre pois cada empresa possui um modelo próprio de aplicação no comércio eletrônico, ou seja, possuem processos críticos diferentes a serem controlados.

6.2.2 Requisitos de Segurança

O projeto deverá ser desenvolvido buscando atender os seguintes requisitos de segurança:

- Não repúdio da empresa, para não negar o cumprimento do seu dever;
- Não permitir a falsificação dos selos de controle de qualidade;
- Sistema genérico com a possibilidade de implantação em qualquer empresa, mas sem possibilidade de alteração no código gerador;

- Deve incluir a prova de sua competência e quais são os comportamentos corretos. A integridade da relação (interface) do sistema é particularmente importante porque é através da relação que a evidência está finalmente apresentada e a confiança está criada;

- O gerenciamento (administração) da confiança dependerá da existência de interfaces (relações) apropriadas com o usuário.

6.3 Negociação

A negociação é uma parte muito importante no processo de venda através da Internet, e a fim de suportar clientes de maneira suficiente os sistemas de comércio eletrônico necessitam habilidade de negociar. Negociação no comércio eletrônico pode ser definida como um processo onde duas partes barganham recursos para um lucro pretendido, usando ferramentas e técnicas para soluções de comércio eletrônico. A complexidade do processo da negociação depende da complexidade do produto ou do serviço que estão sendo negociados.

A sinalização do término do processo de negociação entre as parte é definida no momento em que o cliente ou cancela definitivamente a compra ou concretiza a compra com a confirmação do pedido.

6.3.1 Projeto a ser Desenvolvido

Um projeto deverá ser desenvolvido para criação de um sistema o qual irá agir como agente intermediador da negociação no comércio eletrônico, este poderá ser desenvolvido fazendo uso da tecnologia de agentes inteligentes, onde os clientes, fazendo uso desse sistema, poderão facilmente encontrar os produtos que melhor se adeqüem ao seu perfil de consumidor através de uma busca ao sítio da empresa, e também negociar itens específicos a serem adicionadas no produto/serviço, bem como seu valor, descontos, acréscimos, forma de pagamento, forma de entrega, ou seja, questões que envolvem interação entre o cliente e o vendedor, e que aqui será substituído pelo agente.

Várias pesquisas já foram desenvolvidas em cima de aplicação de agentes móveis no comércio eletrônico, mas não enfocando a questão da segurança e garantindo os interesses de todas as partes envolvidas no processo.

6.3.2 Requisitos de Segurança

Este software deverá estar baseado em cima dos seguintes requisitos de segurança:

- Sigilo;
- Autenticidade;
- Integridade;
- Não deve ser possível o Comprador ser malicioso ou beneficiar-se de alguma forma do processo de compra;
- Não-repúdio - Impossibilidade de uma das partes negar os acordos feitos durante o processo de negociação.

O software terá de resolver os seguintes problemas encontrados numa negociação na Web:

- Como estabelecer os termos da transação;
- Variar em duração e complexidade dependendo do mercado;
- Em mercados tradicionais de revenda, preços e outros aspectos são fixos, em outros mercados, os preços e outros aspectos são acordados integralmente no processo de compra.

O sistema deverá atender aos seguintes requisitos de implementação:

- Alta disponibilidade;
- Robustez;

- Tolerância a falhas;
- Facilidade de uso;
- Legalidade;
- Customizável e flexível (legislação, normas e procedimentos);
- Registro de todas as operações do sistema, para haver a possibilidade de auditoria.

6.4 Entrega

Hoje, muitos sistemas de entrega não são confiáveis. Um exemplo é quando o destinatário apenas assina um documento e recebe a encomenda sem precisar se identificar. Esta pessoa que recebeu a mercadoria pode não ser autorizada, ou não ser de confiança.

Por isso é necessário encontrar uma forma de autenticar o recebedor da mercadoria, podendo identificá-lo e responsabilizá-lo quando necessário.

6.4.1 Projeto a ser Desenvolvido

Um projeto deverá ser desenvolvido com o objetivo de controlar as entregas realizadas pelo sistema de comércio eletrônico, visando a segurança da operação.

Para implementação, uma tecnologia que poderá ser utilizada são os coletores de dados, onde o usuário deverá passar o cartão e ser identificado e certificado.

O sistema deverá ser fácil de ser entendido e utilizado pelo usuário.

6.4.2 Requisitos de Segurança

Requisitos de segurança necessários na solução a ser desenvolvida:

- Autenticidade das partes;
- Integridade da mercadoria recebida;

- Cumprimento dos prazos prometidos de entrega.

6.5 Proteção da Propriedade Intelectual

Segundo Belmon e Yee [BEL 98], *"A proteção propriedade intelectual é, normalmente, vista como necessária para as inovações. Proteger os criadores e seus trabalhos de outras pessoas usarem os seus trabalhos sem o devido pagamento, motiva economicamente a pesquisa e o desenvolvimento de novas idéias e tecnologias. Mas infelizmente, freqüentemente isto gera conflitos com a liberdade de uso"*.

No comércio eletrônico, devido a sua natureza, todos os dados e documentos trafecam de forma eletrônica na rede.

Um documento multimídia contém dados digitais que podem cifrar textos, imagens, audios e vídeo. A representação e distribuição digital dos documentos multimídia aumentaram o potencial para o mau uso e roubo, e intensificou significativamente os problemas associados com proteção dos direitos autorais. Os problemas estão enraizados devido as características intrínsecas de dados digitais, isto é, é fácil, barato e rápida a fabricação e distribuição de cópias, e cada cópia é idêntica a original. Conseqüentemente, a proteção da propriedade intelectual é uma condição necessária para o desenvolvimento próspero de aplicações de comércio eletrônico que dirigem as distribuições de bens imateriais.

6.5.1 Projeto a ser Desenvolvido

Com certeza para as aplicações de comércio eletrônico, tais como bibliotecas digitais e os serviços de publicação *on-line*, será importante usar técnicas de etiquetação eletrônica para proteção dos direito autorais. Estas técnicas poderão ser usadas para embutir secretamente marcas digitais em um material designado como informação protegida pelos direitos autorais, tais como origem, dono, conteúdo, ou receptor.

Conseqüentemente, técnicas de etiquetação eletrônica deverão ser desenvolvidas, o qual deverá ser eficiente, robusto, e seguro. Um exemplo de tecnologia de

etiquetação eletrônica a ser utilzada é a marca d'água.

Esta solução também deverá estar preparada para situações em que o usuário deverá pagar pelo acesso a informação que está protegida pela propriedade intelectual.

6.5.2 Requisitos de Segurança

Requisitos de segurança necessários na solução a ser desenvolvida:

- Controle das cópias dos documentos;
- Não será possível fazer modificação dos dados referente a propriedade intelectual do documento eletrônico;
- Acesso restrito quando o usuário tiver que pagar pela informação recebida.

6.6 Certificação da Segurança dos Softwares

Hoje, existem muitos protocolos para uso no comércio eletrônico inclusive SSL, SET, S-HTTP, S/MIME, Cybercash, e Digicash, entre outros. Estes protocolos garantem a transmissão segura dos dados dos clientes para os servidores. Porém, além da preocupação do tráfego das informações na Internet, está a preocupação com o sistema de comércio eletrônico que está sendo utilizado.

Um preocupação que deve-se ter é a confiabilidade deste software, pois o desenvolvimento de software seguro para uso nas aplicações de comércio eletrônico é um passo importante para sua aceitação e proliferação.

6.6.1 Projeto a ser Desenvolvido

É necessário fazer uma avaliação objetiva e científica da segurança é dos softwares de comércio eletrônico, e para chegarmos neste nível precisa-se desenvolver uma técnica para certificar o software, no sentido de garantir a confiabilidade esperada.

6.6.2 Requisitos de Segurança

Esta técnica de autenticação deverá certificar o software, para garantir:

- Estar de acordo com a política de segurança da empresa;
- Garantir que não seja malicioso, ou seja, que possua um comportamento seguro;
- Seja possível medir a grau de confiabilidade em cima de sua vulnerabilidade;
- Identificar falhas de segurança no sistema de comércio eletrônico;
- Determinar se os riscos do software são aceitáveis para o comércio eletrônico.

Independente das ferramentas utilizadas para o desenvolvimento deste software, questões referente a implementação, garantindo-se que este atende a todos os requisitos de segurança estabelecidos na política de segurança, devem ser resolvidas.

O pesquisador Anup K. Ghosh, da Reliable Software Technologies, proposto um algoritmo formal para a certificação de software, em seu artigo são discutidas questões referente a necessidade de certificação de software [GHO 99].

6.7 Conclusão

A análise das pesquisas a serem desenvolvidas foram feitas a partir do estudo do contexto das aplicações de comércio eletrônico, e identificou-se os seguintes projetos a serem desenvolvidos sobre segurança no comércio eletrônico:

- Administração da confiança no comércio eletrônico;
- Negociação;
- Proteção da propriedade intelectual;
- Auditoria de segurança em sistemas de comércio eletrônico.

Com o desenvolvimento destes projetos, o ambiente de comércio eletrônico se tornará mais seguro e confiável.

Contudo, a necessidade de desenvolver outros projetos surgirão, seja este voltados para o desenvolvimento de tecnologias de segurança que aqui não foram identificadas, ou seja para a integração de todas essas soluções existentes numa ferramenta integrada, tornando uma realidade para as empresas.

Capítulo 7

Desenvolvimento de Sistemas Seguros

7.1 Introdução

O objetivo deste capítulo é propor uma metodologia de desenvolvimento de um sistema de comércio eletrônico seguro através da identificação dos requisitos globais de segurança, da especificação e análise de um protocolo criptográficos que atenda a estes requisitos.

O capítulo está estruturado da seguinte forma: a seção 7.2 apresenta uma metodologia de desenvolvimento das soluções apresentadas no capítulo 6, a seção 7.3 apresenta requisitos globais de segurança para o comércio eletrônico, a seção 7.4 apresenta os requisitos de implementação da solução proposta, a seção 7.5 apresenta algumas das tecnologias existentes para verificação de protocolos criptográficos. A seção 7.6 apresenta o software SPEAR II como uma ferramenta para auxilar a análise do desempenho do protocolo criptográfico desenvolvido, e a seção 7.7 apresenta a conclusão do capítulo.

7.2 Desenvolvimento da Solução

Para o desenvolvimento das aplicações seguras no comércio eletrônico será necessário a criação de protocolos criptográficos específicos, pois estes oferecem a

infra-estrutura necessária para o desenvolvimento de aplicações seguras.

7.2.1 Projeto e Desenvolvimento de Protocolos

O projeto de desenvolvimento de protocolos deverá ser executado utilizando-se técnicas de métodos formais que auxiliam na documentação, especificação, projeto, análise e certificação, com o objetivo de aumentar a qualidade do protocolo criptográfico a ser desenvolvido.

O método formal para o projeto de um protocolo criptográfico envolve basicamente três etapas [BUT 99]:

Especificação A especificação é um dos estágios iniciais no processo de desenvolvimento de um sistema e tem por objetivo especificar de maneira completa e consistente os requisitos funcionais do protocolo criptográfico. Esta fase também engloba a descrição dos requisitos de segurança que o protocolo deve satisfazer.

Especificação Informal: É feito uso da linguagem natural (português) na especificação de protocolos, estando sujeita a ambigüidades, sensibilidade ao contexto e diferentes interpretações;

Especificação Formal: Descrição do funcionamento de um protocolo de forma precisa e concisa, totalmente ausente de ambigüidades. A especificação formal não invalida a especificação informal, complementa-a, e são empregadas técnicas formais de especificação.

Verificação É a fase em que é realizada a análise dos requisitos de segurança. Além da análise dos requisitos, esta fase prevê também a verificação do comportamento do protocolo perante agentes maliciosos;

Construção A construção é a formalização do protocolo. Consiste na utilização de notações formais, baseadas em técnicas matemáticas e na lógica formal para a construção do protocolo. A utilização de notações formais e formalismos matemáticos na construção de protocolos permitem reduzir erros e ambigüidades cometidos

durante este processo, gerando uma formalização precisa e não ambígua, sendo descrito o protocolo passo a passo. Esta etapa do desenvolvimento é responsável também por posteriores testes de consistência.

Um dos benefícios da especificação formal é a possibilidade da geração automática de testes, onde pode-se criar cenários de testes a partir da especificação formal.

A figura 7.1 descreve as etapas do desenvolvimento de um protocolo criptográfico utilizando-se de técnicas de métodos formais.

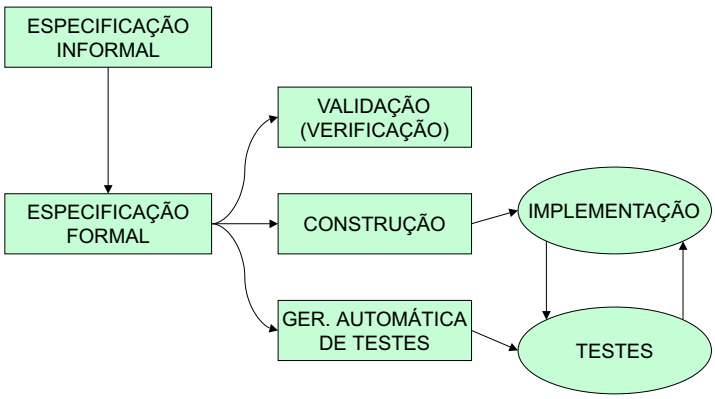

Figura 7.1: Métodos Formais - O método formal para o projeto de um protocolo criptográfico envolve três etapas: especificação, verificação e construção, com a possibilidade da geração automática.

7.3 Requisitos de Segurança

Deve-se estabelecer uma lista de requisitos de segurança para o protocolo a ser desenvolvido. Posteriormente, o sistema será avaliado para verificar se atende a estes requisitos. Caso todos os requisitos sejam atendidos o sistema será considerado seguro. Caso um ou outro requisito não seja atendido o sistema será considerado parcialmente seguro. Em muitas situações o não atendimento de um determinado requisito não implica numa perda de confiança no sistema.

Segue abaixo a lista de requisitos globais de um sistema de comércio eletrônico:

- Não-repúdio;
- Sigilo;
- Integridade;
- Autenticidade;
- Estar de acordo com a política de segurança da empresa.

Esses requisitos foram definidos baseando-se do estudo dos requisitos dos projetos a serem desenvolvidos apresentados no capítulo 6, conforme mostrado na tabela 7.1, podendo-se assim identificar os requisitos globais de segurança.

7.4 Requisitos de Implementação

Na implementação de um protocolo é necessário que se identifique quais os requisitos necessários para a sua implementação.

Requisitos básicos necessários:

Conveniência: tem que ser conveniente sua utilização, pois a usabilidade do software deve ser levada em consideração;

Robustez: deverá ser definido baseando num ambiente ideal, procurando eliminar os possibilidades de falhas na execução;

Flexibilidade: permitir adaptação em várias situações;

Mobilidade: não pode estar restrito apenas a local para utilização;

Escalabilidade: deverá permitir um número indefinido de participantes no processo em questão.

Tabela 7.1: Requisitos de segurança dos projetos. O Proj.1 refere-se ao Administração da Confiança, Proj.2 refere-se a Negociação, Proj.3 Entrega, Proj.4 Proteção da Propriedade Intelectual e Proj.5 Certificação dos Softwares de Comércio Eletrônico

Requisito de Segurança	**Proj.1**	**Proj.2**	**Proj.3**	**Proj.4**	**Proj.5**
Não repúdio das partes	X	X	X	X	X
Não permitir a falsificação dos selos de controle de qualidade	X				
Sistema genérico com a possibilidade de implantação em qualquer empresa	X				
Deve incluir a prova de sua competência e quais são os comportamentos corretos.	X				
O gerenciamento da confiança dependerá da existência de interfaces apropriadas com o usuário	X				
Sigilo	X	X	X	X	X
Autenticidade das partes	X	X	X	X	X
Integridade	X	X	X	X	X
Não deve ser possível o Comprador ser malicioso ou beneficiar-se de alguma forma do processo de compra		X			
Integridade da mercadoria recebida			X		
Cumprimento dos prazos prometidos de entrega			X		
Controle das cópias dos documentos				X	
Não será possível fazer modificação dos dados referente a propriedade intelectual do documento eletrônico				X	
Acesso restrito quando o usuário tiver que pagar pela informação recebida				X	
Estar de acordo com a política de segurança da empresa	X	X	X	X	X
Seja possível medir a grau de confiabilidade em cima de sua vulnerabilidade					X
Identificar falhas de segurança no sistema de comércio eletrônico					X
Determinar se os riscos do software					X

7.5 Verificação dos Protocolos

Os protocolos da segurança são cada vez mais necessários na era da informação. A necessidade estabelecer um nível elevado da confiança, que forneça os serviços de segurança necessários, tem sido reconhecida por muito tempo, mas também se conhece a dificuldade de estabelecer tal garantia [RYA 01b].

Várias tecnologias para verificação da segurança dos protocolos foram desenvolvidas. Burrows, Abadi e Needham desenvolveram a Lógica Ban, e tem como

principal objetivo fazer o raciocínio sobre as propriedades dos protocolos de segurança mais sistematicamente. A idéia básica é a certeza sobre o estado dos agentes envolvidos. Este estado envolve compreensão da certeza sobre as novas informações recebidas. Para este fim, o conhecimento inicial, suposições e etapas do protocolo são mapeadas em fórmulas de lógicas no processo conhecido e idealizado. Pode-se então definir que a Lógica Ban procura resolver o problema de autenticação. O inconveniente é que pode ser difícil interpretar as implicações exatas de uma prova executada usando a lógica [RYA 01a].

A lógica Ban popularizou a noção de usar lógicas para detectar falhas e redundâncias em protocolos. Foi considerado um sucesso por muitos comentaristas e usado para achar várias falhas em protocolos. A Lógica Ban foi base para a criação de várias outras lógicas, todas tentaram melhorar ou somar às premissas desenvolvidas. Um descendente popular da Lógica Ban é a Lógica GNY [SAU 01a], a qual aponta as deficiências do protocolo que está sendo analisado . O nome para a lógica GNY, originou-se do nome de seus autores, Li Gong, Roger Needham e Raphael Yahalom [MON 97].

Kemmerer desenvolveu a solução FDM e InaJo, baseando-se em alguns trabalhos mais adiantados de testes de especificações formal. Ele aplica o método formal FDM com a especificação formal da linguagem InaJo para o problema [RYA 01a]. FDM trata o problema como um máquina de estados, executando transições condicionais e correspondendo com as etapas do protocolo.

Mas, modelar e a analisar sistemas seguros têm sido, por muito tempo, conduzido usando estruturas não lógicas como o CSP (*Communicating Sequential Processes* - Comunicação de processos seqüencialmente). O CSP é uma estrutura matemática para a descrição e a análise dos sistemas que consistem em componentes (processos), e que interagem através da troca das mensagens.

Se a implementação do protocolo estiver sendo baseada em tais noções da análise para realizar-se serviços de segurança, é correto afirmar que esta também é uma ótima solução.

7.6 Software para Verificação de Protocolos

O desenvolvimento de lógicas para analisar a segurança de protocolos criptográficos originou técnica para assegurar o garantia destes protocolos. Para facilitar a especificação e verificação desses protocolos foi desenvolvido o SPEAR II [SAU 01b].

O SPEAR II é um aplicativo que implementou um *framework* para modelagem de protocolos criptográficos, baseado na lógica GNY para análise do desempenho do protocolo desenvolvido.

O software consegue reduzir a complexidade e a demora que normalmente ocorre na construção de protocolos criptográficos. Possui um ambiente amigável, efetivo e poderoso, e que pode ser usado para facilitar a criação de protocolos criptográficos seguros [SAU 01a].

O SPEAR II consiste em três componentes primários: um ambiente de especificação do protocolo (GYPSIE), uma interface de construção das declarações GNY (GNY Visual) e uma ferramenta para análise da construção GNY baseado em Prolog (GYNGER).

Primeiro deve-se entrar com as declarações de GNY que descrevem as condições iniciais, extensões e metas de protocolo. As declaração lógicas são definidas através de fórmulas.

Por exemplo um protocolo de troca de informação entre A e B, como mostra a figura 7.2, onde A envia mensagem X cifrada com a chave *Kab* para B, e B irá decifrar a mensagem recebida X com a chave *Sab*.

O software fornece opção para fazer análise do protocolo proposto. Após feita a análise é mostrado um resumo com os sucessos e fracassos do protocolo que está sendo testado, conforme mostra a figura 7.3.

7.7 Conclusão

Este capítulo apresentou uma proposta de metodologia para o desenvolvimento dos protocolos criptográficos através da utilização de métodos formais. Tam-

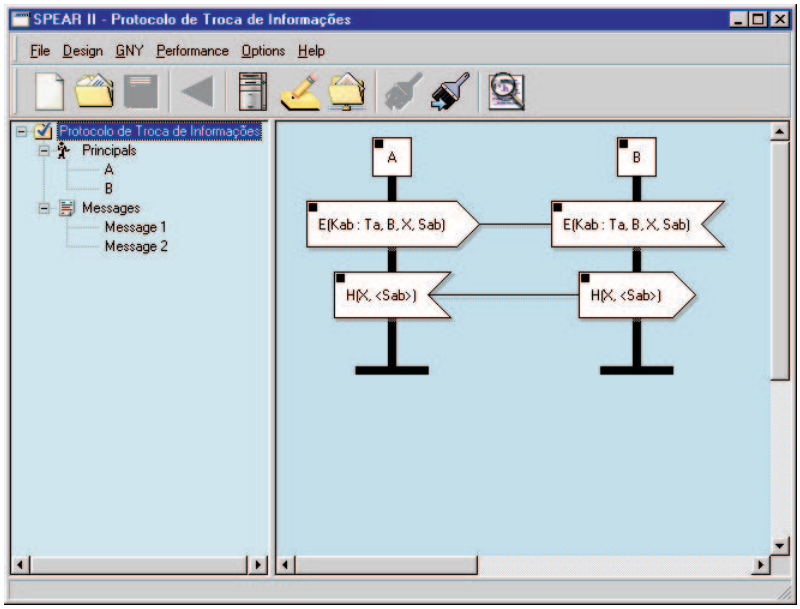

Figura 7.2: Software SPEAR II - A definição dos participantes A e B do protocolo é feito no item Principal do programa, e a definição da comunicação que existirá entre eles, bem como suas regras lógicas é feito no item mensagem do programa SPEAR II. A regra definida no programa mostra que A envia mensagem X cifrada com a chave Kab para B.

bém identificou os requisitos globais de segurança no comércio eletrônico, e os seus requisitos de implementação necessários.

Várias técnicas de verificação de protocolos criptográficos foram apresentadas, com o objetivo de apresentar soluções para elevar a confiança dos protocolos. Também apresentou o software SPEAR II como uma ferramenta para auxilar a análise do desempenho de um protocolo criptográfico desenvolvido.

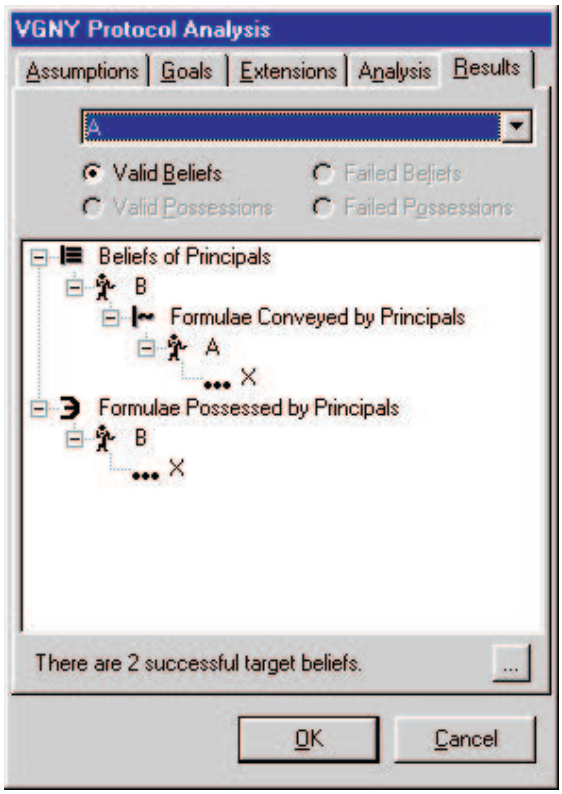

Figura 7.3: Análise do protocolo usando SPEAR II - Testa todas as fórmulas definidas pelos participantes A e B através da análise das fórmulas pela lógica GNY. Também Mostra quais fórmulas tiveram sucesso e quais fórmulas tiveram fracasso.

Capítulo 8

Considerações Finais

Neste trabalho procurou-se apresentar os vários aspectos relevantes ao comércio eletrônico e sua utilização, dando destaque a questão da segurança. Procurou-se desmistificar o comércio eletrônico como um meio vulnerável quanto a segurança, e demonstrar que este poderá ser seguro, desde que seus processos atendam aos requisitos de segurança exigidos.

Os objetivos deste trabalho foram atingidos na sua totalidade, pois atende as propostas definidas nos objetivos desta dissertação.

O primeiro objetivo específico foi ”Apresentar um panorama geral sobre comércio eletrônico”. Este objetivo foi alcançado através do estudo de suas principais definições, características, etapas da comercialização, formas de pagamento, vantagens e desvantagens do comércio eletrônico.

O segundo objetivo específico foi ”Apresentar os conceitos essenciais sobre segurança da informação, e estudar os principais mecanismos de segurança utilizados no comércio eletrônico”. Este objetivo foi alcançado e está relatado no capítulo 3 (Técnicas de Segurança em Computação). Este objetivo é fundamental para o entendimento do funcionamento da segurança de informação e os mecanismos necessários para garantí-la no comércio eletrônico.

O terceiro objetivo específico foi ”Estudar os sistemas de comércio eletrônico e identificar os processos numa aplicação de comércio eletrônico”. Este es-

tudo foi apresentado no capítulo 4 seção 4.2 onde foram identificados os processos de pré-venda, venda e pós-venda numa transação de negócio no comércio eletrônico.

O quarto objetivo específico foi ”Estudar os aspectos de segurança relacionados ao comércio eletrônico”. Este estudo foi apresentado no capítulo 4 seção 4.3 onde foi feita uma distinção entre os assuntos de segurança do lado do cliente, os assuntos de segurança do lado do servidor, os assuntos de segurança das transações e os assuntos de segurança organizacionais e legais.

O quinto objetivo específico foi ”Fazer levantamento dos estudos que estão sendo feitos atualmente quanto a segurança no comércio eletrônico”. Este resultado do levantamento de pesquisa foi apresentado no capítulo 4 seção 4.3.

O sexto objetivo específico foi ”Apresentar os projetos que estão sendo desenvolvidos pelo LabSEC (Laboratório de Segurança) da UFSC e de outros centros de pesquisa, quanto a segurança no comércio eletrônico”. Este objetivo foi atendido através da descrição dos projetos do LabSEC, e através da apresentação dos projetos de pesquisa relacionadas a segurança no comércio eletrônico por outros grupos de pesquisa, obtidos em artigos de revistas científicas e em congressos da área, apresentado no capítulo 5

O sétimo objetivo específico foi ”Propor um programa de trabalho de pesquisa para segurança no comércio eletrônico”. O capítulo 6 apresenta uma proposta de programa de trabalho de pesquisa no comércio eletrônico a fim de resolver os problemas de segurança encontrados e tornar o ambiente de comércio eletrônico via Internet seguro. A identificação dos problemas se deu através do análise dos processos de negócio identificados no capítulo 4 seção 4.2 e do levantamento dos estudos que estão sendo feitos atualmente quanto a segurança no comércio eletrônico, relatados no capítulo 6.

O oitavo objetivo específico foi ”Propor uma metodologia de desenvolvimento para os projetos a serem desenvolvidos”. Para atender este objetivo foi proposto o desenvolvimento de protocolos criptográficos específicos. Como metodologia de desenvolvimento foi sugerida a utilização de métodos formais, os quais auxiliam na documentação, especificação, projeto e análise dos protocolos criptográficos, apresentado no capítulo 7 seção 7.2.

O nono objetivo específico foi ”Identificar os requisitos globais de se-

gurança no comércio eletrônico, os quais deverão ser observados no desenvolvimento dos projetos de pesquisa a serem desenvolvidos". Os objetivos globais de segurança no comércio eletrônico foram apresentados no capítulo 7 seção 7.3.

O décimo e último objetivo específico foi "Apresenta um software que sirva como ferramenta para auxilar a análise do desempenho de um protocolo criptográfico desenvolvido". Apresentou-se o software SPEAR II, o qual é uma ferramenta que auxilia a análise do desempenho de um protocolo criptográfico desenvolvido, apresentado no capítulo 7 seção 7.5.

8.1 Contribuições deste trabalho

Primeiramente forneceu uma avaliação das aplicações de comércio eletrônico procurando dar uma visão geral em relação ao comércio tradicional X eletrônico e suas etapas de comercialização, e fazer uma avaliação geral de seus aspectos segurança, o qual foi apresentado no capítulo 4.

Apresentou-se uma visão dos projetos de pesquisa relacionadas a segurança no comércio eletrônico por grupos de pesquisa, obtidos em artigos de revistas científicas e em congressos da área. O resultado foi apresentado no capítulo 5.

Apresentou-se também uma proposta de programa de pesquisa para segurança no comércio eletrônico, a fim de tentar resolver os problemas de segurança identificados nas fases de pré-venda, venda e pós-venda, e tornar este ambiente seguro. O programa de pesquisa é apresentado no capítulo 6.

E, por fim, apresentou-se uma proposta de metodologia para o desenvolvimento de sistemas seguros de comércio eletrônico, através da identificação dos requisitos globais de segurança, da especificação e análise de um protocolo criptográficos que atenda a estes requisitos. Também apresentou o software SPEAR II como uma ferramenta para auxilar a análise do desempenho do protocolo criptográfico desenvolvido no capítulo 7.

8.2 Trabalhos Futuros

Os trabalhos desenvolvidos dentro do contexto desta dissertação oferecem subsídios ao desenvolvimento de outros projetos de pesquisa nesta universidade ou em outras instituições com interesse na área.

As sugestões são:

1. Desenvolvimento dos projetos sugeridos no programa de pesquisa;

2. Desenvolvimento de projeto para comunicação entre os diversos protocolos criptográficos utilizados numa aplicação de comércio eletrônico;

3. Estudar o aspecto legal que cerca as aplicações de comércio eletrônico;

4. Para a área de administração, desenvolver trabalho de levantamento de requisitos de implementação de soluções de comércio eletrônico;

5. Implementação dos projetos sugeridos.

Referências Bibliográficas

[ADA 01] ADAMS, C. et al. Internet x.509 public key infrastructure - time stamp Procolo(TSP). Internet Engineering Task Force, Maio, 2001. Relatório técnico.

[ALB 99] ALBERTIN, A. L. **Comércio Eletrônico - Modelo, Aspectos e Contradições de sua Aplicação**. São Paulo, SP: Editora Atlas, 1999.

[AND 00] ANDERSON, R.; LEE, J.-H. Jikzi a new framework for security policy, trusted publishing and electronic commerce. **Elsevier - Information and Management**, [S.l.], p.6, 2000.

[BAU 97] BAUM, M. S.; FORD, W. **Secure Eletronic Commerce**. Prentice-Hall, 1997.

[BEL 98] BELMON, S. G.; YEE, B. S. Mobile agents and intellectual property protection. **NEC Research Institute - Proceedings of the 2nd International Workshop on Mobile Agents**, [S.l.], p.11, 1998.

[BER 97] BERNSTEIN, T. **Segurança na Internet**. Rio de Janeiro, RJ: Editora Campus, 1997.

[BOR 02] BORTOLI, D. L. **O Documento Eletrônico no Ofício de Registro Civil de Pessoas Naturais**. Dissertação de Mestrado. Universidade Federal de Santa Catarina, julho, 2002. Dissertação de Mestrado.

[BRO 01] BROCARDO, M. L. **I2AC: um Protocolo Criptográfico para Análise Segura de Crédito**. Dissertação de Mestrado. Universidade Federal de Santa Catarina, novembro, 2001. Dissertação de Mestrado.

[BUT 99] BUTTYAN, L. Formal methods in the design of cryptographic protocols (state of the art). Swiss Federal Institute of Technology, novembro, 1999. Relatório TécnicoSSC/1999/038.

[CON 00] CONECTIVA. **Guia de Comércio Eletrônico**. Conectiva S.A., 2000.

[COR 99] CORRADI, A. et al. Mobile agents integrity for electronic commerce applications. In: PERGAMON - INFORMATION SYSTEMS, 1999. Elsevier - Computers and Industrial Engineering, 1999.

[EC 01] E-CASH. **E-Cash**. Disponível em <http://www.digicach.com>. Acesso em: outubro.

[FEG 99] FEGHII, J. **Digital Certificates - Applied Internet Security**. Addison Wesley Longman, Inc., 1999.

[GAR 99] GARFINKEL, S.; SPAFFORD, G. **Comércio e Segurança na Web**. Editora Market Books, Sã Paulo, 1999.

[GHI 01] GHISLERI, A. S. A. **Sistema Seguro de Atendimento ao Cliente Garantia da Qualidade de Serviço**. Dissertação de Mestrado. Universidade Federal de Santa Catarina, setembro, 2001. Dissertação de Mestrado.

[GHI 02] GHISLERII, L. R. G. **Proposta de um Protocolo Criptográfico para Auditoria de Publicidade na Web**. Proposta de Dissertação de Mestrado. Universidade Federal de Santa Catarina, junho, 2002. Dissertação de Mestrado.

[GHO 99] GHOSH, A. K. Certifying e-commerce software for security. **IEEE Computer Society - Procedings of the WECWIS'99**, [S.l.], p.4, abril, 1999.

[GUA 02] GUAN, S.-U.; YANG, Y. Safe: Secure agent roaming for e-commerce. **Elsevier - Computers and Industrial Engineering**, [S.l.], p.14, 2002.

[JOS 00] JOSANG, A.; TRAN, N. Trust management for e-commerce. **NEC Research Institute**, [S.l.], janeiro, 2000.

[MAN 00] MANCHALA, D. W. E-commerce trust metrics and models. **IEEE Computer Society**, [S.l.], 2000.

[MAR 02] MARCHANY, R. C.; TRONT, J. G. E-commerce security issues. **IEEE Computer Society**, [S.l.], 2002.

[MAZ 01] MAZIERO, C. **WSeg2001 - Workshop em Segurança em Sistemas Computacionais**. www.ppgia.pucpr.br/ maziero/seguranca/wseg2001.html.

[MAZ 02] MAZIERO, C. **WSeg2002 - Workshop em Segurança em Sistemas Computacionais**. www.ppgia.pucpr.br/ maziero/seguranca/wseg2002-pt.html.

[MON 97] MONNIAUX, D. **Méthodes formelles et cryptographie**. http://www.di.ens.fr/ monniaux/biblio/: École normale supérieure de Lyon, 1997. rapport de stage de seconde année de magistre.

[MUE 02] MUENCHINGER, N. et al. Electronic signatures - regulatory aspects of electronic signatures. **Elsevier - Computers and Industrial Engineering**, [S.l.], p.2, 2002.

[NGA 02] NGAI, E.; WAT, F. A literature review and classification of electronic commerce researchy. **Elsevier - Information e Management**, [S.l.], p.15, janeiro, 2002.

[oC 01] OF COMPUTING, F. O.-L. D. **Free On-Line Dictionary of Computing**. Disponível em <http://foldoc.doc.ic.ac.uk/foldoc>. Acesso em: julho.

[OPP 99] OPPLIGER, R. Shaping the research agenda for security in e-commerce. **IEEE Computer Society - Procedings of the DEXA99**, [S.l.], p.5, setembro, 1999.

[PAS 01] PASQUAL, E. S. **IDDE - Uma Infra-estrutura para a Datação de Documentos Eletrônicos**. Dissertação de Mestrado. Universidade Federal de Santa Catarina, abril, 2001. Dissertação de Mestrado.

[PER 02] PEREIRA, F. C. **Protocolos Criptográficos para Licitações Públicas e Privadas**.

[RIZ 01] RIZZO, I. **Sistemas Baseados em Casos**. Disponível em <http://black.rc.unesp.br/ccomp/ia/ia2000/caso/sistemas.htm>. Acesso em: 30 novembro de 2001.

[ROC 99] ROCKENBACK, A. **SET-F - Um Framework para Sistemas de Transações Eletrônicas Seguras Baseado no Padrão SET**. Dissertação de Mestrado. Universidade Federal de Rio Grande do Sul, 1999. Dissertação de Mestrado.

[ROS 00] ROSELINO, J. E. Comércio eletrônico: Dimensões e perspectivas. [S.l.], 2000.

[RYA 01a] RYAN, P.; SCHNEIDER, S. **Modelling and Analysis of Security Protocols**. Great Britain: Addison Wesley, 2001.

[RYA 01b] RYAN, P. et al. Modelling and analysis of security protocols. **NEC Research Institute**, [S.l.], p.22, 2001.

[SAU 01a] SAUL, E. **Facilitating the Modelling and Automated Analysis of Cryptographic Protocols**. Msc thesis. DNA Research Group, Computer Science Department, University of Cape Town, 2001. 235 p. Dissertação de Mestrado.

[SAU 01b] SAUL, E. Using gypsie, gynger and visual gny to analyze cryptographic protocols in spear ii. **Eighth Annual Working Conference on Information Security Management and Small Systems Security, Las Vegas-Nevada**, [S.l.], p.13, 2001.

[SCH 96] SCHNEIER, B. **Applied Cryptography, Second Edition: Protocols, Algorithms, and Source Code in C.** New York, 1996.

[STA 99] STALLINGS, W. **Cryptography and Network Security. Principles and Practice**. Prentice Hall, New York, 1999.

[STA 01] STANTON, M. **Legislação para o Comércio Eletrônico**. Disponível em <http://www.estadao.com.br/tecnologia>. Acesso em: 05 junho de 2002.

[THU 01] THURAISINGHAM, B. et al. Directions for web and e-commerce applications security. **IEEE Computer Society**, [S.l.], p.6, 2001.

[TOR 01] TORRUBIA, A.; MORA, F. J.; MARTI, L. Cryptography regulations for e-commerce and digital rights management. **Elsevier - Computers and Industrial Engineering**, [S.l.], p.15, 2001.

[VIS 97a] VISA, M. . **"SET - Secure Electronic Transaction Specification - Book 1: Business Description - Version 1.0**. SETco - Secure Electronic Transaction Consortium, 1997.

[VIS 97b] VISA, M. . **"SET - Secure Electronic Transaction Specification - Book 3: Formal Protocol Definition - Version 1.0**. SETco - Secure Electronic Transaction Consortium, 1997.

[W3C 02] W3C, W. W. C. **Worldwide Web Consortium - W3C**. www.w3c.org.

[WAN 00] WANGHAM, M. S. **Estudo e Implementação de um Esquema de Autorização Discricionária Baseado na Especificação CORBAsec**. Dissertação de Mestrado. Universidade Federal de Santa Catarina, março, 2000. Dissertação de Mestrado.

[WAN 02] WANG, T.; GUAN, S.-U.; HAN, T. K. Integrity protection for code-on-demand mobile agents in e-commerce. In: THE JOURNAL OF SYSTEMS AND SOFTWARE, 2002. Elsevier - Computers and Industrial Engineering, 2002. p.15.

[WES 00] WESTPHALL, C. M. **Um Esquema de Autorização para a Segurança em Sistemas Distribuídos de Larga Escala**. Tese de doutorado. Universidade Federal de Santa Catarina, dezembro, 2000. Dissertação de Mestrado.

[WSE 02] WSEG2002. **WSeg2002 - Workshop em Segurança em Sistemas Computacionais**. www.nce.ufrj.br/sbrc2002/wseg.html.

Apêndice A

Glossário

Assinatura Digital - Tem os mesmos propósitos da assinatura em papel e faz basicamente duas coisas: certifica, para o destinatário, que quem efetua a transação é de fato quem diz ser; e garante também que não houve alteração do conteúdo da mensagem entre a origem e o destino.

Autenticidade - garante a identidade de quem está enviando a mensagem, ou seja, poderemos assegurar a autoria de determinado documento. No documento tradicional demonstra-se essa autoria através da assinatura no documento. No documento eletrônico prova-se sua autenticidade com a assinatura digital.

Autoridade Certificadora - entidade que emite certificados de acordo com as práticas definidas na Declaração de Regras Operacionais - DRO. É comumente conhecida por sua abreviatura - AC.

Autoridade de Registro - entidade de registro. Pode estar fisicamente localizada em uma AC ou ser uma entidade de registro remota. É parte integrante de uma AC.

Criptografia - Arte de escrever em cifra ou em código. Conjunto de técnicas que permitem embaralhar informações para o envio das mesmas através de um meio público ou inseguro;

Cifrar - Escrever em cifra ou criptografar um texto aberto;

Chave Privada - senha secreta integrante de um par de chaves da infra-estrutura de chaves públicas utilizada para a cifração e ou decifração através de um algoritmo criptográfico. A chave privada é de conhecimento apenas de quem gerou o par das chaves;

Chave Pública - senha secreta integrante de um par de chaves da infra-estrutura de chaves públicas utilizada para a cifração e ou decifração através de um algoritmo criptográfico. A chave pública é distribuída para todos que desejarem decifrar mensagens cifradas enteriormente por um emissor com a sua chave privada;

Certificado Digital - O Certificado Digital é um arquivo eletrônico que identifica um indivíduo ou instituição. Alguns aplicativos de software utilizam esse arquivo para comprovar eletronicamente a identidade;

Decifrar - Ler, explicar ou interpretar o que está escrito em cifra. Decifrar um hieroglifo. Compreender ou revelar. Decriptografar;

Internet - Rede mundial de computadores interligados através de conexões telefônicas que disponibilizam informações em diversos sítios de inúmeras instituições. Permite também a troca de informações através de correio eletrônico (*e-mail*);

Smart card - pode ser um cartão de memória que armazena dados, mas requer um processador externo para acessar e manipular os dados. Ou pode ser um cartão processador que tem seu próprio microprocessador embutido, completo, com seu próprio sistema operacional, e pode processar e armazenar dados independentemente.

Sítio - Conjunto de documentos apresentados ou disponibilizados na Web por um indivíduo, empresa ou instituição e que pode ser acessado pela Internet;

Texto aberto - Mensagem ou texto legível que pode ser lido ou entendido por qualquer indivíduo;

Texto Cifrado - Resultado da aplicação de um algoritmo criptográfico sobre um texto aberto com a utilização de uma chave;

Web - Recurso ou serviço oferecido na Internet que consiste num sistema distribuído de acesso a informações, as quais são distribuídas na forma de hipertexto;