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

Amauri Sant' Anna Ghisleri

Sistema Seguro de Atendimento ao Cliente Garantia da Qualidade de Serviço

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

Florianópolis, Março de 2002

Sistema Seguro de Atendimento ao Cliente
Garantia da Qualidade de Serviço

Amauri Sant' Anna Ghisleri

Esta Dissertação foi julgada adequada para a obtenção do título de mestre em Ciência da Computação 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

Banca Examinadora

Prof. Ricardo Felipe Custódio, Dr.

Orientador

Prof. Waldir Leite Roque, Dr.

Prof. Carlos Roberto De Rolt, Dr.

Prof. Luiz Carlos Zancanella, Dr.

”Harmonização dos interesses dos participantes das relações de consumo e compatibilização da proteção do consumidor com a necessidade de desenvolvimento econômico e tecnológico, de modo a viabilizar os princípios nos quais se funda a ordem econômica, sempre com base na boa-fé e equilíbrio nas relações entre consumidores e fornecedores.”
Código de Proteção e Defesa do Consumidor
Capítulo II, Artigo 4.

Ofereço este trabalho aos meus pais, como demonstração de que não foram em vão seus esforços e resignações para me proporcionar este momento da minha vida acadêmica.

Agradecimentos

Primeiramente, ao meu orientador, professor Ricardo Felipe Custódio, que com o seu entusiasmo pela ciência, se excedeu em seu papel e me motivou para a realização deste trabalho.

À minha esposa Luciana, que emprestou seus ouvidos às minhas idéias, proporcionando discussões de bom nível técnico, o que, certamente tornou meu trabalho mais consistente.

Também não poderia esquecer da minha primeira professora, a tia Else, que ao me alfabetizar, abriu as portas do conhecimento e do saber.

Ao Professor Júlio da Silva Dias, pelo qual pude enriquecer o meu trabalho através de suas orientações sobre a análise e a verificação do protocolo criptográfico proposto nesse trabalho.

Aos grandes mestres das disciplinas ministradas em Joinville, que contribuíram com suas experiências de vida e seus conhecimentos para ampliar a minha visão da área e aguçar minha vontade de aprender mais.

Aos amigos de sala, que tornaram o ambiente amistoso e favorável ao aprendizado com a troca de experiências profissionais.

E sobretudo à DEUS, por me conceder esta oportunidade extraordinária, a vida.

Conteúdo

Lista de Figuras

Lista de Tabelas

Lista de Siglas

AA - Autoridade de Aviso;

AC - Autoridade Certificadora;

AD - Autoridade de Datação;

AF - Autoridade Fiscalizadora;

ASN.1 - Abstract Syntax Notation One;

BER - Basic Encoding Rules;

CL - Cliente; EM - Empresa;

CTPN - Cryptographic Timed Petri Net;

D - Decifração;

DER - Distinguished Encoding Rules;

E - Cifração;

E-mail - Eletronic Mail.

FEC - Fechamento;

K - Chave;

KR - Chave Privada;

KU - Chave Pública;

OS - Ordem de Serviço;

OSI - Open Systems Interconnections;

PKCS - Public Key Cryptography Standards;

RF - Recibo de Fechamento;

REQ - Requisição;

RR - Recibo da Requisição;

RSA - Rivest, Shamir e Adleman;

SAC - Sistema de Atendimento ao Cliente;

WWW - World Wide Web.

Resumo

Este trabalho apresenta 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.

Com a intenção de resolver este problema e garantir um nível aceitável de atendimento aos clientes, propõe-se neste trabalho um protocolo criptográfico com base em tecnologias de segurança e criptografia.

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.

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.

Técnicas de segurança e criptografia são amplamente utilizadas para a proposta do protocolo, de forma a garantir os requisitos de segurança necessários para transações eletrônicas de tal natureza.

Palavras chaves: Atendimento ao cliente, protocolos criptográficos, segurança, *helpdesk*.

Abstract

This paper introduces present-day models of cutomer service, dealing with difficulties of quality guarantee in service and in the preservation of customer rights as defined by law.

With the intention of solving this problem and assuring an acceptable level of consumer service, it is suggested in this paper a cryptographic protocol based on security and cryptographic tecnology.

The adoption of the suggested protocol is identifiable through a mark in the company web site that also determines the companys commitment to quality in consumer service.

The suggested protocol elects an inspecting authority that can keep pace and interfere with custumer service processes, in case their rights are threatened. Such inspecting authority can be companys own quality guarantee division, or a governmental division which may wish to monitor the activies of a civil service grant.

Security and criptographic techniques are widely used on protocol proposals, so as to guarantee security requiriments necessary on eletronic transactions of such a nature.

Key words: Consumer service, criptographic protocols, security, helpdesk.

Capítulo 1

Introdução

Com a concorrência acirrada das empresas pela conquista dos clientes, a busca da qualidade dos produtos e serviços prestados vem aumentando consideravelmente com o objetivo de fidelizá-los. A quantidade e similaridade de opções dadas ao cliente exige necessariamente uma maior qualidade das empresas que precisam encantá-lo para obter a sua confiança.

Ao contrário do que parece, manter um cliente fiel não é assim tão simples. Entretanto, isso é ainda mais barato do que se conquistar um novo. É necessário que exista um canal estreito de comunicação entre cliente e empresa para que o mesmo se sinta à vontade para manifestar suas opiniões e impressões sobre a empresa, atendimento, serviços e produtos.

A diversificação no atendimento com a utilização de recursos tecnológicos é uma boa receita para o sucesso no relacionamento com o cliente e pode também ser um fator preponderante para diferenciação da empresa em relação aos seus concorrentes. Com o inegável crescimento da Internet, muitas empresas apostam no atendimento eletrônico, o qual também, está se tornando muito popular e bem aceito pelos clientes. Deve-se porém, observar as características que tornam essa modalidade de atendimento eficaz. Disponibilizar recursos desse tipo e não tratá-los com a devida atenção, pode resultar no disperdício destes recursos e prejudicar ainda mais o relacionamento com os clientes.

Um sistema de atendimento eletrônico disponibilizado por uma empresa, deve, em primeiro lugar, garantir os direitos do consumidor previstos em lei, se utilizando de mecanismos que, de maneira confiável proporcionem isso. A garantia da qualidade desse tipo de atendimento prestado, de fato, encantará os clientes e diferenciará a empresa dos seus concorrentes. Outro fator preponderante para o sucesso de implementações de serviços dessa natureza é o tratamento personalizado aos pedidos dos clientes, onde o atendimento deverá ser individualizado para não dar a impressão fria de um processo automático. Em Santa Catarina, após a privatização da companhia telefônica estadual, houve grandes protestos contra a automatização dos serviços de atendimento aos clientes por não contemplarem a personalização dos mesmos, dando a impressão ao cliente, de que ele não passa de apenas mais um número para a empresa.

Para garantir a qualidade do atendimento eletrônico aos clientes, diversos requisitos de segurança devem ser atendidos para o sucesso da implementação desse tipo de serviço. As entidades envolvidas no processo deverão ser identificadas de forma segura e confiável e o transporte das transações deve ser sigiloso e íntegro.

1.1 Objetivos

O objetivo geral deste trabalho é propor um Protocolo Criptográfico de Atendimento ao Cliente, considerando-se a hostilidade relativa a segurança das informações em transações eletrônicas e garantindo a qualidade do serviço no atendimento aos clientes.

Levando-se em consideração as questões de segurança e de atendimento aos clientes, pode-se observar a necessidade de estudos minuciosos em muitos assuntos na área de segurança em computação e também na área da qualidade. Tais assuntos, nos permitem traçar objetivos específicos de aprendizagem e resultados durante o desenvolvimento deste trabalho como um todo. Dentre os objetivos específicos traçados durante as pesquisas relacionadas ao tema principal, pode-se destacar:

- Entender os modelos de relacionamento entre empresas e clientes, observar os sucessos e fracassos e identificar o perfil de empresas e clientes satisfeitos;

- Identificar problemas no relacionamento entre clientes e empresas resultantes da qualidade do atendimento;
- Estudar os modelos empregados pelas empresas e disponibilizados para o cliente no atendimento, suporte e pós-venda. Observar como as empresas procuram encantar para fidelizar seus clientes;
- Entender os modelos de comércio convencional e eletrônico;
- Avaliar os riscos das transações eletrônicas para as empresas e também para os clientes;
- Conhecer e levantar questões relacionadas a legalidade das transações eletrônicas e direitos dos consumidores;
- Estudar as tecnologias de segurança eletrônica de dados, criptografia e protocolos criptográficos;
- Entender a vulnerabilidade de sistemas eletrônicos, avaliando as ameaças e os riscos de ataques aos mesmos;
- Entender os requisitos de segurança através do estudo e avaliação de alguns protocolos criptográficos utilizados em diversos sistemas disponíveis;
- Avaliar e compreender as normas para a análise e especificação de protocolos, como também os padrões para o desenvolvimento dos mesmos;
- Propor um protocolo criptográfico seguro para a aplicação no atendimento à clientes através de transações eletrônicas com garantias de qualidade de serviço e auditoria;
- Descrever minuciosamente as fases do protocolo proposto e avaliá-lo de acordo com os objetivos traçados dentro dos requisitos de segurança estudados;
- Modelar o protocolo proposto com a utilização das técnicas das redes de Petri para a avaliação de suas propriedades.

1.2 Motivação

Com o crescimento no volume das transações eletrônicas, é importante observar a tendência que, em pouco tempo, muitos outros serviços poderão estar disponíveis a um simples clique do mouse. Para resolver os problemas de ataques e atender os requisitos de segurança em tais transações, muitas técnicas de criptografia e protocolos criptográficos são propostos e discutidos constantemente. No entanto, começa a surgir uma nova necessidade diante dessa realidade: a qualidade dos serviços prestados eletronicamente, a comprovação das transações e o respeito aos direitos do consumidor. A motivação desse trabalho fundamenta-se nestas necessidades.

A disponbilização deste tipo de serviço pela Internet precisa ser bem orquestrada pela empresas que o fazem, sob pena dos mesmos caírem em descrédito por parte dos clientes e consumidores. A possibilidade de criar um protocolo criptográfico que garanta o atendimento dos clientes que recorrem ao mesmo e, o interesse que algumas empresas demonstraram quando lhes apresentei essa idéia, me motivaram para a busca desse objetivo.

Um sistema de atendimento ao cliente (SAC) seguro, deve, além de atender os requisitos de segurança, gerar comprovantes eletrônicos confiáveis para assegurar os direitos do consumidor e garantir a idoneidade dos participantes. Tais comprovantes, poderão, a qualquer momento serem utilizados como prova para resolver eventuais litígios entre as entidades participantes do protocolo.

1.3 Materiais e Métodos

Para a realização deste trabalho, foi feito um amplo levantamento bibliográfico inerente aos problemas de atendimento ao cliente, e das tecnologias de segurança em computação disponíveis para o emprego em transações eletrônicas seguras. Também foi realizada uma pesquisa para a avaliação dos métodos atualmente empregados pelas empresas, no atendimento às sugestões e reclamações de seus clientes.

Diversas consultas eletrônicas em sistemas de atendimento ao clien-

te foram realizadas com o intúito de se obter informações sobre o funcionamento dos serviços disponibilizados pela Internet[1].

Para a especificação do protocolo proposto neste trabalho, foram utilizadas as técnicas das redes de Petri, aplicadas com a utilização do *software* ARP 2.4 LCMI-EEL-UFSC[2], o qual foi utilizado para a análise dos modelos e verificação da robustez do sistema proposto.

1.4 Trabalhos Correlacionados

Em diversas pesquisas realizadas na Internet à procura de algum produto relacionado com o tema do trabalho proposto nesta dissertação, pode-se observar a preocupação das empresas com o atendimento aos seus clientes em ambientes eletrônicos no que diz respeito a segurança das transações. Entretanto, nenhuma implementação que se preocupe com a garantia da qualidade dos serviços e o cumprimento dos acordos estabelecidos no atendimento eletrônico, foi encontrada.

O sítio http://www.helpdeskinst.com/ trata de questões relacionadas ao atendimento eletrônico em centrais de *Helpdesk*, tendo como associados empresas desenvolvedoras de *software* tais como a Tree Tools Informática Ltda. de Curitiba que desenvolveu um sistema de atendimento a clientes voltado para a resolução de problemas com o emprego de técnicas de inteligência artificial. Esse é um produto comercial de boa qualidade, porém também não implementa funcionalidades relacionadas com o tema do trabalho proposto.

[1]Diversos sítios foram consultados para a breve pesquisa mencionada acima. Entre eles estão: www.petrobras.com.br, www.angeloni.com.br, www.besc.com.br e www.brasiltelecom.com.br

[2]O *software* citado acima foi desenvolvido na Universidade Federal de Santa Catarina e pode ser obtido através do endereço http://www.das.ufsc.br/ farines/das6604/das6604.html#rdp na Internet.

1.5 Organização do Texto

O texto, dividido em capítulos, está organizado da seguinte maneira: no capítulo 2 são tratadas as questões de atendimento ao cliente, assim como os modelos mais empregados. Questões relacionadas a legalidade de transações eletrônicas e direitos do consumidor são tratadas no capítulo 3. No capítulo 4 são abordadas as tecnologias de segurança já amplamente testadas e que farão parte do protocolo proposto neste trabalho. O capítulo 5 trata do protocolo proposto, objeto principal deste trabalho. O capítulo 6 apresenta a formalização do protocolo proposto utilizando redes de petri. E finalmente, o capítulo 7 apresenta considerações finais sobre o trabalho desenvolvido. O anexo A contém as opiniões, obtidas através de comunicação via *e-mail*, da ombudsman da Petrobrás, as quais reforçam a importância deste trabalho. O anexo B apresenta a especificação das redes do protocolo de acordo com a sintaxe do programa ARP 2.4. O anexo C apresenta os padrões para o emprego de tecnologias de chave pública e criptografia. Estes padrões e recomendações deverão ser utilizados na implementação do protocolo proposto. No anexo D, é apresentada uma lista de termos utilizados na confecção deste trabalho com os seus respectivos significados que poderão facilitar a compreensão do texto.

Capítulo 2

Atendimento ao Cliente

2.1 Introdução

O atendimento ao cliente tem sido constantemente pauta de muitas reuniões nas empresas que fazem da qualidade dos seus serviços e produtos uma prioridade. Buscar a qualidade somente não basta. É preciso encantar os clientes para garantir a sua satisfação e fidelização.

As empresas que mantiverem o foco em seus clientes com a incorporação de eficácia no atendimento e qualidade em seus produtos e serviços, serão aquelas que experimentarão prosperidade a longo prazo [SHI 93]. Segundo Paladini [PAL 00], o que realmente induz um cliente a adquirir um produto, é o fato do mesmo atender às suas necessidades. Entretanto, os produtos que superam as expectativas dos consumidores, tendem a garantir a permanência das empresas no mercado. Deste modo, observa-se que o consumidor é a principal fonte de avaliação de um produto. "*A qualidade, assim, tem sua definição condicionada com o grau com que produtos e serviços atendem o consumidor*" [PAL 00].

Após a segunda guerra mundial, as empresas ocidentais, aproveitando-se da voracidade de consumo dos clientes, viveram um grande momento de crescimento e se voltaram para sofisticar as suas organizações. Preocupadas com os acionistas, as empresas se distanciaram dos clientes.

Por outro lado, no continente asiático, japoneses e coreanos desenvolviam modelos leves de organizações que buscavam acima de tudo a satisfação e atendimento dos anseios dos clientes.

Com a conquista de grandes fatias de mercado pelas empresas japonesas e coreanas no ocidente, constatou-se que o modelo asiático de relacionamento com os clientes era mais eficaz [dM 94]. Sendo assim, a adoção de estratégias de Qualidade Total por parte de empresas européias e americanas na busca de uma certificação de qualidade baseada em normas internacionais, foi apenas uma questão de tempo.

Filho [FIL 99] no entanto, adverte quanto a implementação do sistema de garantia da qualidade somente com o objetivo de se obter um certificado de qualidade total. Desta forma, a manutenção deste certificado poderá ser um problema, pois, o mesmo não reflete o comportamento real da empresa com relação aos compromissos de qualidade e sim apenas, como mais um apelo mercadológico.

Este capítulo aborda os aspectos estratégicos de atendimento ao cliente, assim como, os modelos adotados pelas empresas para fazê-lo. A seção 2.2, destaca a importância de se ouvir o cliente e como isso torna-se importante para a organização. Na seção 2.3, é feita uma abordagem dos modelos convencionais de atendimento ao cliente e da utilização do computador e métodos eletrônicos, dando-se um destaque para a Internet, estrutura sobre a qual, o protocolo proposto neste trabalho funcionará.

2.2 A Voz do Cliente

Segundo Moura [dM 94], as estratégias de qualidade das empresas, como não poderia deixar de ser, estão voltadas para a excelência de serviços e satisfação de seus clientes. Esse processo consiste em conhecer as suas expectativas e necessidades de forma mais profunda através de métodos que venham identificar o produto ou serviço que o cliente necessita, e ainda, o que ele está disposto a pagar ou esperar pelo produto ou serviço. Juran [JUR 95] recomenda às empresas que, para se descobrir as necessidades dos clientes é preciso: ser um cliente, comunicar-se com os seus clientes e simular o uso que os clientes fazem dos seus produtos.

Por outro lado, pesquisas de satisfação realizadas periodicamente pela empresa, oferecem uma visão geral dos problemas apontados pelos clientes e que devem ser discutidos pelos gerentes, supervisores e equipes de garantia da qualidade em geral.

"*Toda queixa lhe dá uma oportunidade de diferenciar sua companhia das outras"* [WHI 99]. Toda queixa se torna valiosa para uma empresa e a diferencia da concorrente, a partir do momento em que elas denunciam as expectativas e necessidades dos clientes. Whiteley [WHI 99] vai ainda mais longe ao afirmar que: "A única forma correta de administrar uma companhia - e a forma mais rentável - consiste em saturá-la com a voz dos clientes". Juran [JUR 95] destaca também a importância da comunicação com o cliente no sentido de obter informações a respeito da sua satisfação com o produto, para que as qualidades do mesmo possam ser acentuadas na sua comercialização.

No entanto, Shiozawa [SHI 93] afirma que a maioria dos clientes insatisfeitos com um produto ou serviço, não conta com o mesmo fornecedor novamente, caso sua queixa ou reclamação seja tratada com indiferença. Muitos são os casos em que as empresas nem tomam conhecimento da insatisfação dos clientes. Por outro lado, o cliente torna-se fiel a empresa à medida que seus problemas são resolvidos ou pelo menos, tratados com atenção.

2.2.1 O Ombusdsman

Esta palavra, de origem sueca que significa ouvidor ou representante do cidadão, passou a fazer bastante sentido a partir dos anos 90 para os brasileiros, quando os serviços de ombudsman de várias empresas se tornaram verdadeiros aliados dos clientes. Atuando em empresas públicas e privadas, o ombudsman, segundo matéria da Revista Época edição 89 de 31/01/2001, tem acesso direto a direção da empresa onde atua e ainda conta com uma certa imunidade pelo fato de criticar os modelos de gestão. Por desenvolver um trabalho de defesa do cliente da empresa, o ombudsman obtém estabilidade de emprego durante o cargo e ainda em algumas empresas, certo tempo depois. Algumas empresas, personificam essa figura e baseiam o serviço de ombudsman em um funcionário, do qual utilizam a imagem para campanhas de *marketing*, o que com certeza, torna o tratamento

com o cliente mais pessoal. As formas de acesso ao ombudsman de cada empresa podem ser através do contato pessoal, caixas de sugestões e reclamações com formulários pré-impressos, ligações telefônicas gratuitas e ainda pela Internet, através do preenchimento de um formulário padrão através de correio eletrônico. Segundo a visão que a Petrobrás tem desse serviço, as qualidades e atribuições da sua ombudsman são:

- Representar o cidadão perante a instituição em que atua;
- Viabilizar um canal direto de comunicação entre a empresa e o cidadão;
- Ter acesso direto ao dirigente do órgão em que atua;
- Ter autonomia e independência;
- Atuar para melhorar a qualidade do produto/serviço prestado, devendo promover uma parceria interna em prol da qualidade;
- Agilizar informações e simplificar procedimentos;
- Encaminhar a questão apresentada à área que deve solucioná-la e acompanhar os procedimentos;
- Ter acesso livre às informações internas para apurar e propor soluções;
- Atuar na solução e prevenção de conflitos;
- Preservar a credibilidade;
- Garantir os direitos do cidadão;
- Apresentar relatórios regulares ao dirigente da instituição em que atua.

2.3 Os Modelos de Atendimento ao Cliente

Muitas são as formas atualmente utilizadas de atendimento ao cliente, tanto para ouvir suas reclamações de pós-venda, como para esclarecer dúvidas sobre produtos e serviços e ainda a própria contratação e compra de serviços e produtos respectivamente.

Moura [dM 94] salienta a importância da criação e manutenção de mecanismos e oportunidades para que os clientes exponham suas reclamações, expectativas e solicitações. Quanto mais simplificado e próximo do cliente for o meio de comunicação, melhor, pois, sabe-se que a maioria deles não reclama e simplesmente procura outro fornecedor.

A variação desses métodos para a coleta de informações das impressões dos clientes a respeito dos produtos e serviços, pode variar bastante de acordo com o tipo de cliente que a empresa tem e também pelo tipo de produto ou serviço comercializados. Alguns métodos são os que se pode chamar de universais como os formulários de avaliações e comentários ou ligações telefônicas através de números gratuitos.

A seguir, serão abordados alguns desses métodos com as suas respectivas características, mas, que tem como objetivo comum estreitar a relação com o cliente.

2.3.1 Caixa de Coleta de Sugestões

Este é sem dúvida, um dos métodos mais simples e de baixo custo de implementação, porém, muito eficiente pela sua popularidade. Consiste da disponibilização de uma urna para a coleta de sugestões, críticas ou reclamações sobre o atendimento. Como incentivo do seu uso, em alguns casos, o cliente recebe ao final do atendimento um formulário apropriado para que manifeste as suas impressões, o qual, serve também de cupom para um sorteio qualquer.

2.3.2 Painéis Eletrônicos

É bastante comum encontrarmos painéis eletrônicos com as opções ótimo, bom, regular e ruim, ou ainda, satisfeito e insatisfeito, para a manifestação das impressões referente a instituição. Quando pressionado pelo cliente um botão que desaprove o atendimento, imediatamente o mesmo é abordado pelo ombudsman que ouve a sua queixa. Esse modelo é utilizado pelas Lojas Renner[1] com a intenção de captar as necessidades e anseios dos clientes.

[1]Existe um painel eletrônico nas lojas, ao qual foi dado o nome de Encantômetro.

2.3.3 Ligações Gratuitas 0800

Outra forma que se tornou bastante popular para o atendimento ao cliente, é o serviço de ligações telefônicas gratuitas. Muitas empresas, estruturam a sua forma de atendimento somente pelo telefone. Este é o caso de empresas que trabalham no sistema de tele-entrega como os "disk-pizza", "disk-flores", "disk-mensagem", entre outros. O telefone realmente se tornou popular no atendimento ao cliente e atualmente é inconcebível que empresas, mesmo as chamadas 'virtuais' (ponto com), não possuam atendimento por telefone. É muito comum encontrarmos em diversos produtos um número 0800 ... para a ligação gratuita com incentivo ao cliente em manifestar sua opinião e conversar com a empresa fornecedora do seu produto ou serviço. Novamente, se observa a insistência no contato com o cliente, para que ele reporte as suas impressões sobre a empresa, seus produtos e/ou serviços.

Muitas empresas possuem setores específicos para o tratamento de chamadas telefônicas desse tipo (*CALL CENTER*), onde o atendimento é altamente padronizado, sendo feitos por atendentes muito bem qualificados no tratamento com o cliente. Nestes casos, centrais telefônicas computadorizadas atendem automaticamente o cliente e direcionam a ligação de forma inteligente. Em alguns casos, o atendimento poderá parecer frio com o cliente por se tratar de gravações. Neste caso enquadram-se as operadoras de cartões de crédito.

Existem ainda alguns outros serviços que seguem a mesma linha de raciocínio, porém, contam com um marketing para torná-los personalizados para o cliente. É o caso da figura do Ombudsman dos Supermercados Angeloni[2] (Sr. João, da Petrobrás[3] (Sra. Vera) e do Banco do Estado de Santa Catarina[4] (projeto ouvidor), por exemplo. O cliente, sabendo da existência de uma pessoa designada especialmente para ouvir os seus comentários, sente-se mais valorizado e também mais à vontade para fazê-los.

Alguns serviços para o atendimento telefônico, são bastante criativos, pois facilitam a memorização dos números através de técnicas como a associação dos

[2] www.angeloni.com.br

[3] www.petrobras.com.br

[4] www.besc.com.br

números às letras no teclado do telefone que formam o nome da empresa.

2.3.4 Correios

Na compra de qualquer produto de empresas comprometidas com a qualidade e satisfação de seus clientes, juntamente com a documentação e manuais do mesmo, encontra-se quase sempre um carta resposta comercial (com porte já pago), para qualquer manifestação do usuário. Formulários de sugestões e críticas de serviços prestados por uma oficina, podem ser também remetidos pelos correios. O cliente recebe tal formulário logo após o serviço ter sido executado e com isso pode então manifestar sua opinião. Esse modelo é adotado pela Dpaschoal[5] em todo o Brasil.

A Brasil Telecom[6] , dispõe de vários serviços que os seus assinantes podem realizar através dos correios. Um desses serviços, é a possibilidade de mudança de titularidade da assinatura de uma linha telefônica. O usuário preenche um formulário específico disponível nas agências dos correios com os seus dados e os do novo titular, reconhece a assinatura de ambos em cartório e devolve-o aos correios. Dentro de alguns dias, a transação é realizada pela empresa.

A Editora Abril[7] também está fortemente estruturada com o uso dos serviços dos correios. As solicitações de assinaturas de revistas são aceitas pelos correios e após a confirmação do(s) pagamento(s), a entrega dos exemplares passa a ocorrer periodicamente.

2.3.5 O Computador

Cortada [COR 94] diz que é impossível se imaginar processos e serviços de qualidade sem considerar-se a utilização das tecnologias da informação. O computador pode realizar muito bem três tarefas que para a garantia da qualidade dos serviços e atendimento ao cliente são fundamentais:

[5] www.dpaschoal.com.br

[6] www.brasiltelecom.com.br

[7] www.abril.com.br

- **Controle**: o controle da eficácia dos processos e a geração de dados para que o mesmo possa ser melhorado pelo seu responsável, é algo desejado nos sistemas de informações disponíveis nas empresas para o relacionamento com os seus clientes;

- **Armazenamento de informações**: armazenar informações em bancos de dados para acesso on-line dos atendentes é outro fator positivo, pois, permite a consulta das características dos produtos e serviços e também a disponibilidade dos mesmos, dando assim, maior dinamismo ao processo. Alguns sistemas de informação vão ainda mais longe, disponibilizado na própria Internet, essas informações para consulta direta dos clientes;

- **Linhas de comunicação**: a redução no ciclo de tempo de uma transação ou atendimento é a terceira virtude do uso dos computadores. O uso do correio eletrônico possibilita uma aproximação virtual do cliente com a empresa fornecedora de produtos e/ou serviços. Atualmente, o comércio eletrônico também já é uma realidade.

O emprego dos computadores e sistemas de informação tem objetivado, já há muito tempo o aumento da eficácia dos processos e a redução de custos para proporcionar a tomada de decisões. A comercialização de produtos com o auxílio dos computadores começou a ocorrer na metade da década de 1980. No final dos anos 80, as empresas, mais concentradas na prestação de serviços, descobriram que os computadores poderiam elevar a qualidade dos serviços prestados e não somente melhorar a eficiência, como se pensava.

2.3.6 Internet

O atendimento aos clientes através da Internet, merece aqui um destaque especial por diversas razões. A praticidade e comodidade proporcionada ao cliente, a rapidez com que o processo como um todo pode ocorrer aliados aos aspectos multimídia da Internet, fazem dela um instrumento para garantir a qualidade das empresas, além do seu baixo custo de manutenção. Utilizar uma tecnologia como essa, é uma estratégia que segundo a definição de Denton [DEN 90] é descobrir e desenvolver serviços diferenciados que proporcionem

à empresa um avanço sobre os seus concorrentes. Uma tecnologia apropriada poderá trazer grandes benefícios e resultados para o relacionamento com o cliente.

Embora essa tecnologia esteja extremamente difundida no mundo todo, a sua utilização, em muitos casos, ainda ocorre de forma bastante relaxada. Muitas empresas ainda não se deram conta de que a Internet é uma ferramenta barata e com grande crescimento de adeptos. O número de clientes que, justamente pela comodidade preferem primeiro navegar na grande rede para então comprar produtos e contratar serviços cresce a cada dia.

No entanto, a segurança é ainda um fator melindroso para os clientes internautas que, em muitos casos, pela falta de conhecimento das tecnologias que tornam as transações seguras, acabam recorrendo aos métodos tradicionais de comércio e atendimento. Espera-se que assim como no caso dos bancos, que contam hoje com grande volume de transações eletrônicas, essa cultura mude rapidamente. É preciso que as empresas se conscientizem a respeito desta questão e tornem a segurança um atrativo para o atendimento virtual de seus clientes.

Segundo Garfinkel [GAR 99], um computador é seguro se pudermos ter certeza de que tanto ele como o software se comportarão da forma desejada e esperada por nós. A segurança na Web, pode ser conseguida com a prática de procedimentos e tecnologias usadas para resguardar os servidores das empresas e seus usuários dos comportamentos inesperados. Sendo a Internet uma rede pública, a segurança na utilização da mesma deve ser tratada sob diversos aspectos:

- **Uma rede de duas vias:** enquanto empresas disponibilizam informações para milhões de pessoas, *hackers*[8] e *crackers*[9], procuram violar a segurança desses servidores;

- **Reputação das empresas:** cada vez mais empresas aderem ao uso da Internet para a divulgação de seus produtos e serviços e o número de transações comerciais

[8] profundos conhecedores de computadores e computação e habilidosos para enganar os mecanismos de segurança de sistemas, conseguindo assim acesso não autorizado.

[9] *hackers* mal-intencionados que ao obterem sucesso no ataque, podem destruir, corromper, ou roubar informações.

cresce a cada instante, porém, a imagem dessas empresas pode estar seriamente comprometida se os seus computadores estiverem sujeitos a ataques;

- **Falhas nos softwares:** navegadores e servidores de Internet são programas que como já se sabe, podem apresentar falhas potenciais de segurança pela maneira com que muitos recursos são adicionados aos mesmos a cada versão. Logo, mesmo um software que tenha sido instalado adequadamente, pode ainda assim representar uma ameaça à segurança;

- **Informações na mão do inimigo:** tendo a segurança sido quebrada uma vez, *crackers* poderão se valer dos navegadores e servidores para desferir novos ataques contra os usuários e as empresas;

- **Consciência dos riscos:** os usuários, precisam lidar com questões de segurança, que, muitas vezes eles nem sequer ouviram falar. Isso torna o processo como um todo de certa forma vulnerável;

- **O preço:** é muito mais dispendioso se resolver problemas de segurança causados por ataques aos sistemas, do que se tomar medidas preventivas para evitá-los.

Afinal, o que pode-se chamar então de um servidor Web seguro? Existem três visões, que segundo Garfinkel [GAR 99], podem ser dadas sob o ponto de vista dos fornecedores de softwares, dos usuários e das empresas que possuem os servidores Web:

- **Fornecedores de software:** é um programa que implementa esquemas de segurança (protocolos criptográficos), que garantem a troca de informações sigilosas, entre o servidor e um navegador de um cliente;

- **Usuário ou Cliente:** é toda uma tecnologia que garante a sua privacidade, resguardando os seus dados que são enviados ou recebidos pela Web;

- **Empresa:** é aquele que resiste a ataques feitos através da Internet ou mesmo de dentro da própria empresa por pessoas mal-intencionadas.

Na verdade, pode-se dizer que um servidor de Web seguro é tudo isso e ainda deve contar com cópias de segurança de hardware e software, para que se ocorrerem eventuais falhas, o sistema como um todo possa ser reconstituído rapidamente sem traumas. Outro quesito desejável ainda, é a possibilidade de expansão, onde o servidor possa ser constantemente reconfigurado para suportar mais adequadamente as crescentes requisições.

Muitos serviços, hoje em dia, são disponibilizados pelas empresas a seus clientes através da Internet. Para facilitar a compreensão, a seguir serão descritas cada uma dessas categorias separadamente, observando sempre o tipo de serviço prestado pelo sítio, estratégias das empresas e aspectos de segurança tanto para os negócios como para os clientes:

- **Sítios de Informações:** a grande maioria dos sítios, inclusive os que se enquadrarão também nas categorias seguintes se encontram aqui. Todo sítio sobre uma empresa ou organização, visa em primeiro lugar divulgar as características dos produtos e serviços que oferecem. Através da Web, pode-se transcender fronteiras a custos irrisórios se comparados aos de outras mídias. O compromisso com a veracidade e autenticidade das informações disponíveis nestas páginas porém, deve ser grande e de inteira responsabilidade do(s) seu(s) publicador(es). Um ataque por cracker a um servidor deste tipo pode comprometer seriamente a imagem da empresa e tornar as informações ali publicadas, não confiáveis. Nessa categoria, aparecem também os sítios de empresas jornalísticas que são muito visitados pois fornecem a todo momento, informações atualizadas de acontecimentos no mundo todo, previsão do tempo, indicadores econômicos e assim por diante. Destacam-se pelo conteúdo disponibilizado aos internautas. Os sítios www.uol.com.br, www.terra.com.br e www.globo.com, são exemplos dessa categoria. Outros gigantes neste gênero são os sítios de pesquisa. Servem como ponto de partida para se encontrar qualquer tipo de informação na Web pela simples digitação de palavras-chave para busca. São mantidos por anunciantes interessados nos usuários dos seus serviços. São exemplos destes sítios: www.cade.com.br, www.yahoo.com, www.google.com, entre outros.

- **Sítios de Comércio Eletrônico:** Este é um segmento que sem dúvida alguma está em franca expansão na Internet. Todas as expectativas de crescimento do comércio eletrônico, vem sendo superadas a cada ano pelo faturamento apurado das empresas em seus exercícios anteriores. Isso demonstra que as pessoas, de fato, estão cada vez mais aderindo a esse tipo de serviço. Porém, como no processo tradicional, uma compra com cartão de crédito pela Internet também está sujeita a fraudes. De acordo com Garfinkel [GAR 99], numa transação de comércio eletrônico, tanto o proprietário de um cartão de crédito quanto o negociante correm riscos. Do lado do cliente, existem duas situações críticas:

  – A rede pode ter sido interceptada e no momento que o cliente informa o número do seu cartão, o interceptor toma conhecimento e passa então a fazer uso do mesmo. Como agravante ainda, o dono do cartão só saberá que o seu número foi roubado quando receber a próxima fatura de pagamento;

  – O débito pode ter sido efetuado no cartão, mas, a mercadoria jamais chegar. Quando o cliente se der conta de verificar a empresa com a qual realizou a transação, poderá descobrir que a mesma nem existe. É tudo fraude.

  Tecnologias de criptografia que serão tratadas no capítulo, 4 resolvem com eficiência essas duas questões, garantindo de forma extremamente segura o transporte dos dados pela rede de forma sigilosa e a identificação das empresas.

  Sobre os riscos para o negociante neste proce sso, pode-se também apontar dois, dentre vários outros:

  – Se o seu servidor não for devidamente seguro, poderá ser invadido por *crackers* que terão acesso aos números de cartões e poderão, no futuro, gerar transações fraudulentas;

  – Uma pessoa com um número de cartão roubado pode inserir no sistema do negociante diversos pedidos de compra sem levantar suspeitas (crime de falsidade ideológica).

O atendimento ao cliente, através de sítios de comércio eletrônico, segue os passos descritos abaixo e identificados na figura 2.1. Para ilustrar uma transação eletrônica, será utilizado o exemplo clássico da compra de um CD por um internauta:

1. **Passo:** o cliente, através do preenchimento de um formulário próprio disponível no sítio do comerciante, envia a sua solicitação de compra;
2. **Passo:** o provedor no qual o cliente possui uma assinatura, recebe as informações e as envia para o servidor de transações do comerciante;
3. **Passo:** no servidor do negociante, os dados do cartão do cliente, assim como a disponibilidade do(s) produto(s) solicitado(s) pelo mesmo, são devidamente checados e então, neste momento, a transação é realizada. O estoque da empresa é automaticamente baixado pela solicitação de compra;
4. **Passo:** O valor da compra é repassado para o banco do cliente para futuro débito e para o banco do comerciante para futuro crédito;
5. **Passo:** após isso, uma ordem de despacho das mercadorias é encaminhada ao setor de expedição da empresa;
6. **Passo:** o setor de expedição da empresa remete os produtos ao cliente através de serviços de entrega, os quais chegarão em média ao destino, 2 ou 3 dias após o pedido.

Os sítios para transações financeiras são os outros grandes utilizadores desta tecnologia que à exemplo dos sítios de compra e venda, também precisam de muita segurança. Neste caso, o número de participantes do processo é menor, tendo-se o cliente, seu provedor de acesso à Internet e a instituição financeira.

Para garantir a segurança de todas essas transações, são implementadas tecnologias de certificação, assinaturas digitais e criptografia, onde pode-se com segurança, identificar os participantes do processo e transportar os dados de forma sigilosa. Essas tecnologias serão abordadas com detalhes no próximo capítulo, onde serão tratadas as questões específicas de segurança.

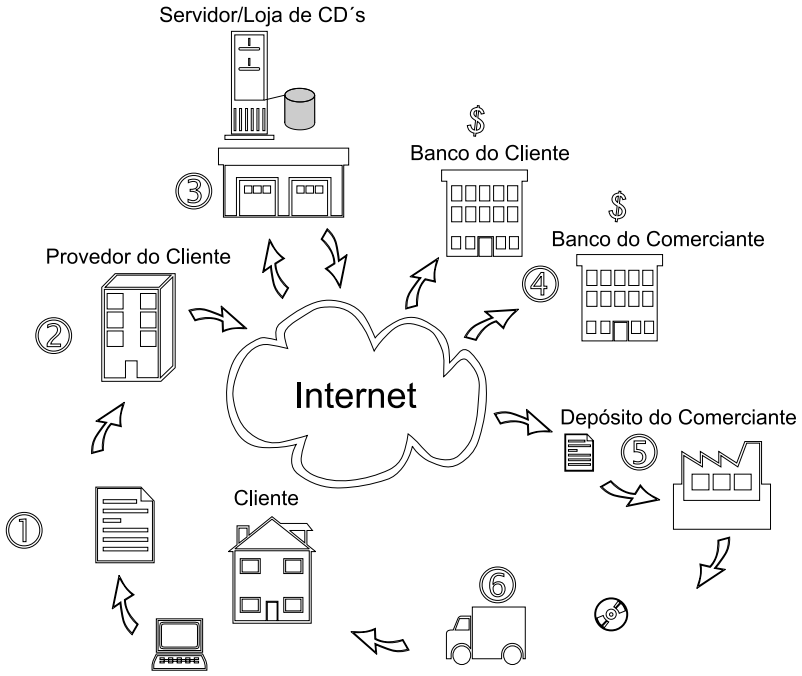

Figura 2.1: Modelo de Comércio Eletrônico. O modelo atual para o comércio eletrônico é apresentado nesta figura, onde são identificadas as operações para a realização da transação desde o pedido do cliente até o recebimento da mercadoria.

- **Sítios de Sistemas de Ajuda (*HELPDESK*):** Na grande maioria dos sítios, inclusive os que já foram citados acima, é comum encontrarmos uma opção do tipo *fale conosco*. Esses links criados nas páginas das empresas, geralmente levam a um formulário padrão onde o cliente é obrigado a fornecer seus dados para um atendimento futuro. Esse processo porém, não passa de um assistente para o envio de um *e-mail* que o cliente poderia ter mandado diretamente. Em outros casos, o sítio simplesmente abre uma nova mensagem no programa de *e-mail* do cliente, permitindo que ele escreva à vontade. De uma forma ou de outra, isso não mede a qualidade do atendimento das empresas, mas sim, a rapidez e maneira com que se manifestam ao receber as mensagens. Segundo Ciancio [CAR 01], utilizar corretamente as técnicas de marketing virtual, é o segredo para um bom atendimento via *e-mail*. Possuir uma estrutura adequada como um *Call Center* bem equipado e uma política de privacidade, entre outras qualidades, permite que se mantenha de forma coerente os serviços disponibilizados aos clientes, nunca deixando uma solicitação sem resposta. Confirmações automáticas do recebimento de mensagens são bons

sinais, demonstram organização e preocupação com o cliente, no entanto, de nada adiantam e ainda pioram as coisas quando um contato definitivo demora. Por se tratar de um recurso popular da Internet, o *e-mail* pode levar as empresas do céu ao inferno se não forem devidamente gerenciados como um recurso estratégico. Para exemplificar essa situação, pode-se tomar como base uma experiência feita durante a realização desse trabalho utilizando a opção *fale conosco* ou equivalente de cinco sítios, para os quais foi mandada uma mesma mensagem (solicitando informações da empresa). Os resultados, após sete dias, foram os seguintes:

- 2 enviaram respostas automáticas no mesmo dia, porém, nos dias seguintes nenhum contato foi feito;
- 2 responderam no dia seguinte. Uma delas inclusive com o convite para que eu conhecesse as instalações da empresa. A outra informou um link no qual, não encontrei as informações desejadas;
- 1 simplesmente não respondeu.

É preciso muito mais que isso para que as empresas encantem seus clientes. Disponibilizar serviços e não mantê-los de forma eficaz, pode comprometer seriamente a imagem e a credibilidade. Ciancio [CAR 01] cita alguns segredos para um bom relacionamento com os clientes através de mensagens eletrônicas:

- Quando a empresa for responder um *e-mail*, é fundamental a personificação da resposta. O usuário deve ser tratado pelo nome e a mensagem deve ser assinada por um funcionário, com identificação de cargo. Isso quer dizer que o aspecto humano é primordial, mesmo com toda tecnologia que possa ser empregada;
- O serviço de *fale conosco* deve estar muito bem sinalizado dentro do sítio, para facilitar a vida do internauta;
- A empresa deve ter a consciência de que o tempo de resposta de um *e-mail* agrega valor ao produto - quanto mais rápida a resposta, mais ficará evidenciado que a empresa se preocupa com o cliente;

- O relacionamento deve evoluir aos poucos. Muitos sítios pedem, logo no primeiro contato, dados como telefone, endereço, CPF e muito mais. A pergunta é: Será que o cliente preenche um cadastro desses logo na primeira visita ao sítio?
- Uma personalização do atendimento pode ser feita pela identificação do cliente com o pedido do seu nome e senha. Dessa forma, pode-se garantir um atendimento diferenciado e mais agradável para o cliente. Este recurso é especialmente empregado nos casos em que a empresa disponibiliza informações de interesse apenas de sua clientela como notícias de novas versões de produtos, seção de *download* para se obter manuais e outros arquivos, listas de discussão, etc...

Sistemas autônomos para atendimento com bancos de dados organizados de forma a permitir que usuários e clientes sanem suas dúvidas, podem ser uma boa receita de sucesso. Os FAQs (frequently asked questions) ou Perguntas e Respostas Frequentes, podem ser uma alternativa bastante simples para esse gênero de atendimento. É desejável que essas listas de perguntas e respostas possam ser incrementadas inclusive com a interação do próprio cliente. Com um sistema como esse, pode-se evitar o acúmulo de mensagens recebidas e o risco de nem sequer serem lidas.

Entretanto, quando o cliente não conseguir sanar suas dúvidas e/ou problemas através do FAQ, é importante que haja um canal direto e eficaz com a empresa, onde qualquer profissional que receba o chamado, possa resolvê-lo rapidamente.

Ainda que tudo isso funcione de forma adequada, uma outra questão, pertinente a essa modalidade de atendimento vem à tona: a segurança. Tanto a empresa quanto o cliente desejam que tudo ocorra conforme o esperado, porém o sistema de atendimento deve se precaver com algumas situações que podem ocorrer. Algumas perguntas ficam no ar, quando procuramos analisar o atendimento automático sob esse aspecto:

1. Como saber se o cliente é realmente quem diz ser?

2. Como saber se a empresa fornecedora dos produtos e/ou serviços é realmente quem diz ser?
3. Como garantir que uma reclamação ou uma solicitação de um cliente seja atendida nos prazos estipulados pela lei ou por contrato entre ambos?
4. Como garantir que, tendo um trocado mensagens com o outro, nenhum dos dois possa negar?
5. Como garantir o sigilo e a integridade das informações trocadas entre eles?

Em resumo, como garantir que os direitos do cliente e da empresa em suas transações sejam assegurados?

2.3.7 Comunidades Virtuais

Um outro método bastante interessante e revolucionário no atendimento ao cliente pela Internet, são as comunidades virtuais. Um determinado sítio na Web, promove o encontro entre clientes e empresas fornecedoras de produtos e/ou serviços a fim de trocarem informações técnicas, comerciais e de utilização.

Em [dR 00], observa-se que uma comunidade virtual, possui características que a diferenciam de um sítio comum, destacando-se a intensa comunicação dos seus participantes, o que aumenta consideravelmente o poder na relação estabelecida entre cliente-fornecedor. São apresentados também, cinco elementos para a definição do modelo comercial de uma comunidade virtual:

- Foco diferenciado permitindo aos membros participantes entender que tipo de recursos poderão encontrar ali e também aos organizadores, o espectro de recursos necessários para atender as necessidades dos participantes;
- Capacidade de integrar conteúdo através de um rico ambiente de comunicações;
- Avaliação do conteúdo gerado pelos membros por meio de ambientes utilizados para a geração e disseminação de conteúdos;

- Acesso a editores e fornecedores concorrentes;
- Orientação comercial objetivando maior retorno financeiro, fornecendo aos membros recursos valiosos e ambientes através dos quais, poderão aumentar o seu próprio poder.

Rolt [dR 00] destaca ainda, a necessidade de existir um organizador que atue em favor da comunidade virtual a fim de proporcionar aos membros os recursos relevantes para eles e ainda, agregar os perfis de dados de utilização da rede e os tipos de transações realizadas.

2.4 Conclusão

Não dá para se negar que o perfil dos clientes vêm mudando muito nos últimos anos e que eles tem se tornado cada vez mais exigentes com a globalização. Tornar esses clientes fiéis à empresa, através de mecanismos que garantam a qualidade no atendimento, pode ser fator vital para os negócios de agora em diante.

Prestar esse tipo de serviço pela Internet, requer mecanismos que garantam a segurança sob diversos aspectos, para que se possa resguardar os direitos, tanto da empresa fornecedora quanto do cliente.

No capítulo 4, esses mecanismos serão abordados com profundidade para que se entenda o problema de forma minuciosa e de como as tecnologias disponíveis combinadas, podem resolvê-lo.

As questões legais do atendimento ao cliente através de métodos eletrônicos devem também ser consideradas e para tanto, uma visão geral da legislação que aborda esse assunto é dada no capítulo 3.

Capítulo 3

Legislação

3.1 Introdução

Neste capítulo, serão abordadas as questões legais sobre os direitos do consumidor em transações comerciais convencionais e eletrônicas. Por se tratar de uma questão recente, o direito comercial eletrônico ainda dá os primeiros passos no Brasil, tentando adequar as leis que antes não previam o comércio digital, a uma nova realidade. Embora não trate especificamente dos direitos do consumidor em transações de comércio eletrônico, o código de defesa do consumidor dá margens a outras formas de comércio e transações que não são citadas na própria legislação. Isso pode ser reforçado pelo fato de que o consumidor é considerado como a parte mais vulnerável do processo perante a lei. A seção 3.2, destaca o código de defesa do consumidor e caracteriza os elementos participantes de uma transação comercial. A questão dos contratos, desistência e reclamações do consumidor, são abordadas na seção 3.3. Na seção 3.4, é destacada a admissão de provas eletrônicas em processos.

3.2 O Código de Defesa do Consumidor

Muito embora as empresas estejam se empenhando cada vez mais em satisfazer seus clientes, o Código de Defesa do Consumidor foi instituído para proteger o consumidor que,

pelo ponto de vista da lei, é o mais vulnerável de todo o processo. Reconhecendo essa vulnerabilidade, estabeleceu-se normas para garantias, durabilidade, segurança e qualidade dos produtos e serviços comercializados de modo a proteger efetivamente o consumidor ou cliente. Segundo o Código de Defesa do Consumidor, Lei nr. 8.078 de 11 de Setembro de 1.990, temos as seguintes definições:

- **Consumidor** é toda pessoa física ou jurídica que adquire ou utiliza produtos ou serviços como destinatário final;
- **Fornecedor** é toda pessoa física ou jurídica, pública ou privada, nacional ou estrangeira, bem como os entes despersonalizados, que desenvolvem atividades de produção, montagem, criação, construção, transformação, importação, exportação, distribuição ou comercialização de produtos ou prestação de serviços;
- **Produto** é qualquer bem, móvel ou imóvel, material ou imaterial;
- **Serviço** é qualquer atividade fornecida no mercado de consumo, mediante remuneração, inclusive as de natureza bancária, financeira, de crédito e securitária, salvo as decorrentes das relações de caráter trabalhista.

3.3 Direitos do Consumidor

O código de defesa do consumidor foi criado com o objetivo tornar as relações comerciais entre as empresas e seus clientes transparentes. O princípio básico do código, é assegurar os direitos do cliente, que é considerado economicamente mais fraco e exigir do fornecedor a prova de que não causou prejuízos de qualquer natureza em caso de litígio.

Dentre os principais direitos do consumidor, pertinentes ao tema deste trabalho e previstos na legislação brasileira, pode-se destacar os seguintes:

- O **Código de Defesa do Consumidor, de 11 de Setembro de 1990**, no seu artigo 4 prevê: *"A Política Nacional das Relações de Consumo tem por objetivo o atendimento das necessidades dos consumidores, o respeito à sua dignidade, saúde e*

segurança, a proteção de seus interesses econômicos, a melhoria da sua qualidade de vida, bem como a transparência e harmonia das relações de consumo..."

- A identificação deste artigo com o tema do trabalho proposto, acentua a necessidade de utilização de um artifício de controle das transações comerciais eletrônicas;

  Ainda no **Código de Defesa do Consumidor, de 11 de Setembro de 1.990**, artigo 49, consta: *"O consumidor pode desistir do contrato, no prazo de 7 (sete) dias a contar de sua assinatura, ou do ato de recebimento do produto ou serviço, sempre que a contratação de fornecimento de produtos e serviços ocorrer fora do estabelecimento comercial, especialmente por telefone ou a domicílio. Parágrafo único. Se o consumidor exercitar o direito de arrependimento previsto neste artigo, os valores eventualmente pagos, a qualquer título, durante o prazo de reflexão, serão devolvidos, de imediato, monetariamente atualizados."*

- Na modalidade de fornecimento fora do estabelecimento comercial, apesar de não estar explícito no artigo, o comércio eletrônico também se enquadra. O **Sistema Nacional de Defesa do Consumidor (SNDC), através do Decreto n 2.181 de 1997**, artigo 34, tem a seguinte redação: *"O consumidor poderá apresentar sua reclamação pessoalmente, ou por telegrama, carta, telex, fac-símile ou qualquer outro meio de comunicação, a qualquer dos órgãos oficiais de proteção e defesa do consumidor."*

  A citação no artigo acima de *"qualquer outro meio de comunicação"*, permite o cliente utilizar o correio eletrônico e até mesmo fazer o preenchimento de um formulário de reclamações no sítio de um órgão de defesa do consumidor.

3.4 Provas Eletrônicas

De acordo com o código de defesa do consumidor, em casos de litígio, cabe a empresa, considerada como a parte economicamente mais forte, apresentar as provas de que não causou prejuízos ao consumidor. Diante disso, a legislação trata

a questão das provas eletrônicas ou informáticas de forma generalizada, conforme pode ser interpretado pela citação do art. 5 inciso LVI da Constituição Federal Brasileira, que determina: *"São inadmissíveis, no processo, as provas obtidas por meios ilícitos."* O artigo 332 do Código de Processo Civil prevê que: *"Todos os meios legais, bem como os moralmente legítimos, ainda que não especificados nesse código, são hábeis para provar a verdade dos fatos, em que se funda a ação ou a defesa."* Segundo Paesani [PAE 99], de forma genérica, a lei não exclui a prova eletrônica, desde que esta seja lícita. Contudo, se faz necessária a materialização da prova, ora virtual, e com a identificação de sua origem. E finalmente, no caso de ausência de lei, cabe à jusrisprudência um papel importante para a resolução dessas questões.

No Brasil recentemente, através da medida provisória 2.200 de Agosto de 2.001 foi instituída a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, para garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica para a realização de transações de tal natureza.

3.5 Conclusão

Do ponto de vista do direito, não há justiça sem lei e sem lei não há crime.

O comércio eletrônico de uma maneira geral, vem com o seu crescimento anunciado já há muito tempo. Uma legislação clara, específica e abrangente se faz indispensável neste momento para a contenção de abusos eventualmente não previstos ou omitidos na legislação em vigor, por esta, não acompanhar o ritmo das transformações tecnológicas.

O recurso da jurisprudência avança lentamente na formação de dispositivos específicos a cada caso julgado, porém, uma legislação apropriada daria mais segurança a todas as entidades participantes de um processo eletrônico de comércio.

Capítulo 4

Tecnologia da Segurança em Computação

4.1 Introdução

No capítulo anterior, muitas foram as citações relacionadas à segurança dos dados que trafegam nas redes de computadores no mundo todo. Essa segurança deve ser garantida nas transações realizadas entre empresas e seus clientes. São diversos os aspectos que devem ser analisados como ameaças para a segurança, daí, a necessidade de entendermos as tecnologias da segurança em computação.

No início de sua existência, as redes de computadores foram basicamente utilizadas em universidades para a troca de mensagens de correio eletrônico e também, por funcionários de empresas, para o compartilhamento de impressoras. Diante de um cenário como esse, a preocupação com segurança, não necessitou de maiores cuidados. Atualmente, porém, com as inúmeras aplicações voltadas as operações bancárias e de comércio eletrônico, a necessidade de segurança é indiscutível [TAN 97]. A segurança segundo Soares [SOA 95], está relacionada à necessidade de proteção contra o acesso ou manipulação, intencional ou não, de informações confidenciais por elementos não autorizados.

Este capítulo aborda a problemática da quebra da segurança através de ameaças constantes aos sistemas e a proposta de algumas tecnologias para resolvê-la. A seção 4.2 destaca e caracteriza as ameaças e ataques aos quais os ambientes eletrônicos estão sujeitos. Os requisitos de segurança para um sistema eletrônico de dados são estudados na seção 4.3. As tecnologias de criptografia e a infra-estrutura de chave pública são respectivamente apresentadas nas seções 4.4 e 4.5. As características das assinaturas digitais são abordadas na seção 4.6. Concluindo o capítulo, são analisados alguns protocolos criptográficos na seção 4.7.

4.2 Ameaças e Ataques

Diversas são as ameaças na segurança onde sistemas de informação ou redes de computadores podem estar expostos. Segundo Stallings [STA 99], essas ameaças podem ser caracterizadas da seguinte forma:

- **Interrupção**: O fluxo da mensagem é interrompido com o corte da linha de comunicação entre a fonte e o destino da mensagem, por exemplo, ou com a destruição de uma peça do *hardware*, como o *winchester*. Este é um ataque de disponibilidade;
- **Interceptação**: Uma pessoa, programa ou computador tem acesso não autorizado à rede fazendo cópia ilegal de dados ou arquivos. Este é um ataque de confidencialidade;
- **Modificação**: Uma pessoa, programa ou computador tem acesso não autorizado à rede fazendo modificações em arquivos, mensagens ou em programas, de modo a se comportarem diferentemente. Este é um ataque de integridade;
- **Fabricação**: Uma pessoa, programa ou computador tem acesso não autorizado à rede inserindo objetos no sistema para que os mesmos gerem novas informações como mensagens na rede ou adição de registros em um arquivo. Este é um ataque de autenticidade.

A figura 4.1 detalha cada um dos tipos de ameaças à segurança de um sistema.

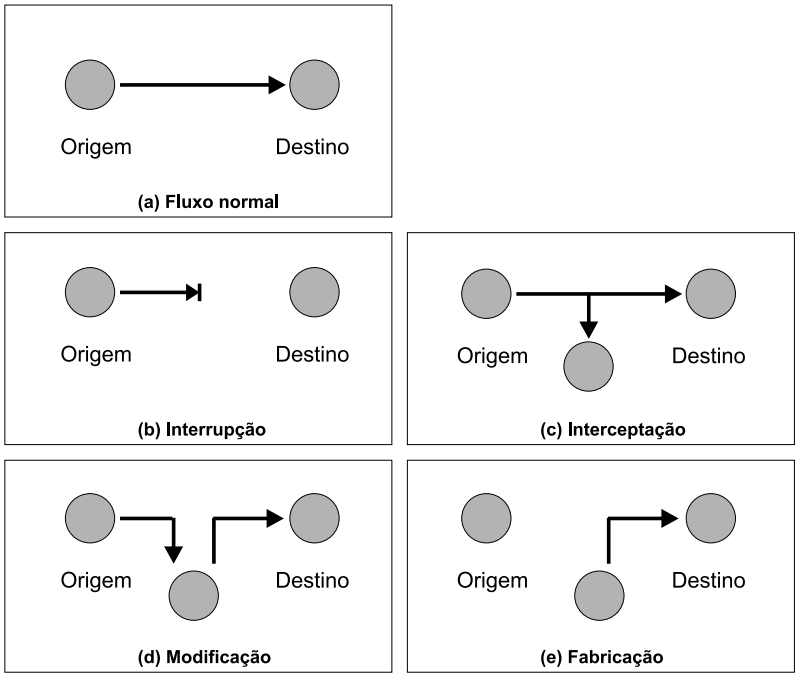

Figura 4.1: Tipos de ameaça. Idealmente, em uma comunicação, o que se espera é que haja um fluxo normal (a), porém, diversos tipos de ataques podem ocorrer. O ataque por interrupção (b), bloqueia o envio de mensagens para um destinatário. A interceptação (c), faz com que mensagens trocadas sejam armazenadas para uso futuro. Um oponente pode se passar pela fonte de uma mensagem interceptada, modificando e retransmitindo a mesma para o destinatário (d). O ataque por fabricação (e), consiste na geração de mensagens para um destinatário por um intruso, como se fosse de um remetente válido.

Os ataques, que são as materializações das ameaças, ocorrendo, podem ser caracterizados de dois tipos: os passivos e os ativos. Ataques passivos, são aqueles que, quando ocorrem não geram nenhuma modificação nas informações contidas nos sistemas, em sua operação ou estado [SOA 95]. A leitura do conteúdo de mensagens e a análise do tráfego das mensagens são dois tipos de ataque passivo. O primeiro deles objetiva bisbilhotar as mensagens trocadas entre fonte e destino. No segundo caso, se as mensagens estiverem protegidas com o uso de criptografia, o oponente pode ainda determinar a localização dos elementos da comunicação e observar a freqüência e tamanho das mensagens trocadas entre fonte e destino. Ataques passivos são muito difíceis de se detectar, pois, não envolvem nenhuma alteração de dados, entretanto, é possível se prevenir contra eles. Os ataques ativos podem ge-

rar alterações nos dados ou criar dados falsos em uma troca de mensagens, sendo divididos em quatro categorias [STA 99]:

- **Personificação**: Uma entidade, com um nível de privilégio menor, se faz passar por outra, para obter algum benefício extra;
- **Repetição**: Uma mensagem, ou parte dela, é capturada de uma comunicação entre duas entidades e retransmitida para a entidade destino, gerando com isso, um efeito não autorizado. Uma mensagem contendo uma transação financeira, por exemplo, entre duas entidades, pode ser interceptada e enviada diversas vezes por um oponente para o destino, caracterizando assim um ataque por repetição;
- **Modificação**: O conteúdo de uma mensagem é interceptado, alterado e retransmitido para a entidade de destino causando um efeito não autorizado;
- **Recusa ou negação de serviço**: Uma entidade oponente, pode gerar uma rajada de mensagens com a intenção de prejudicar o funcionamento de uma entidade destino. A sobrecarga nesta entidade, faz com que a mesma não execute as suas funções apropriadamente e ainda impeça outras entidades de fazê-las.

4.3 Requisitos de Segurança

Diante do exposto acima, podemos então identificar claramente as características desejáveis dos sistemas ditos seguros e dos protocolos criptográficos, que são:

- **Confidencialidade**: Propriedade que garante aos participantes da comunicação que somente eles possam ter conhecimento do conteúdo das informações e mensagens trocadas;
- **Integridade**: Propriedade que assegura aos participantes da comunicação que a mensagem enviada por um será transmitida de forma fiel para o outro;

- **Autenticação**: Propriedade que garante a identificação dos elementos participantes da comunicação;
- **Não recusa**: Propriedade que imputa a autoria das mensagens ou transações eletrônicas, garantindo que o emissor não negue a mesma posteriormente.

Sabe-se que para alcançar tais características, muitas vezes, deve-se recorrer aos protocolos criptográficos. Os métodos criptográficos por si só não são sempre suficientes para garantir a segurança de um sistema. O protocolo é a forma, mesmo que simples, de se usar os algoritmos criptográficos para obter uma solução segura [CAR 00].

A seguir, serão descritos alguns protocolos criptográficos básicos que integrarão a proposição do protocolo criptográfico, objeto deste trabalho, proposto no capítulo 5.

4.4 Criptografia

Imaginemos a seguinte situação: Duas entidades (A e B), desejam trocar informações de maneira segura. Para isso vamos aplicar dois protocolos criptográficos conhecidos, um com o uso de criptografia simétrica que emprega apenas uma chave secreta entre os participantes e o outro usando a criptografia assimétrica com duas chaves, uma para cifrar e a outra para decifrar. Tanto um quanto o outro deverão atender aos requisitos básicos para uma comunicação segura conforme mencionado acima. Vejamos as características de cada um.

4.4.1 Criptografia Simétrica

Os protocolos que utilizam criptografia simétrica são de fácil entendimento e consistem basicamente no compartilhamento de uma chave secreta (K) entre as entidades envolvidas na comunicação, para cifrar e decifrar as mensagens. A figura

4.2 mostra o esquema da troca de mensagens entre duas entidades que previamente definiram uma chave secreta para o uso do algoritmo criptográfico.

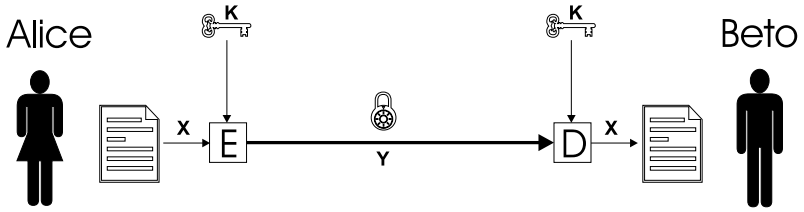

Figura 4.2: Protocolo Criptográfico Simétrico. Protocolo utilizando criptografia simétrica para a troca de mensagens entre duas entidades (Alice e Beto). Utiliza um algoritmo criptográfico para cifrar a mensagem com uma chave, a qual, também é utilizada para decifrar. É simples e robusto, no entanto, a troca das chaves de forma segura entre os participantes é um problema.

De acordo com a figura 4.2, os passos para a troca da mensagem entre a entidade A (Alice) e a entidade B (Beto) são os seguintes:

1. Alice, de posse do texto aberto (X) que deseja enviar para Beto, utiliza um algoritmo de criptografia para cifrar a mensagem com a chave secreta (K) que foi definida e compartilhada com Beto. Sendo assim, pode-se obter o texto cifrado (Y) com:

   Y = E_K(X);

2. A mensagem cifrada (Y) é enviada pela rede para Beto;

3. Beto recebe o texto cifrado e, aplicando o mesmo algoritmo usado por Alice, decifra a mensagem com a chave secreta compartilhada:

   X = D_K(Y).

A utilização de protocolos criptográficos simétricos é muito bem aceita, pois, os algoritmos são mais rápidos que os de criptografia assimétrica. A desvantagem principal deste protocolo é a problemática da distribuição das chaves. A menos que Alice e Beto possam se encontrar pessoalmente para combinar a chave, este protocolo pode estar comprometido. A solução para este problema é a utilização da Infra-estrutura de Chaves Públicas (ICP) com criptografia assimétrica para a troca

de mensagens que será abordada na próxima seção. Historicamente, o foco principal da criptografia tem sido o uso de criptografia convencional para se prover a confidencialidade na troca de informações. Nas últimas décadas, novas considerações passaram a fazer parte da criptologia como a autenticação, integridade, assinaturas digitais e chaves públicas [STA 99]. Que a confidencialidade é uma das características mais desejáveis nos protocolos criptográficos, é indiscutível, porém, a inobservância das outras ameaças, poderá inviabilizar todo o sistema.

4.4.2 Criptografia Assimétrica

A criptografia assimétrica é assim chamada por utilizar um par de chaves, sendo uma delas para cifrar e a outra para decifrar as mensagens. Cada entidade participante da comunicação, possui um par de chaves, uma pública e uma privada. A chave pública, conforme o próprio nome diz, é distribuída para todos e até em alguns casos, é enviada juntamente com a mensagem para que o receptor possa decifrá-la. Uma mensagem cifrada com uma chave privada, só poderá ser decifrada com o seu par, neste caso, a chave pública e vice-versa. Com isso, pode-se determinar a autenticidade das mensagens recebidas, visto que, se uma mensagem for criptografada com a chave privada de uma entidade, a mesma só poderá ser decifrada com seu par. Neste caso a chave pública.

A figura 4.3 mostra uma troca de mensagem com a utilização de criptografia assimétrica. Neste caso, a autenticação do emissor da mensagem é garantida, no entanto, qualquer pessoa pode ter acesso ao teor da mesma, pois a chave para se decifrar é pública. Os passos para a troca da mensagem entre Alice e Beto, são os seguintes:

1. Alice, de posse do texto aberto que deseja enviar para Beto, utiliza um algoritmo de criptografia assimétrica para cifrar a mensagem com a sua chave privada. Sendo X o texto aberto, Y o texto cifrado e KR_A a chave privada de Alice, temos:

Y = E_{KR_A}[X];

2. A mensagem cifrada é enviada para Beto. Conforme já foi observado anteriormente, este protocolo não garante a confidencialidade das informações, pois, qualquer entidade que obtenha a mensagem cifrada, pode chegar ao texto aberto facilmente com o uso da chave pública de Alice (KU_A);

3. Beto recebe o texto cifrado e, aplicando o mesmo algoritmo usado por Alice, decifra a mensagem com a chave pública (KU_A), onde temos:

   X = D_{KU_A}[Y].

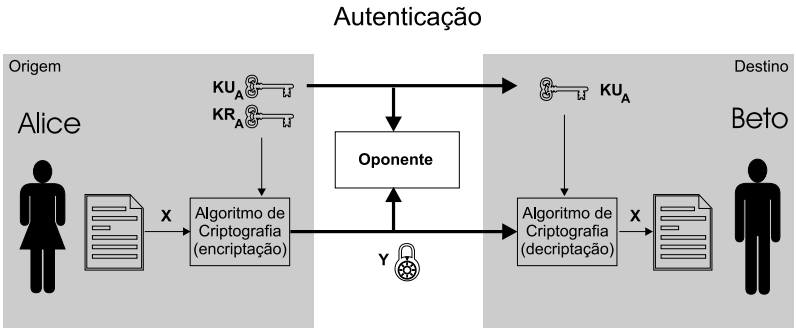

Figura 4.3: Protocolo Criptográfico Assimétrico - Autenticação. Buscando a identificação do remetente de uma mensagem, pode-se utilizar este protocolo de criptografia assimétrica, onde, uma chave é usada para cifrar os dados e a outra para decifrar (pública e privada). Conforme ilustrado na figura acima, pode-se observar que Alice, utilizando um algoritmo de criptografia assimétrica, cifra a mensagem que deseja enviar para Beto com a sua chave privada (KR - Key pRivate). Sendo utilizado um algoritmo assimétrico e a chave pública de Alice (KU - Key pUblic) conhecida por Beto, ele pode, a qualquer momento obter a mensagem plana. Isso caracteriza uma assinatura de Alice na mensagem, pois, somente ela, com sua chave privada, poderia produzir uma mensagem cifrada que pudesse ser decifrada por Beto com a sua chave pública. Isso garante aos participantes do protocolo, a autenticidade da mensagem, mas, não a confidencialidade, já que a chave para se decifrar a mensagem enviada por Alice é pública.

Na figura 4.4, o problema de confidencialidade é resolvido com uma dupla cifração. O destinatário da mensagem recebe, primeiro cifra com a chave privada do emissor para comprovar a fonte e segundo com a sua chave pública, para garantir que somente ele a decifre. Nesta figura temos:

1. Alice, de posse do texto aberto que deseja enviar para Beto, utiliza um al-

goritmo de criptografia assimétrica para cifrar a mensagem com a sua chave privada. Sendo X o texto aberto, Y o texto cifrado e KR_A a chave privada de Alice, temos:

Y = E_{KR_A}[X];

2. A mensagem resultante do passo anterior (Y) é novamente criptografada, desta vez, com a chave pública de Beto (KU_B) para se assegurar que somente ele possa abri-la com a sua chave privada (KR_B):

   Z = E_{KU_B}[Y];

3. A mensagem (Z), duplamente cifrada, é então enviada pela rede para Beto;

4. Beto recebe o texto cifrado e, aplicando o mesmo algoritmo usado por Alice, decifra a mensagem, primeiramente com a sua chave privada para obter (Y) e depois com a chave pública de Alice para obter o texto aberto. Sendo assim, temos:

   X = $D_{KR_B}[D_{KU_A}$[Z]].

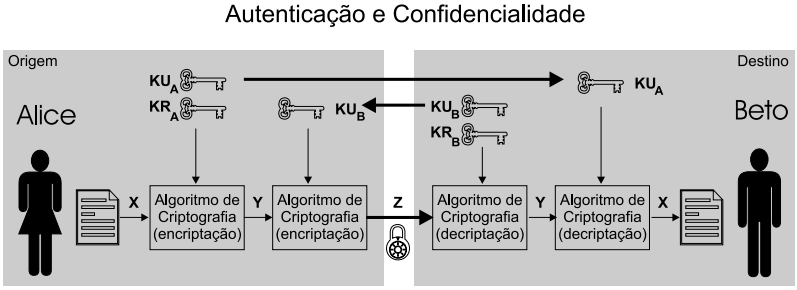

Figura 4.4: Protocolo Criptográfico Assimétrico - Autenticação e Confidencialidade. Com a utilização da infra-estrutura de chave pública, Alice e Beto possuem um par de chaves, os quais, através da utilização de um algoritmo de criptografia assimétrica com uma dupla cifração, podem garantir autenticidade e confidencialidade aos participantes da transação. Primeiramente, Alice assina a mensagem cifrando-a com a sua chave privada (KR_A). Em seguida, repete-se o processo, porém agora, com a chave pública de Beto (KU_B). Quando Beto receber a mensagem de Alice, ele executa o processo de maneira inversa para chegar até o texto aberto. A autenticação neste protocolo, se deu pela assinatura de Alice e a confidencialidade com o uso da chave pública de Beto. Somente Alice poderia ter a chave privada para cifrar e somente Beto poderia ter a chave privada para decifrar.

Este protocolo é bastante conhecido e utilizado para a resolução do problema de

troca de chaves dos algoritmos de criptografia simétrica. Observando novamente o protocolo ilustrado na Figura 4.4, podemos imaginar que a mensagem trocada entre Alice e Beto contém a escolha de um algoritmo simétrico e uma chave para que os dois a utilizem. Desta forma, maximiza-se a velocidade na troca de mensagens, pois, pode-se utilizar a criptografia assimétrica, que é mais lenta, apenas para a troca de chaves simétricas. Com isso, pode-se usar as chamadas chaves de seção. Estas são chaves simétricas que só serão usadas em uma seção de comunicação, sendo posteriormente descartadas. Diante disso, as chaves de seção aumentam a segurança, pois são efêmeras, existindo apenas durante aquela seção de comunicação. Mesmo que um oponente consiga obter uma das chaves, ele só conseguirá ler as mensagens trocadas durante a seção em que a chave descoberta foi usada.

Este protocolo, entretanto, pode ser alvo de ataque ativo, onde um oponente pode se fazer passar por Alice ou Beto, interceptando e retransmitindo as mensagens de um para o outro até descobrir a chave de seção. Isso pode ocorrer, pois Alice não possui meios para verificar a autenticidade da chave pública de Beto e vice-versa. Alguém, se passando por Beto e também por Alice, pode distribuir uma chave pública para interceptar as mensagens trocadas entre os dois futuramente. No entanto, um oponente pode atacar esse protocolo com sucesso somente se Alice e Beto não conhecerem com antecedência as chaves públicas um do outro [CAR 00]. O ataque descrito acima, pode ser facilmente compreendido na análise da Figura 4.5.

Para se resolver este problema, deve-se adotar uma terceira entidade que conheça as chaves públicas de Alice e Beto e possa garantir sua autenticidade. As autoridades de chave pública e certificadoras, como são chamadas, devem ser reconhecidas como seguras e aceitas por todos os participantes do protocolo. Na seção 4.5 será abordada a troca de chaves através da infra-estrutura de chaves públicas.

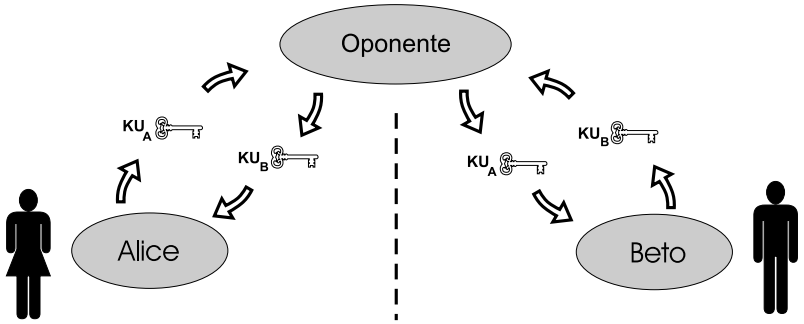

Figura 4.5: Ataque ao Protocolo para troca de chaves públicas. Um oponente, interceptando a comunicação entre duas entidades, pode se passar por uma e por outra, distribuindo chaves públicas falsas de cada uma de forma que ele possa decifrar qualquer mensagem trocada entre elas.

4.5 Infra-estrutura de Chaves Públicas - ICP

Uma alternativa bastante eficiente para a resolução do problema de distribuição de chaves públicas de forma segura, é a inclusão de uma terceira entidade no protocolo mostrado acima, na qual, Alice e Beto confiam. Essa entidade, pode ser abordada de duas formas: sendo a primeira, a de uma autoridade de chave pública, que detém em um banco de dados todas as chaves para a distribuição confiável e a outra para a emissão de certificados digitais que garantem a autenticidade da chave pública de uma entidade para outra. Na primeira abordagem, a autoridade de chave pública, consiste em um banco de dados que contém a chave pública de todos os participantes dos processos de comunicação. Cada participante conhece a chave pública da autoridade, que por sua vez, somente ela conhece a chave privada correspondente [STA 99]. Assim, se alguém tentar se passar por ela, não obterá sucesso. A Figura 4.6 mostra a comunicação entre Alice e Beto com as garantias de distribuição de chaves da autoridade de chave pública. Nesta figura, temos os seguintes passos:

1. Alice envia uma mensagem para a autoridade de chave pública com a requisição da chave pública de Beto e uma marcação de tempo:

   $Req||Tempo_1$

2. A autoridade responde para Alice, cifrando com a sua chave privada, a chave pública de Beto e a requisição recebida. Com isso, Alice pode ter certeza de

que a mensagem veio da autoridade certificadora, podendo decifrá-la usando a chave pública da mesma. O conteúdo da resposta enviada para Alice é o seguinte:

$E_{KRaut}[KUb||Req||Tempo_1]$

A devolução da requisição original pela autoridade para Alice, permite a ela determinar que a mesma não foi alterada e no caso da marcação de tempo, assegura-se que a chave pública de Beto é aquela e não uma mais antiga;

3. Alice, de posse da chave pública de Beto, usa-a para cifrar uma mensagem para ele com a sua identificação e um número aleatório para a identificação dessa transação entre os dois:

   $E_{KUb}[ID_A||N_1]$

4. Beto, recebendo a mensagem, procede da mesma maneira com a autoridade de chave pública para obter a chave pública de Alice:

   $Req||Tempo_2$

5. Da mesma maneira, a autoridade responde para Beto, cifrando com a sua chave privada, a chave pública de Alice e a requisição recebida:

   $E_{KRaut}[KUa||Req||Tempo_2]$

6. Para provar que Beto recebeu a mensagem de Alice, ele responde cifrando com a chave pública dela, o número aleatório recebido (que somente ele poderia tomar conhecimento), concatenado com um outro gerado por ele:

   $E_{KUa}[N_1||N_2]$

7. Por sua vez, Alice devolve o número aleatório gerado por Beto, cifrado com a chave pública dele para comprovar o recebimento da mensagem:

   $E_{KUb}[N_2]$

Nesse protocolo, pode-se observar que para o estabelecimento da comunicação entre um usuário e outro, a autoridade de chave pública é consultada. Isso pode gerar um certo congestionamento no sistema [STA 99].

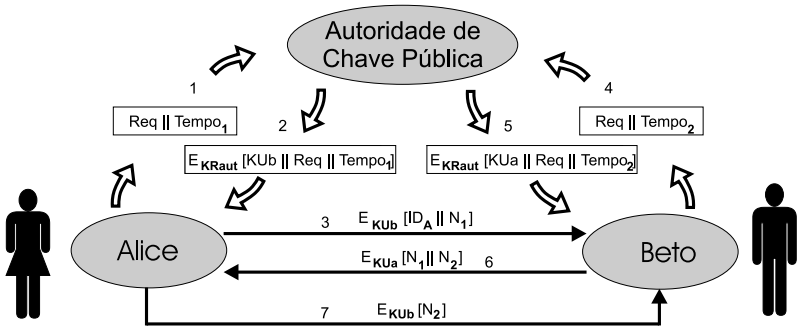

Figura 4.6: Protocolo para distribuição de chaves públicas através de uma Autoridade de Chave Pública. O emprego de uma autoridade de chave pública - ACP, torna a distribuição de chaves mais confiável. As entidades envolvidas na comunicação podem solicitar as chaves públicas de seus destinatários para a ACP que responde, enviando uma mensagem contendo a chave pública solicitada, assinada digitalmente. Uma associação de tempo é feita para essas requisições, para se evitar a distribuição de chaves públicas de certificados já revogados. Após o recebimento da chave pública de Beto, Alice troca uma mensagem com ele para fazer a verificação de autenticidade da mesma. A identificação de Alice e um número randômico é gerado para a composição desta mensagem. Se a chave pública de Beto, que Alice obteve pela ACP, estiver correta, somente Beto poderá decifrar a mensagem recebida. Sendo assim, ele gera outro número randômico e manda-o juntamente com o que recebeu para Alice. Esta última mensagem, permitirá verificar a autenticidade da chave pública de Alice. Se a chave pública de Alice, obtida por Beto através da autoridade de chave pública for correta, somente Alice poderá decifrar a mensagem recebida de Beto. Sendo assim, Alice responde para Beto, enviando-lhe o número randômico recebido dele para comprovar a autenticidade de sua chave pública. Um ponto de falha neste protocolo, pode ser a segurança da própria autoridade certificadora e o comprometimento da sua chave privada.

Uma outra abordagem para a distribuição de chaves públicas é o uso de um certificado digital emitido por uma AC. Nesse caso, a entidade que desejar um certificado digital deve gerar um par de chaves e enviar a chave pública para a autoridade certificadora que a devolve, cifrando com a sua chave privada, uma marca de tempo, a identificação da entidade e a sua chave pública. Sendo a autoridade certificadora reconhecida pelas entidades participantes da comunicação e tendo cifrado o certificado emitido com a sua chave privada, o certificado é confiável e passa a ser aceito por todos. A Figura 4.7 mostra a emissão e a troca de certificados digitais entre Alice e Beto.

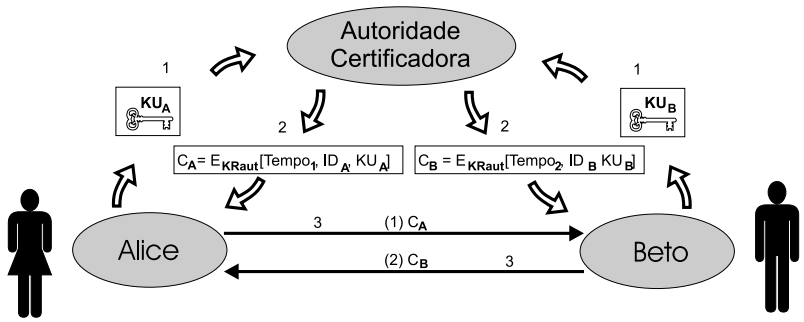

Figura 4.7: Protocolo para emissão e distribuição de certificados digitais. Uma entidade, para garantir a autenticidade e resolver os problemas com a distribuição de sua chave pública, pode requisitar a uma autoridade certificadora, um certificado digital. Após gerar um par de chaves, a entidade envia a sua chave pública para a autoridade certificadora solicitando um certificado. A AC, que é confiável e aceita por todos os participantes do protocolo, gera o certificado digital, cifrando a sua chave privada, a identificação, a chave pública do requisitante e a validade do certificado emitido. De posse desta mensagem recebida da AC, o requisitante poderá distribuir tranqüilamente a sua chave pública que está cifrada no certificado e que poderá ser facilmente verificada utilizando-se a chave pública da AC.

Descrevendo então os passos mostrados na Figura 4.7 temos:

1. Alice e Beto submetem as suas chaves públicas para a autoridade certificadora (KU_a e KU_b);
2. A autoridade certificadora, emite o certificado digital para eles, cifrando com a sua chave privada, uma marcação de tempo, a identificação e a chave pública de cada um:

   $C_A = E_{KRaut}[Tempo_1, ID_A, KU_A]$ para Alice e

$C_B = E_{KRaut}[Tempo_2, ID_B, KU_B]$ para Beto;

3. Alice envia o seu certificado digital para Beto;
4. Beto envia o seu certificado digital para Alice.

Como o certificado digital é cifrado com a chave privada da autoridade certificadora, o mesmo só poderá ser decifrado com a sua chave pública correspondente, o que comprova a sua autenticidade. A marcação de tempo no certificado digital emitido, determina a validade do mesmo. Supondo-se que a chave privada de um usuário esteja comprometida, ele pode gerar um outro par de chaves para a emissão de um novo certificado, sendo o atual revogado. Enquanto isso, um oponente pode ler o conteúdo das mensagens interceptadas [STA 99]. Este cenário é semelhante ao da perda de um cartão de crédito onde, mesmo tendo sido cancelado, ele pode ainda ser aceito por alguns estabelecimentos.

4.6 Assinatura Digital

A infra-estrutura de chaves públicas, conforme foi abordada na seção anterior, permite a concepção das assinaturas digitais. Uma assinatura digital tem basicamente os mesmos propósitos de uma assinatura em papel, entretanto, considerando o meio eletrônico de transmissão de documentos assinados, deve-se empregar técnicas para garantir a integridade e autenticidade de tais documentos.

O protocolo da assinatura digital emprega o certificado digital da entidade que está assinando o documento e uma função de resumo da mensagem permite que durante a verificação da assinatura, tenha-se também a certeza da integridade do documento. A figura 4.8 ilustra esse protocolo que garante aos participantes autenticação e integridade. Alice gera um resumo (*hash*) da mensagem a ser enviada e o cifra com a sua chave privada. A mensagem aberta é então concatenada com o resumo e ambos são enviados para Beto que ao receber a mensagem, verifica a assinatura de Alice decifrando o resumo com a chave pública dela. O resumo recebido é decifra-

do e comparado com outro que Beto gera a partir da mensagem aberta que recebeu. Se os dois forem iguais, então a mensagem não foi alterada durante o envio o que garante a sua integridade.

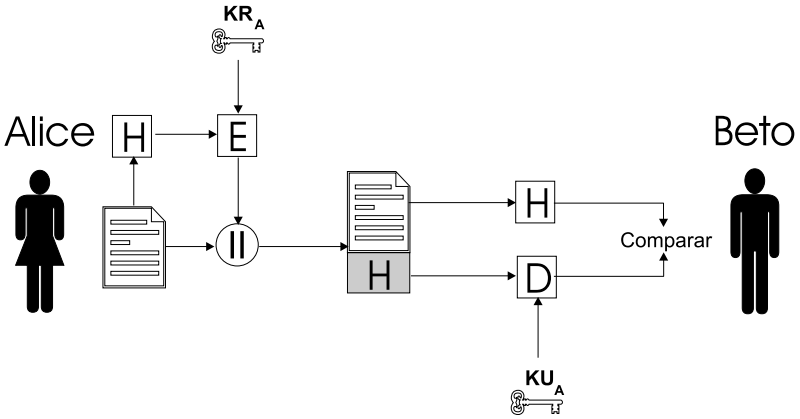

Figura 4.8: Protocolo de assinatura digital. Assinatura digital de Alice garantindo a autenticidade da mensagem para Beto e permitindo a verificação da integridade através do resumo.

O RSA (Rivest, Shamir e Adleman) e o DSS (Digital Signature Standard) são exemplos de algoritmos para assinaturas digitais e são abordados em detalhes em [STA 99].

4.6.1 Funções de Resumo

Uma função de resumo quando aplicada a uma mensagem deve gerar um resultado criptografado e de tamanho fixo. Empregando-se uma função de resumo em uma comunicação, pode-se garantir que o conteúdo de uma mensagem não foi alterado durante a sua transmissão. O remetente da mensagem gera o resumo, obtendo como resultado da função um bloco de bytes sempre de tamanho fixo. O destinatário, ao receber a mensagem juntamente com o resumo, poderá verificar a sua integridade gerando outro resumo sobre a mensagem recebida e comparando com o resumo recebido. Se os dois resumos forem iguais, então a mensagem recebida não sofreu nenhuma alteração durante a sua transmissão. A seguir são relacionadas as características desejadas das funções de resumo:

- A função deverá permitir ser aplicada a mensagens de qualquer tamanho;

- A função sempre deverá produzir uma saída de tamanho fixo, independente do tamanho da mensagem a ser resumida;
- Deverá também ser de fácil implementação tanto em *hardware* como em *software*;
- Não permitir a operação reversa, isto é, que através de um resumo obtido que chegue a mensagem completa novamente;
- Não permitir que duas mensagens diferentes levem ao mesmo resumo calculado.

Uma outra aplicação para as funções de resumo seria por exemplo, garantir a integridade das informações obtidas através de um *download*. Um arquivo é baixado pela Internet com o seu respectivo resumo concatenado. Após isso, calcula-se o resumo da mensagem original e compara-se com o recebido. Se forem iguais, o *download* obteve sucesso e a integridade dos dados está garantida.

Os algoritmos MD5 (Message Digest 5) e SHA (Security Hash Algorithm) são exemplos de funções para cálculo de resumo de mensagens e podem ser encontrados em detalhes em [STA 99].

4.7 Protocolos Criptográficos

O emprego da criptografia e o acordo entre as partes envolvidas na comunicação para a troca de informações, dá origem ao protocolo criptográfico, ou seja, uma forma específica de utilização dos métodos de cifragem dentro dos passos utilizados para transferir as mensagens. Um protocolo criptográfico é uma série de passos, envolvendo duas ou mais partes, projetadas para realizar uma tarefa. Os passos deverão ser executados, um de cada vez, e nenhum deles pode ser iniciado antes do anterior ter acabado [SCH 96]. Protocolos criptográficos são utilizados para estabelecer comunicação segura em redes abertas e sistemas distribuídos com o objetivo de proporcionar confidencialidade, autenticidade, integridade de dados e

não-repúdio, protegendo os objetivos do mesmo em um ambiente hostil [GRI 99]. O protocolo irá garantir a legitimidade da comunicação. A seguir, serão abordados dois protocolos criptográficos conhecidos, para que se possa futuramente entender os aspectos de especificação e análise.

4.7.1 Autoridade de Aviso

Considerando-se que num sistema de atendimento ao cliente disponível através da Internet poderão ocorrer problemas de comunicação e indisponibilidade de serviços, e que também, eventualmente um participante, esteja interessado na interrupção dessa comunicação, elege-se para isso, uma autoridade de aviso.

A autoridade de aviso (AA) é uma entidade participante de um protocolo que tem como objetivo principal garantir a comunicação e o não recusa 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.

Maiores informações sobre o funcionamento das Autoridades de Aviso poderão ser encontradas em [BRO 01].

4.7.2 Autoridade Certificadora

O papel da autoridade certificadora no protocolo proposto neste trabalho e também em muitos outros protocolos seguros, é o de emitir, manter e validar os certificados

e assinaturas digitais utilizados nas transações eletrônicas. Sabe-se que para assegurar os requisitos de segurança confiados aos certificados e assinaturas digitais, é necessário que a autoridade certificadora que os emitiu seja idônea e confiável. São elas que dão suporte a toda infra-estrutura de chave pública.

Tendo a chave privada de um certificado digital sido comprometida, o certificado poderá ser revogado à pedido do seu titular pela autoridade certificadora. Com isso um novo certificado poderá ser emitido a partir de um novo par de chaves. Paralelamente, uma lista de certificados revogados é divulgada periodicamente para informação de todos os usuários.

4.7.3 Autoridade de Datação

Como o objetivo principal do protocolo a ser proposto neste trabalho é a garantia da qualidade de serviço e ainda com segurança, o emprego de uma autoridade de datação se faz extremamente necessário. A função da autoridade de datação é de protocolar 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 Adams [ADA 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.

Adams [ADA 01] destaca entre outros, alguns requisitos que uma autoridade de datação deve satisfazer para ser considerada por seus usuários como segura e confiável:

- 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.

Maiores informações sobre o funcionamento das Autoridades de Datação poderão ser encontradas em [PAS 01].

4.7.4 Autoridades Fiscalizadoras

A autoridade fiscalizadora, como o próprio nome sugere, tem como objetivo principal garantir os direitos dos participantes do protocolo e ainda intervir, caso hajam situações de litígios entre qualquer uma das partes. A eleição de uma autoridade fiscalizadora, vai depender da aplicação e do ramo da empresa que emprega o protocolo seguro de atendimento aos clientes. Para algumas empresas, por conseqüência do seu ramo de atuação, existem órgãos civis e do governo que controlam as suas atividades, podendo assim, serem eleitos como autoridades fiscalizadoras naturais. Nesta situação enquadram-se a ANATEL (Agência Nacional de Telecomunicações) e a FEBRABAN (Federação Brasileira das Associações de Bancos). De uma forma mais universal, para praticamente todos os tipos de empresas, pode-se também eleger o IDEC (Instituto Brasileiro de Defesa do Consumidor), PROCON (Programa Estadual de Proteção e Orientação ao Consumidor) e até mesmo a justiça comum como autoridades fiscalizadoras a serem empregadas pelo protocolo.

Uma outra abordagem ainda para a autoridade fiscalizadora, é o emprego do próprio setor de garantia da qualidade da empresa, entretanto, deve-se considerar a potencial parcialidade no tratamento dos litígios com clientes.

4.7.5 Especificação e Análise de Protocolos

A especificação formal e a análise de protocolos criptográficos exercem um importante papel na avaliação de criptossistemas. Sendo assim, uma eficiente especificação e a análise do modelo do protocolo proposto é altamente recomendada para se garantir que o mesmo obtenha os resultados esperados. Assim sendo, a especificação e análise do protocolo, bem como os testes de segurança dos algoritmos criptográficos é de fundamental importância [LEE 97]. Os modelos de análise e especificação convencional para protocolos, podem ser classificados da seguinte forma:

Modelos Algébricos que modelam um protocolo com um conjunto de regras para transformar expressões algébricas em mensagens. Essa abordagem de análise de protocolos foi utilizada para uma classe restrita de protocolos [GRI 99]. Segundo Lee [LEE 97], este modelo garante apenas o sigilo de mensagens iniciais e aplica-se somente para protocolos do tipo ping-pong.

Modelos Lógicos formais conhecidos como lógica BAN propostos por Burrows, Abadi e Needham tem sido amplamente utilizados para a análise de protocolos de autenticação [GRI 99]. Lee [LEE 97] aponta algumas desvantagens da utilização desse modelo como a necessidade de especificação de cada parte do protocolo, não considerar estados de conhecimento e propriedades semânticas dos protocolos.

Lógicos e Algébricos onde enquadra-se o analisador de protocolos NRL que foi escrito em Prolog, podendo tanto ser utilizado para a verificação de propriedades de segurança de protocolos criptográficos como na detecção de quebras de segurança [GRI 99]. Entretanto, Lee [LEE 97] observa que esse modelo é incapaz de especificar importantes características de protocolos como paralelismo, assincronismo e não-determinismo, possui uma leitura fraca da especificação, por ser textual e a consistência entre a especificação e análise é pobre.

Modelos baseados em redes de Petri são altamente recomendados para a análise e especificação de protocolos por já terem sido empregados para a análise de modelos e na avaliação de importantes características como paralelismo, concorrência e assincronismo. Têm profunda base matemática e permitem a especificação gráfica de um protocolo, a qual proporciona a identificação de quebras de segurança do mesmo. Lee [LEE 97] propõe um novo modelo baseado em redes de Petri, o qual denomina CTPN (Cryptoghaphic Timed Petri Net) e apresenta também uma nova especificação e metodologia de análise para os protocolos baseados neste modelo. O modelo CTPN consiste em um analisador de protocolos (CTPN-analyzer), o qual interpreta uma linguagem de especificação textual (CTPN-language) e permite a verificação e validação de um sistema. O relacionamento entre a linguagem de especificação e o analisador é ilustrado na figura 4.9.

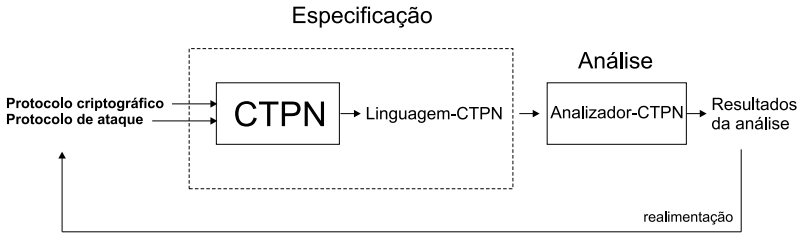

Figura 4.9: Metodologia CTPN. A fase de especificação do protocolo criptográfico é feita em uma linguagem própria dentro da metodologia CTPN e submetida ao analisador, que verifica os requisitos de segurança e outros aspectos do mesmo. Os resultados obtidos da análise, realimentam a especificação com o objetivo de tornar o protocolo mais robusto e seguro.

Gritzalis [GRI 99] destaca os princípios de robustez propostos por R. Anderson e R. Needham para a especificação e construção de protocolos:

- Ser muito claro sobre seus objetivos e suposições;
- Ter clareza sobre os objetivos da cifração. Não assumir que seu uso é sinônimo de segurança;
- Ter cuidado para que o protocolo não crie suposições não verificadas com relação às propriedade do algoritmo criptográfico empregado;

- Ter certeza de que os diferentes protocolos empregados comunicam-se entre si;
- Não assumir que uma mensagem recebida tenha sempre uma mesma forma, ainda que isso possa ser checado;
- No caso de uso de um carimbo de tempo (*timestamp*), usando a referência de tempo absoluto, a variação no sincronismo entre as máquinas locais deve ser menor que o período de validade da mensagem;
- Onde a identificação de uma entidade é essencial para o significado de uma mensagem, deve-se mencioná-la explicitamente na mensagem;
- Assinar digitalmente os dados antes de cifra-los. A assinatura em dados cifrados não comprova que o assinante conhece o seu conteúdo.

4.8 Conclusão

Sabe-se que para garantir a segurança em transações eletrônicas é necessário o emprego de protocolos criptográficos e que esses protocolos, devem ser inteiramente conhecidos e aceitos por todos os seus participantes.

Através de técnicas criptográficas como os algoritmos de cifragem, certificados e assinaturas digitais, pode-se conceber os protocolos criptográficos dentro dos requisitos de segurança indispensáveis em tal meio.

Um protocolo criptográfico deve ser tanto ou até mais seguro que um processo convencional para a realização de uma transação. Para isso, muitas técnicas tem sido propostas com o objetivo de controlar situações fraudulentas e participantes maliciosos. Novas entidades, também têm sido empregadas como participantes dos protocolos com objetivos específicos para controle de certificados digitais, protocolação de documentos eletrônicos e garantia de comunicação entre duas partes.

Para a definição de protocolos criptográficos são utilizados padrões, os quais orientam a implementação dos mesmos. No próximo capítulo esses padrões serão

abordados para que se possa compreender as proposições do protocolo, objeto deste trabalho, de forma a permitir a sua implementação futuramente.

Capítulo 5

SAC Seguro

5.1 Introdução

O sistema de atendimento proposto visa garantir a qualidade de serviços no atendimento ao cliente. Todas as requisições devem ser tratadas igualmente pela empresa e os direitos dos clientes garantidos. Caso isso não ocorra, uma autoridade fiscalizadora com poderes de punição pode intervir. As tecnologias de segurança já mencionadas, permitem a concepção deste protocolo, de modo a gerar um lastro das transações com comprovantes eletrônicos que são confiáveis e aceitos por todos os participantes dele.

Neste capítulo, serão mencionadas todas as peculiaridades deste sistema. A seção 5.2, descreverá as fases do protocolo de acordo com a ordem em que ocorrem para o atendimento ao cliente. Para melhor compreensão dos processos, transações e participantes do protocolo, a seção 5.3, destaca esses elementos e os identifica, associando nomes e siglas. Na seção 5.4, o protocolo proposto é apresentado detalhadamente, avaliando-se cada transação e processo de acordo como as fases descritas na seção 5.2. As seções 5.5 e 5.6, apresentam, respectivamente, as hipóteses consideradas na aplicação do protocolo e avaliam o atendimento dos requisitos de segurança, através da consideração dos problemas de comunicação e ataques do

homem do meio.

5.2 Fases do Protocolo

Para melhor entendimento e tratamento das diversas questões relacionadas ao protocolo proposto, faz-se a seguir, uma divisão das etapas a serem executadas para o atendimento ao cliente. Tais etapas, são caracterizadas pelas fases de atendimento de acordo com a ordem em que ocorrem.

5.2.1 Requisição

O cliente, através de um formulário apropriado no sítio do fornecedor, faz a requisição de um atendimento, seja para uma reclamação ou para a contratação de um serviço. A requisição é o ponto de partida do protocolo. Nesta fase, para o cumprimento dos requisitos de segurança desejados em um atendimento eletrônico, o cliente precisa ser identificado com a sua assinatura digital, que comprove para o protocolo a fonte e autoria da requisição. Ao mesmo tempo, o cliente deve receber um comprovante de que sua requisição foi aceita e que a partir desse momento começa a contar o prazo para o seu atendimento. Um recibo[1] então, é emitido pela empresa, contendo a requisição do cliente concatenada com um protocolo emitido por uma autoridade de datação. A autoridade de datação serve apenas para protocolar a requisição do cliente, dando assim uma referência temporal para a mesma. Uma autoridade fiscalizadora, definida durante a implantação do protocolo também recebe uma cópia do recibo[2] para acompanhamento ou intervenção no processo,

[1] Pode-se também, ao invés de recibo, utilizar-se o termo *protocolo* que de acordo com Aurélio [dHF 99], é um requerimento que serve como recibo, onde se anota a data e um número de ordem com que foi registrado no livro de protocolos. Entretanto, para se evitar ambigüidades com o protocolo eletrônico proposto, será adotado o termo *recibo*.

[2] Pode-se determinar que o próprio setor de garantia da qualidade da empresa seja a autoridade fiscalizadora ou então, em atividades controladas pelo governo, o setor ou entidade competente (PROCON, ANATEL, FEBRABAN, etc...)

caso isso seja necessário. Terminada essa fase, passa a decorrer o prazo para o atendimento ao cliente, iniciando-se assim, a fase seguinte. Caso o cliente não receba o recibo comprovando a sua solicitação, poderá recorrer após um determinado período (questão de minutos), contado a partir do momento da solicitação, para uma autoridade de aviso, que se encarregará de todas as formas em estabelecer a comunicação com a empresa. Se ainda assim, não se obtiver sucesso, a autoridade de aviso poderá acionar a autoridade fiscalizadora para que tome as providências cabíveis em relação à empresa por indisponibilidade dos serviços.

5.2.2 Atendimento

Nesta fase do protocolo, ocorre o atendimento propriamente dito, ou seja, a requisição do cliente passa a ser tratada pela empresa com a abertura de uma ordem de serviço. Após concluído o atendimento à requisição, a empresa emite um comunicado de conclusão da ordem de serviço para o cliente e também para a autoridade fiscalizadora. Esse comunicado deve também ser protocolado pela autoridade de datação para comprovar o prazo de atendimento ao cliente. A autoridade fiscalizadora registra todos os eventos em seu banco de dados para uso futuro em caso de auditoria na empresa que adota o protocolo, ou ainda, em caso de litígio com o cliente.

5.2.3 Fechamento da Requisição

Entende-se por fechamento da requisição, o encerramento de uma transação entre cliente e empresa. Esta fase pode tomar dois caminhos, dependendo do comportamento do cliente junto ao protocolo:

Fechamento natural pelo cliente - sendo o cliente notificado pela empresa do atendimento à sua requisição, ele deve verificá-la e naturalmente efetuar o fechamento da requisição junto à empresa, enviando para a mesma a notificação recebida assinada digitalmente.

Fechamento forçado por decurso de prazo - caso o cliente não se manifeste a respeito da notificação, a empresa aciona a partir de uma determinado prazo uma autoridade de aviso. A autoridade de aviso tem como objetivo terceirizar a notificação de conclusão da ordem de serviço pela empresa. Essa terceirização é salutar ao protocolo na medida em que a autoridade de aviso conta com todos os meios de comunicação possíveis para contatar o cliente, podendo ser esses físicos ou eletrônicos. Para a empresa comprovar o decurso de prazo para o fechamento natural da requisição, ela pode utilizar a própria notificação que foi enviada ao cliente, pois esta contém o protocolo gerado pela autoridade de datação quando a ordem de serviço foi encerrada. Caso ainda assim persista a indiferença do cliente para o fechamento da requisição, esta poderá ser fechada automaticamente após um determinado período.

Quando a requisição for encerrada naturalmente pelo cliente, a empresa pode aproveitar o momento para obter as opiniões dele sobre o atendimento através do preenchimento de um simples formulário eletrônico. Isso criará oportunidades de melhoria na qualidade do atendimento e também nos serviços prestados.

5.2.4 Litígio

Em caso de litígio, a autoridade fiscalizadora poderá agir como mediadora dos interesses dos participantes, pois, durante todas as transações ela recebe informações que documentam cada ato. De acordo com a definição dada de protocolo criptográfico, espera-se que todos os participantes estejam cientes e aceitem as disposições do mesmo. Logo, os recibos de contratação de serviços ou reclamações e as notificações de encerramento de ordens de serviço, são documentos oficiais do protocolo e podem ser utilizados como prova em caso de qualquer dúvida. Os registros das transações efetuadas com sucesso e encerradas entre os clientes e as empresas, poderão, a critério da autoridade fiscalizadora, ser descartadas para a redução dos custos de armazenamento e manutenção com o banco de dados.

5.3 Notação e Identificação dos Participantes

Para se entender claramente a notação utilizada nas mensagens trocadas entre os participantes do protocolo, faz-se necessária a identificação dos elementos utilizados nas mesmas através das siglas abaixo:

CL - Cliente: usuário do protocolo;

EM - Empresa: quem adota o protocolo;

AD - Autoridade de Datação: responsável por protocolar os recibos das requisições e os de fechamento;

AF - Autoridade Fiscalizadora: mediadora dos eventuais litígios entre o cliente e a empresa;

AC - Autoridade Certificadora: provedora dos certificados digitais para a identificação dos elementos participantes;

AA - Autoridade de Aviso: responsável pela notificação do cliente através de diversos meios de comunicação;

E - Cifrar: processo de embaralhamento de uma mensagem com a utilização de um algoritmo de cifragem e uma chave;

D - Decifrar: processo de reversão da cifração com a utilização de um algoritmo de cifragem e uma chave;

K - Chave: código secreto a ser utilizado por um algoritmo de critografia simétrica tanto para cifrar quanto para decifrar mensagens;

KR - Chave Privada: código secreto a ser utilizado por um algoritmo de critografia assimétrica tanto para cifrar quanto para a decifrar mensagens;

KU - Chave Pública: código secreto a ser utilizado por um algoritmo de critografia assimétrica tanto para cifrar quanto para decifrar mensagens;

REQ - Requisição: que é assinada digitalmente pelo cliente e enviada para a empresa;

RESUMO_REQ - Resumo da Requisição: gerado pela empresa para ser protocolado junto à autoridade de datação;

PROTOCOLO_REQ - Protocolo da Requisição: gerado pela autoridade de datação para compor o recibo de requisição a ser enviado para o cliente;

OS - Ordem de Serviço: gerada pela empresa para atender a requisição enviada pelo cliente;

RR - Recibo da Requisição: mensagem composta pela requisição do cliente e o protocolo gerado pela autoridade de datação. Serve como garantia para o cliente que efetuou a requisição;

RESUMO_FEC - Resumo de Fechamento: gerado pela empresa para ser protocolado junto à autoridade de datação;

PROTOCOLO_FEC - Protocolo de Fechamento: gerado pela autoridade de datação para compor o comprovante de fechamento da requisição a ser enviado para o cliente;

FEC - Fechamento: ordem de serviço assinada digitalmente pela empresa e protocolada pela autoridade de datação. Serve como garantia para a empresa de que efetuou o serviço naquele determinado prazo;

RF - Recibo de Fechamento: gerado pelo cliente com a sua assinatura na mensagem de fechamento da ordem de serviço recebida da empresa.

5.4 O Protocolo Proposto

Após se entender as fases do protocolo proposto conforme descrito nas seções anteriores e conhecer a notação para a referência dos elementos e processos realizados, pode-se detalhar o funcionamento do mesmo, descrevendo formalmente cada mensagem, com base na figura 5.1:

Observando então, os passos numerados na figura 5.1, temos:

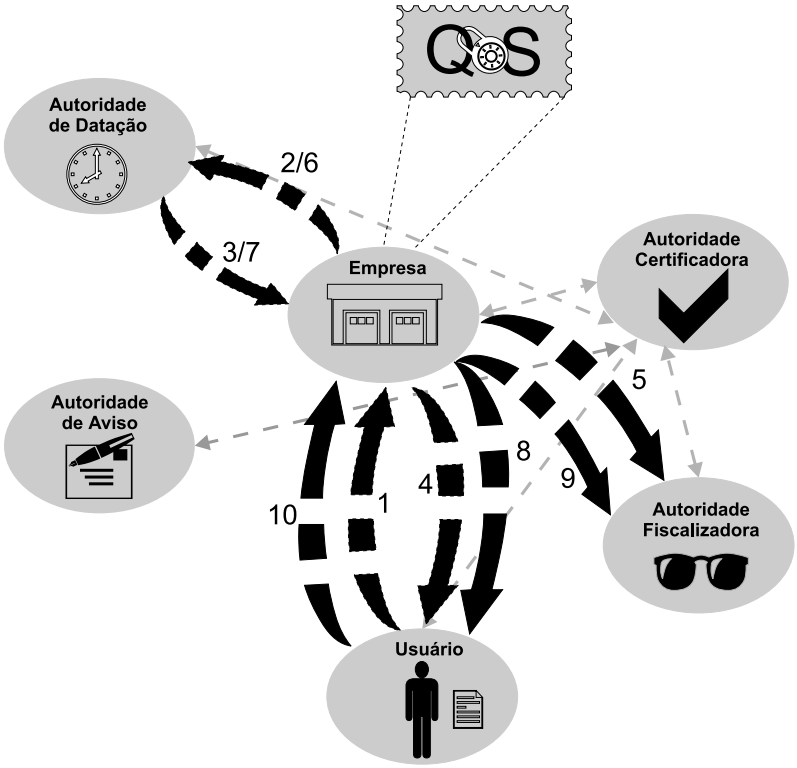

Figura 5.1: Protocolo Proposto. 1. **CL** faz a requisição; 2. **EM** envia em recibo da requisição para **AD**; 3. **AD** protocola o recibo e devolve-o para **EM**; 4. **EM** envia o recibo de requisição para **CL**; 5. **EM** envia uma cópia do recibo de requisição para **AF**; 6. Após concluir a **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.

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.

5.4.1 Empresa não responde

Conforme ilustrado na figura 5.2, se após um determinado período, o cliente não tenha ainda recebido o recibo de sua requisição, ele poderá invocar a autoridade de aviso para que retransmita a sua requisição. Se esta por sua vez, não obtiver resultado com a empresa, poderá comunicar a autoridade fiscalizadora, que irá imediatamente intervir junto a empresa pela indisponibilidade e ou, negação de serviço. Tendo a empresa atendido ao comunicado da autoridade de aviso, deverá providenciar o recibo da requisição para o cliente, como o faria normalmente.

5.4.2 Cliente não responde

Conforme ilustrado na figura 5.3, caso o cliente não se manifeste em relação ao fechamento do pedido até um determinado prazo, contado a partir da data de fechamento da OS, a empresa encaminha o mesmo para a autoridade de aviso que se encarregará de notificá-lo. O papel da autoridade de aviso, consiste em, de todas as formas possíveis (telefonemas, cartas, *e-mail*, jornal), dar ciência ao cliente, de que sua requisição junto a empresa foi atendida. A contagem do prazo citado, pode ser feita facilmente através da verificação da mensagem de fechamento, gerada pela

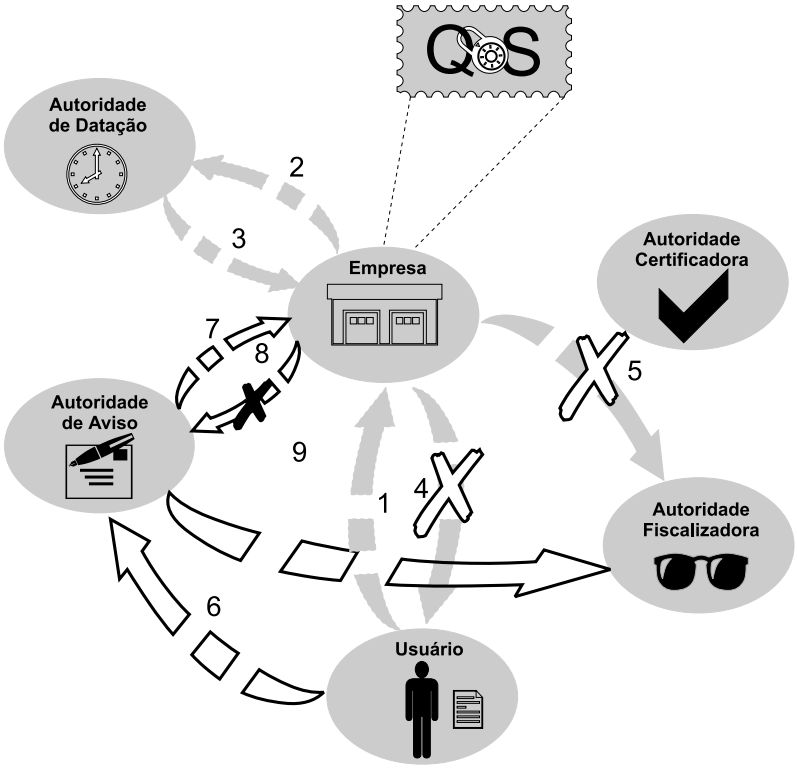

Figura 5.2: Comportamento do protocolo quando a empresa não responde ao cliente. Quando expira o tempo da resposta esperada da empresa à solicitação do cliente (passos 4 e 5), este recorre a autoridade de aviso para tentar nova comunicação (6). A autoridade de aviso, tenta estabelecer contato com a empresa para transmitir a requisição do cliente (7). Caso a empresa não responda novamente (8), a autoridade de aviso comunica o fato para a autoridade fiscalizadora (9).

empresa e protocolada pela autoridade de datação (FEC). Caso as tentativas anteriores de contato com o cliente para fechamento das transações fracassem, a empresa poderá fechar a requisição por decurso de prazo.

5.4.3 Litígio

Essa etapa do protocolo, somente irá acontecer se a empresa não cumprir o prazo acordado com o cliente ou o determinado por lei para o atendimento. Sendo assim, o cliente pode recorrer à autoridade fiscalizadora e apresentar o seu recibo de requisição (RR). A **AF**, verifica em seu banco de dados a existência de uma solicitação de fechamento (FEC) correspondente ao recibo de requisição apresen-

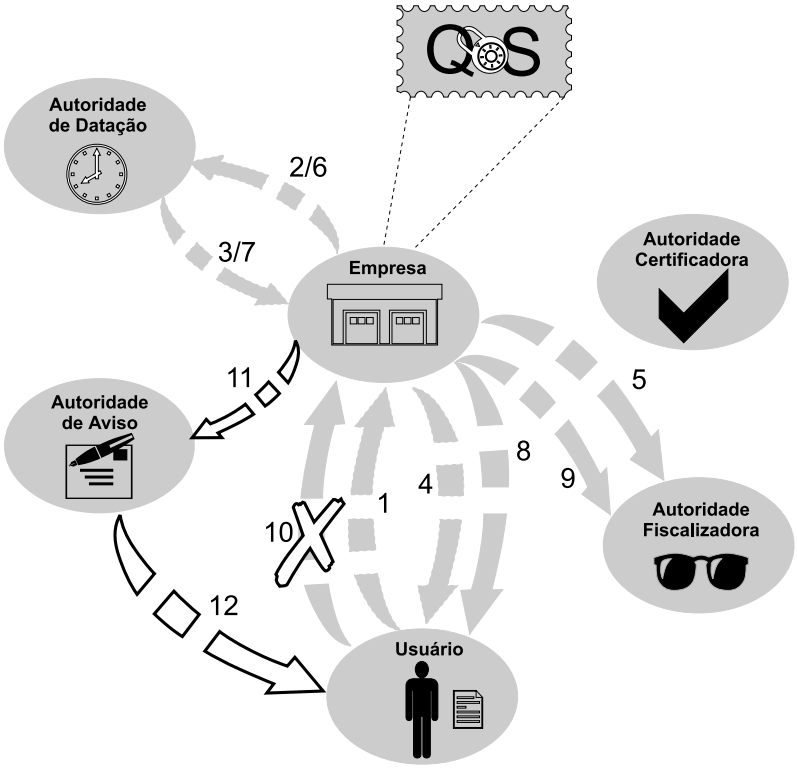

Figura 5.3: Comportamento do protocolo quando o cliente não responde a solicitação de fechamento da OS. Caso o cliente se omita no fechamento da OS (10), a empresa poderá acionar a autoridade de aviso para tentar no contato (11). A autoridade de aviso, por sua vez, tentará de todas as formas possíveis, notificar o cliente a pedido da empresa (12). Caso mesmo assim o cliente não se manifeste, a ordem de serviços poderá ser fechada por decurso de prazo.

tado pelo cliente. Caso não haja, esta poderá intervir junto à empresa em favor do cliente. Existindo tal correspondência, significa que de algum modo a empresa atendeu o cliente e este por algum motivo não recebeu a solicitação de fechamento ou simplesmente a ignorou. A figura 5.4 ilustra esse processo.

5.5 Premissas Básicas

Naturalmente que, dada a pretensão do protocolo proposto e ao enorme grau de desdobramentos ocorridos pela complexidade do sistema apresentado, parte-se de algumas premissas básicas para que se possa estabelecer uma base e dar limites para a análise e verificação. Tais premissas são tidas como verdades absolutas perante o

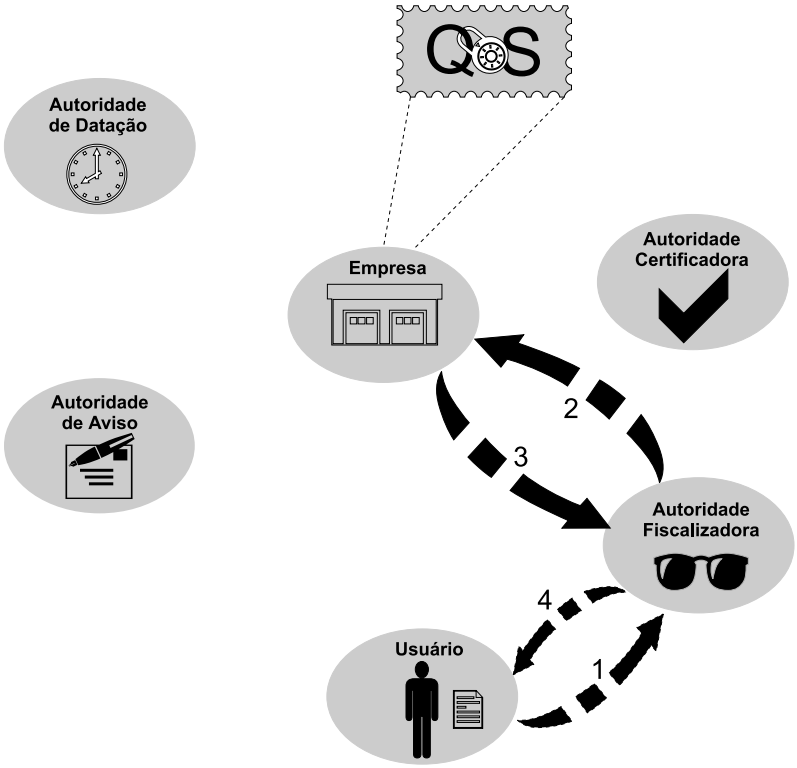

Figura 5.4: Litígio. Em caso de reclamação por não atendimento, o cliente poderá invocar a autoridade fiscalizadora de posse do seu recibo de requisição (1). A autoridade fiscalizadora, por sua vez, fará uma verificação em seu banco de dados buscando uma correspondência para tal recibo. Caso não encontre, notificará a empresa (2), da qual solicitará uma justificativa (3) e a encaminhará para o cliente (4).

protocolo.

- O protocolo conta com quatro entidades de suporte (Autoridade de Datação (AD), Autoridade Certificadora (AC), Autoridade de Aviso (AA) e Autoridade Fiscalizadora (AF)), as quais, são tidas como honestas e confiáveis;
- Considera-se também, que as entidades de suporte tenham redundância de unidades para que não hajam problemas com indisponibilidade de serviços ou até mesmo de comunicação que possam comprometer a funcionalidade do protocolo;
- Todos os clientes usuários do protocolo tem um certificado digital para garantir a sua autenticação perante o sistema e também para a geração de documentos eletrônicos confiáveis.

5.6 Segurança

A segurança no protocolo proposto, pode ser avaliada com a análise do papel de cada um dos participantes e a conjectura de suas atitudes. Conforme mencionado na seção 5.5, considera-se as entidades de suporte são seguras e confiáveis, restando apenas a verificação do comportamento da empresa e do cliente ou usuário. O protocolo deve ser robusto o suficiente, na utilização de técnicas de segurança para suportar e prever as diversas tentativas de fraude que possam vir a ocorrer.

Supondo-se que o cliente seja malicioso perante o protocolo, pode-se levantar algumas hipóteses para a avaliação do comportamento e robustez do protocolo:

- O cliente faz uma reclamação improcedente junto a autoridade fiscalizadora pelo não atendimento da empresa:

  Para toda e qualquer reclamação por parte do cliente, a autoridade fiscalizadora exigirá um comprovante de que uma requisição foi realmente feita. Só assim a AF poderá interceder pelo cliente junto a empresa. Quando o cliente faz uma requisição e recebe o recibo de requisição (RR), a AF também recebe uma cópia para que no momento de litígio ela possa verificar a validade da reclamação;

- O Cliente recorre a autoridade de aviso para tentar comprometer a empresa, sem antes ter tentado fazer a requisição:

  A autoridade de aviso, tem o objetivo de garantir a comunicação e o não repúdio entre a empresa e o cliente e vice-versa. Sendo assim, ela não tem poderes de punição ou fiscalização das entidades. Se o cliente tentar fazer a requisição diretamente pela autoridade de aviso, e a empresa responder, emitindo o recibo (RR), o processo pode ser considerado normal para o protocolo. Caso a empresa não atenda a AA, esta poderá então notificar a autoridade de fiscalização do ocorrido;

- O cliente faz uma solicitação de serviço ou reclamação e tenta negar futuramente:

Como o cliente assina digitalmente a requisição e essa é considerada como um documento oficial do protocolo, ele não poderá repudiá-la futuramente. Entretanto, de acordo com os direitos do consumidor, qualquer pedido de serviço fora do ambiente da empresa (por telefone ou Internet), dá ao cliente o direito de arrependimento até sete dias após o mesmo ter sido feito;

- O cliente se recusa a fechar a ordem de serviço referente à sua requisição:

  A empresa poderá recorrer a autoridade de aviso para que o cliente seja novamente notificado. Se mesmo assim ele não responder, o fechamento da ordem de serviço se dará automaticamente. Se o cliente não ficar satisfeito com o atendimento recebido, poderá apresentar uma queixa a autoridade fiscalizadora apresentando o seu recibo de requisição dentro de um prazo legal;

- O cliente utiliza um recibo de uma requisição já atendida para efetuar uma reclamação junto a autoridade fiscalizadora:

  A autoridade fiscalizadora, mantém em seu banco de dados todos os registros de requisições que ainda não foram atendidas e poderá, a qualquer momento acessá-los para verificação. Os registros de transações concluídas entre os clientes e as empresas são descartados pela AA. Quando uma requisição é feita, a empresa efetua um protocolo da mesma junto a autoridade de datação. Assim, ela não pode ser utilizada com outro fim. A empresa também, por sua vez, dispõe de um recibo de fechamento referente a requisição em questão, logo, a reclamação do cliente se torna infundada.

A empresa, por sua vez poderá tentar se apresentar maliciosamente ao sistema quando:

- Negar serviço ao cliente ignorando a sua requisição por não lhe interessar:

  O cliente, após poucos minutos da requisição, poderá acionar a AA para questionar o não recebimento da confirmação de sua requisição;

- Retardar o envio da requisição do cliente para a autoridade de datação com o objetivo de ganhar tempo:

Após receber uma requisição, a empresa deverá imediatamente gerar um resumo da mesma e protocolá-la junto a AD para a emissão do recibo do cliente. Se isso não ocorrer dentro de poucos minutos (tempo a ser definido e configurado na implantação do protocolo), ela será interpelada pela AA, que não obtendo uma resposta dentro do mesmo prazo, poderá invocar a AF;

– Utilizar um recibo de fechamento de uma requisição antiga para comprovar o atendimento ao cliente junto a autoridade fiscalizadora:

  Da mesma maneira que ocorre com o cliente, uma cópia da solicitação de fechamento (FEC), é enviada para a autoridade fiscalizadora. Essa solicitação de fechamento contém dados específicos de uma única requisição e também é protocolada pela AD, impedindo com isso, a sua reutilização.

5.6.1 Problemas de Comunicação

Na concepção do protocolo proposto considera-se um ambiente isento de falhas ou interrupções das linhas de comunicação de cada participante com a Internet e também, na disponibilidade de serviços das entidades de suporte, entretanto, na prática isso poderá ocorrer.

Com relação às entidades de suporte, sendo essas independentes e das quais dependem muitos outros protocolos, operações de contingência devem ser previstas para esses casos, garantindo a alta disponibilidade dos serviços oferecidos por elas.

A Autoridade de Aviso, por sua vez, tem como finalidade estabelecer a comunicação entre a empresa e o cliente de diversas formas, dando assim, maior robustez ao protocolo e resgatando a comunicação que eventualmente estivesse indisponível no momento de uma requisição ou de um fechamento de OS.

5.6.2 Ataque do Homem do Meio

Com a existência de uma grande troca de mensagens no protocolo, uma questão que deve ser minuciosamente avaliada é a dos ataques. Conforme visto no capítulo 4, a

comunicação está sujeita a ataques passivos e ativos, podendo aumentar ou diminuir a circulação de mensagens entre os participantes, dependendo das atividades ou intenções do oponente. O oponente ou *homem do meio*, como também é chamado, é aquele que participa da comunicação entre duas entidades de forma clandestina, objetivando algum benefício próprio com a interceptação, fabricação ou captura de informações para uso futuro. O protocolo, por sua vez, deve prever situações deste tipo e por isso, cada uma das mensagens trocadas descritas na seção 5.4, serão avaliadas sobre este aspecto:

1. A requisição do cliente:

   REQ = E_{KR_CL}[requisição]

   Essa mensagem pode ser um dos alvos preferidos por um oponente para a geração de um ataque por repetição (*replay*). Uma vez interceptada, a mesma poderia ser incansavelmente apresentada para a empresa solicitando um mesmo serviço. No entanto, como a mensagem é assinada pelo cliente e o seu conteúdo não pode ser alterado, facilmente poderia se identificar tal ataque através de testes com regras de consistência das mensagens. Uma outra alternativa para se resolver este problema, seria a determinação de um tempo de validade para a mensagem através de um carimbo de tempo (*time stamp*) no momento da requisição. Maiores detalhes sobre *time stamp* podem ser encontrados no capítulo 4

2. A empresa recebe a requisição:

   Ao receber uma requisição do cliente, a empresa gera um resumo (*hash* da mensagem e envia para a AD para que este seja datado:

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

   Esse processo faz parte de um protocolo específico para a datação de documentos eletrônicos e é considerado seguro e confiável pelo protocolo proposto;

3. A datação da requisição:

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

Essa mensagem também é parte integrante do protocolo de datação citado acima e portanto, também é considerada neste caso, segura;

4. Composição e envio do recibo da requisição (RR) para o cliente:

   RR = [REQ || PROTOCOLO_REQ]

   Essa mensagem comprova a requisição do cliente e o aceite de execução pela empresa. Como encontra-se datada, passa a ser um documento oficial do protocolo, podendo ser utilizada como prova. Logo, a sua captura e apresentação permitirá o acionamento da autoridade fiscalizadora da empresa a qualquer momento. Entretanto, como a AF também tem em seu banco de dados uma cópia, (tanto da requisição como do fechamento), ela poderá verificar facilmente a fraude, acionando a empresa somente se a sua apresentação for procedente.

   Caso o envio da mensagem seja interrompido por um intruso e o prazo de resposta à requisição se esgote, o cliente poderá acionar a autoridade de aviso para que esta estabeleça contato com a empresa. Com isso, a empresa tomará conhecimento da interrupção da mensagem;

5. Cópia do recibo que é remetida para a autoridade fiscalizadora:

   Sendo a mesma mensagem do passo anterior e servindo apenas para atualizar o banco de dados da AF, ela não é fundamental neste momento. Caso haja uma reclamação por parte do cliente e a AF não tenha os devidos registros dos recibos, a empresa poderá ser intimada de qualquer forma;

6. O fechamento da OS:

   Para gerar o comprovante de fechamento (FEC), após a empresa fechar a OS, ela deverá datá-la para comprovar o prazo de atendimento ao cliente com o envio da seguinte mensagem para a AD:

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

   Assim como acontece na requisição, esse processo faz parte de um protocolo específico para a datação de documentos eletrônicos e é considerado seguro e

confiável pelo protocolo proposto, dispensando a análise de possíveis ataques;

7. A datação do fechamento:

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

   Essa mensagem é gerada pelo protocolo de datação e portanto, considerada segura;

8. Composição e envio da solicitação de fechamento da OS (FEC) para o cliente:

   FEC = [OS || PROTOCOLO_FEC]

   A utilização maliciosa dessa mensagem, pouco poderá afetar o protocolo, pois, qualquer entidade participante poderá verificar o seu conteúdo, observando que se trata de uma requisição e de uma OS em específico, inclusive com datação.

   Caso o envio da mensagem seja interrompido por um intruso e o prazo de atendimento se esgote, o cliente poderá reclamar com o seu recibo de requisição (RR) junto à AF. Se a AF recebeu o FEC, ela poderá retransmiti-lo ao cliente, caso contrário, ela intimará a empresa;

9. Cópia da solicitação de fechamento da OS (FEC) que é remetida para a autoridade fiscalizadora:

   Sendo a mesma mensagem do passo anterior e servindo apenas para atualizar o banco de dados da AF, ela não é fundamental neste momento. Caso haja uma reclamação por parte do cliente e a AF não tenha os devidos registros dos recibos, a empresa poderá ser intimada;

10. O recibo de fechamento:

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

    O cliente precisa assinar o fechamento da transação (FEC) para comprovar que a mesma foi concluída. Se tratando de uma requisição e de uma OS em específico, e podendo isso ser verificado facilmente, essa mensagem de nada serve para um oponente do protocolo. Caso o seu envio seja interrompido, a empresa poderá recorrer à autoridade de aviso após um certo período para que

esta estabeleça contato com o cliente. Assim o cliente tomará conhecimento da interrupção da mensagem.

5.7 Conclusão

Considerando as hipóteses previstas neste capítulo como ponto de partida para a implementação, instalação e utilização do SAC seguro, pode-se considerar o protocolo seguro e confiável para a garantia da qualidade de serviços.

A legislação brasileira para o tratamento de transações eletrônicas precisa ainda evoluir muito para que as provas geradas pelo protocolo que são computacionalmente seguras, possam ser utilizadas em casos de litígio entre as entidades.

Capítulo 6

Formalização do SAC Seguro

6.1 Introdução

No capítulo anterior, o protocolo proposto foi descrito conforme as fases de sua utilização, porém, a formalização do modelo se faz necessária para que através de uma representação matemática, seja assegurado o seu funcionamento e eficácia para a resolução do problema estudado nesse trabalho. Segundo Tanenbaum [TAN 97], os protocolos são geralmente complicados e por isso, diversas pesquisas foram realizadas com o intuito de se aplicar técnicas matemáticas formais para a especificação e verificação dos mesmos.

Naturalmente, os resultados alcançados com a análise e verificação do SAC seguro poderão ser empregados na fase de implementação do protocolo, proporcionando uma visão confiável do comportamento dos elementos e entidades envolvidas.

Para a análise e verificação do SAC seguro, serão empregadas as técnicas das redes de Petri, abordadas na seção 6.2. A análise das fases do protocolo será realizada com base nos modelos criados nas redes de Petri na seção 6.3. Os resultados obtidos da modelagem das fases do protocolo, serão discutidos na seção 6.4.

6.2 Redes de Petri

Conforme já mencionado no capítulo 4, os modelos baseados nas redes de Petri são altamente recomendados para a análise e especificação de protocolos, pois têm profunda base matemática e permitem a especificação gráfica de um protocolo, que entre outras coisas, proporciona a identificação de quebras de segurança do mesmo e avaliação de desempenho.

Em [CAR 97], são apresentados os três elementos básicos de uma rede de Petri:

Lugar - representado por um círculo, tem em geral um predicado associado como *necessidade do cliente, sítio disponível, requisição feita*. Esse predicado por ser uma condição, uma espera, um procedimento ou um conjunto de recursos;

Transição - representada graficamente por uma barra ou um retângulo, expressa um evento que ocorre no sistema, como *requisitar serviço*;

Ficha - também conhecida por *token* representada por um ponto dentro do lugar (círculo), pode determinar uma condição do lugar onde se encontra. Supondo-se que exista uma ficha no lugar *Web site disponível*, pode dizer que esta condição é verdadeira e do contrário não.

A figura 6.1, ilustra os elementos básicos apresentados para melhor compreensão dos conceitos. De acordo com a ilustração (a), pode-se observar que a transição *Requisitar serviço* está habilitada para a execução, pois, existem fichas nos dois lugares de entrada. Ao ser executada, a transição gera uma ficha de saída para o lugar imediatamente ligado a ela obedecendo o fluxo da rede (b). Segundo Cardoso [CAR 97], um estado parcial no sistema é representado por um lugar na rede de Petri, enquanto que as transições são associadas aos eventos que ocorrem no mesmo. O disparo de uma transição, que representa a ocorrência de um evento, consiste na mudança das fichas dos lugares de entrada para os de saída.

Muitas variações da combinação de lugares, transições e fichas poderão ser encontradas em uma rede de Petri, isto é, essas variações, permitem a representação

de diversos modelos, assim também como características fundamentais para a suas análises como concorrência, conflitos e paralelismo de processos. Maiores informações sobre as redes de Petri podem ser obtidas em [CAR 97].

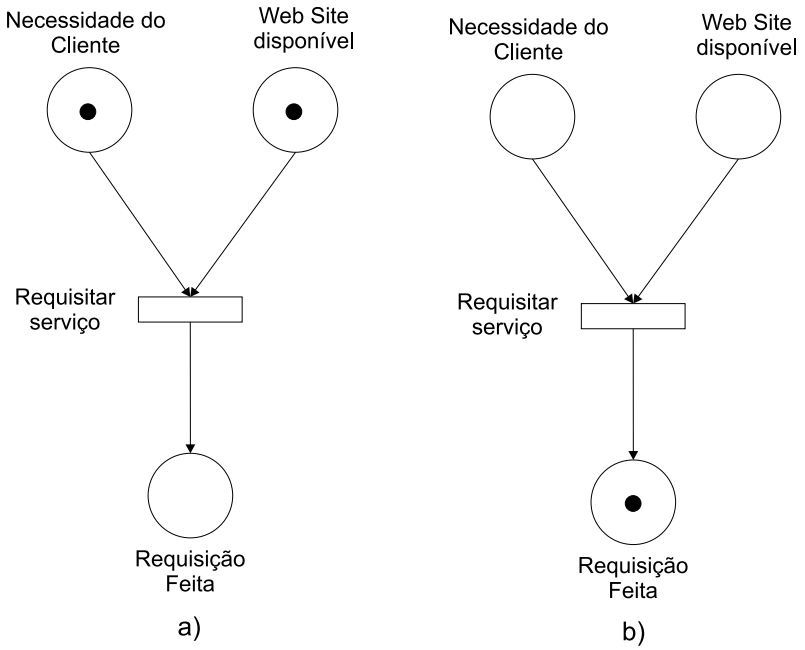

Figura 6.1: Rede de Petri. Representação gráfica básica de uma rede de Petri com as fichas nas marcações iniciais habilitando a transição (a) e a transição já disparada posicionando a ficha no lugar *requisição feita* (b).

6.3 Especificação do SAC Seguro

Para a especificação do SAC seguro proposto serão empregadas as técnicas das redes de Petri, onde as fases do sistema proposto serão modeladas conforme apresentado no capítulo 5. Os modelos estudados são no total quatro e consideram as questões principais do problema, avaliando o comportamento do sistema como um todo, o momento em que a empresa não responde às solicitações do cliente, quando o cliente não responde às solicitações da empresa e o caso do litígio entre as partes. As mensagens trocadas entre os participantes do protocolo que foram detalhadas no capítulo anterior, serão aqui, transformadas em transições e lugares para o estudo com as redes de Petri.

6.3.1 O SAC Seguro modelado

A rede de Petri da figura 6.2, mostra o SAC seguro modelado e permite se ter uma visão clara do fluxo do atendimento ao cliente. Observando a figura, pode-se verificar uma marcação inicial nos lugares *Cliente* e *Web site disponível*, os quais precisam estar simultaneamente ocupados por uma ficha para o disparo de uma requisição de serviços. A seguir, são detalhados todos os lugares e transições dessa rede conforme mostrados na figura para uma melhor compreensão do modelo apresentado:

Lugar *Cliente* - Início da rede que juntamente com o lugar *Web site disponível*, disparam juntos uma requisição de serviços;

Lugar *Web site disponível* - Início da rede que juntamente com o lugar *Cliente*, disparam juntos uma requisição de serviços. A existência desses dois lugares marcados são fundamentais para o disparo da transição a seguir;

Transição *Requisitar serviço* - Essa transição é automaticamente disparada quando os seus lugares de entrada tiverem fichas e ela, por sua vez, dá a entrada em dois outros lugares: *Espera* e *Requisição Cliente*. O lugar *Espera*, habilita o disparo de uma reclamação se o cliente não for atendido em um determinado prazo e o lugar *Requisição Cliente*, habilita a transição para a geração da ordem de serviços (OS);

Lugar *Requisição Cliente* - Quando possui uma ficha, indica na rede que existe uma requisição de cliente a ser atendida;

Transição *Gerar OS* - Habilitada pela requisição do cliente, essa transição dispara o processo de atendimento da requisição do cliente e também da protocolação da OS para a geração do recibo de requisição (RR);

Lugar *OS protocolação* - Seguindo a ramificação da rede no sentido da protocolação do pedido do cliente que lhe servirá como garantia futuramente, tem-se esse lugar que habilita a transição para a protocolação da OS;

Transição *Protocolar OS* - Como resultado dessa transição, que objetiva datar a requisição do cliente para se ter uma marcação temporal do pedido, é gerado o recibo de requisição (RR);

Lugar *Recibo de Requisição* - Indica quando marcado, a geração com sucesso do recibo da requisição feita pelo cliente e a protocolação do mesmo junto à autoridade de datação, habilitando assim, o envio do mesmo;

Transição *Remeter RR* - Essa transição responde por encaminhar uma cópia do recibo da requisição gerado e datado para a autoridade fiscalizadora do protocolo (AF) e a outra para o próprio cliente;

Lugar *AF* - Acusa quando marcado, o recebimento de uma cópia do recibo da requisição protocolado pela empresa;

Lugar *RR* - Acusa quando marcado, o recebimento de uma cópia do recibo da requisição protocolado pela empresa e habilita parcialmente as transições para a conclusão da requisição que dependerá do tempo de espera para atendimento (lugar *Espera*), configurado no sistema e também do tempo decorrido entre a requisição do cliente e a emissão do RR;

Transição *Concluir Requisição no Prazo* - É disparada se os lugares *RR* e *Espera* estiverem marcados, o que significa que o recibo da requisição do cliente foi emitido com um tempo menor que o prazo de espera configurado no sistema;

Lugar *Atendimento no Prazo* - Determina quando marcado, que um recibo de uma requisição de um cliente foi emitido dentro do prazo aceitável de espera definido no sistema;

Lugar *Espera* - Determina quando marcado, que uma requisição de serviço foi feita por um cliente e que a mesma está no aguardo do RR;

Transição *Disparar Reclamação* - Essa transição é habilitada quando uma requisição de um cliente é feita e disparada quando um prazo de espera definido pelo sistema se esgotar;

Lugar *Reclamação* - Acusa quando marcado, a existência de uma reclamação de

um cliente pelo não atendimento à sua requisição de serviços dentro do prazo de espera e habilita o acionamento da autoridade de aviso (AA);

Transição *Acionar AA* - Essa transição é disparada com uma reclamação de um cliente e gera um aviso para a empresa solicitando atendimento;

Lugar *Aviso Cliente* - Determina quando marcado, que a autoridade de aviso foi acionada e por sua vez, habilita para disparo a transição que deverá acionar a empresa;

Transição *Acionar Empresa* - A autoridade de aviso aciona a empresa através da existência de uma reclamação de um cliente;

Lugar *Empresa Acionada* - Quando marcado, esse lugar habilita parcialmente a transição para a conclusão da requisição com atraso *Concluir Requisição com Atraso*;

Transição *Concluir Requisição com Atraso* - Essa transição é disparada se os seus dois lugares de entrada estiverem marcados (*RR* e *Empresa Acionada*). Isso significa que a requisição do cliente foi atendida com atraso, pois, somente após o prazo de espera estabelecido no sistema e através da reclamação feita, é que o RR foi emitido;

Lugar *OS Produção* - Esse lugar, quando marcado inicia a produção da ordem de serviços gerada pela requisição do cliente;

Transição *Executar OS* - Essa transição, quando habilitada é disparada e representa a execução do serviço propriamente dito solicitado pelo cliente;

Lugar *OS Concluída* - Representa quando marcado, a conclusão do serviço requisitado pelo cliente e dá início ao processo de fechamento da OS, habilitando a transição *Protocolar Fechamento*;

Transição *Protocolar Fechamento* - Para comprovar o prazo de atendimento ao cliente, essa transição de protocolação é disparada a partir da conclusão da OS para se dar uma marcação temporal através da autoridade de datação;

Lugar *OS Fechamento* - Acusa quando marcado, que uma OS foi protocolada pela autoridade de datação e habilita assim, o envio da solicitação de fechamento da OS para o cliente e para a autoridade fiscalizadora;

Transição *Remeter FEC* - Remete com o seu disparo habilitado pelo lugar *OS Fechamento*, a solicitação de fechamento da OS (FEC) para o cliente e para a autoridade fiscalizadora;

Lugar *FEC AF* - Acusa quando marcado, o recebimento pela autoridade fiscalizadora da solicitação de fechamento da OS concluída (FEC);

Lugar *FEC Cliente* - Acusa quando marcado, o recebimento pelo cliente da solicitação de fechamento da OS concluída;

Transição *Assinar FEC* - Essa transição, quando disparada gera o recibo de fechamento da OS e representa o aceite do cliente ao serviço prestado pela empresa;

Lugar *Recibo de Fechamento* - Determina quando marcado, que uma solicitação de fechamento de OS (FEC) foi assinada pelo cliente e habilita o envio do RF para a empresa;

Transição *Remeter RF* - Remete com o seu disparo habilitado pelo lugar *Recibo de Fechamento*, o RF para a empresa;

Lugar *OS Fechada* - Quando marcado, determina que a requisição do cliente foi atendida e a OS foi fechada pelo cliente.

6.3.2 Empresa não responde

A rede de Petri da figura 6.3, mostra o comportamento do SAC seguro quando a empresa não responde à requisição do cliente. Numa primeira instância, o cliente recorre para a autoridade de aviso, que por todas as maneiras possíveis tentará comunicar-se com a empresa, porém, não obtendo sucesso, essa poderá acionar a autoridade fiscalizadora da empresa para que a mesma a notifique. A seguir, são detalhados todos os lugares e transições dessa rede conforme mostrados na figura para uma melhor compreensão do modelo apresentado:

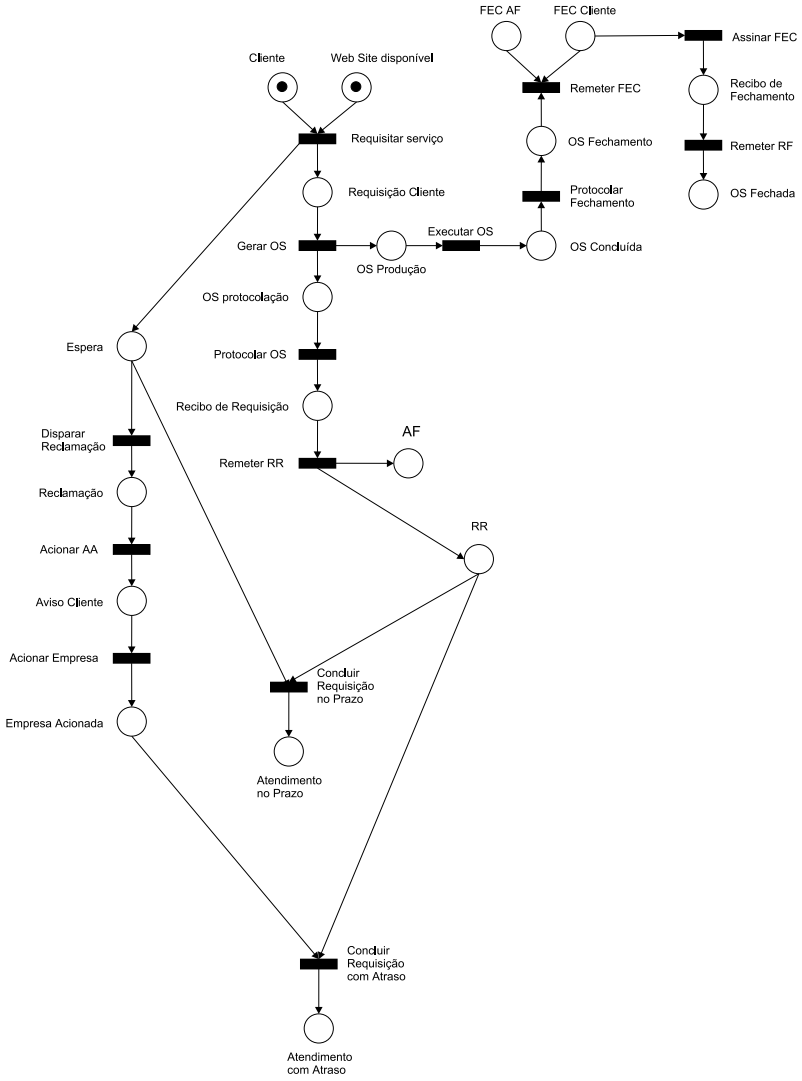

Figura 6.2: Rede de Petri do protocolo proposto. Modelo do protocolo exibindo o fluxo da comunicação entre e as fases do atendimento de geral.

Lugar *Empresa não responde* - Esse lugar, inicialmente marcado na rede, determina uma reclamação de um cliente pelo não atendimento à uma requisição feita e dispara uma transição para o acionamento da autoridade de aviso;

Transição *Acionar AA* - É disparada pela marcação do lugar *Empresa não responde* e gera uma solicitação de um cliente;

Lugar *Solicitação Cliente* - Quando marcado, representa o acionamento da AA pelo cliente por não atendimento pela empresa;

Transição *Acionar Empresa* - Essa transição é disparada pela existência de uma

solicitação de um cliente, a qual gera para a empresa uma solicitação da autoridade de aviso;

Lugar *Solicitação AA* - Determina, quando marcado, que a empresa foi acionada e que recebeu uma solicitação da AA;

Transição *Atender Solicitação* - A existência da solicitação da AA habilita essa transição que pede à empresa providências no atendimento ao cliente e gera um lugar de espera;

Lugar *Espera* - Determina quando marcado, que uma solicitação de atendimento foi feita à empresa pela autoridade de aviso e que o cliente está no aguardo do atendimento de sua requisição;

Transição *Atender Cliente por Aviso* - Se o tempo de resposta ao atendimento da requisição do cliente for menor que o estipulado pelo sistema, então essa transição é disparada e conclui-se que o cliente que a intervenção da AA foi suficiente para o atendimento ao cliente. Como resultado, essa transição marca o lugar *Requisição Cliente*;

Transição *Acionar AF* - Entretanto, se o tempo de resposta ao atendimento da requisição do cliente for maior que o estipulado pelo sistema, então essa transição é disparada para a intervenção da AF no atendimento. Como resultado, essa transição marca o lugar *Notificação* para que a empresa seja novamente acionada;

Lugar *Notificação* - Acusa quando marcado, a necessidade de notificação da empresa pela AF para o atendimento ao cliente;

Transição *Notificar Empresa* - Essa transição é habilitada e disparada com a marcação do lugar *Notificação*, exigindo da empresa o atendimento ao cliente;

Lugar *Empresa Notificada* - Esse lugar, determina quando marcado, a notificação da empresa pela autoridade fiscalizadora e habilita a transição de atendimento ao cliente por notificação;

Transição *Atender Cliente por Notificação* - Ao ser disparada, essa transição de-

termina que o atendimento à requisição do cliente foi feito através de uma notificação da AF. Tanto o atendimento através da autoridade de aviso como pela autoridade fiscalizadora, marcam o lugar *Requisição Cliente*;

Lugar *Requisição Cliente* - Esse lugar quando marcado, determina que o atendimento à requisição do cliente foi feito, permitindo o disparo da transição *Enviar Requisição*;

Transição *Enviar Requisição* - Ao ser disparada, essa transição remete ao cliente o recibo de sua requisição (RR). Nesse estágio, supõe-se que a protocolação da requisição do cliente já tenha sido feita junto à autoridade de datação;

Lugar *Requisição Atendida* - Com a marcação desse lugar, pode-se concluir que a requisição do cliente foi atendida de uma forma ou de outra e que os problemas de comunicação com a empresa foram resolvidos.

6.3.3 Cliente não responde

A rede de Petri da figura 6.4, mostra o comportamento do SAC seguro quando o cliente não responde à solicitação de fechamento da ordem de serviços. Por eventuais problemas de comunicação e também para garantir a ciência dos participantes em relação aos acontecimentos dentro do protocolo, a autoridade de aviso é empregada também nesse caso. A seguir, são detalhados todos os lugares e transições dessa rede conforme mostrados na figura para uma melhor compreensão do modelo apresentado:

Lugar *Cliente não responde* - Esse lugar, com sua marcação inicial, dispara o processo para o acionamento da AA;

Transição *Acionar AA* - a exemplo do que ocorre com a empresa, a autoridade de aviso é acionada para tentar estabelecer a comunicação com o cliente;

Lugar *Solicitação Empresa* - Acusa quando marcado, que existem uma solicitação da empresa para contato com o cliente na autoridade de aviso;

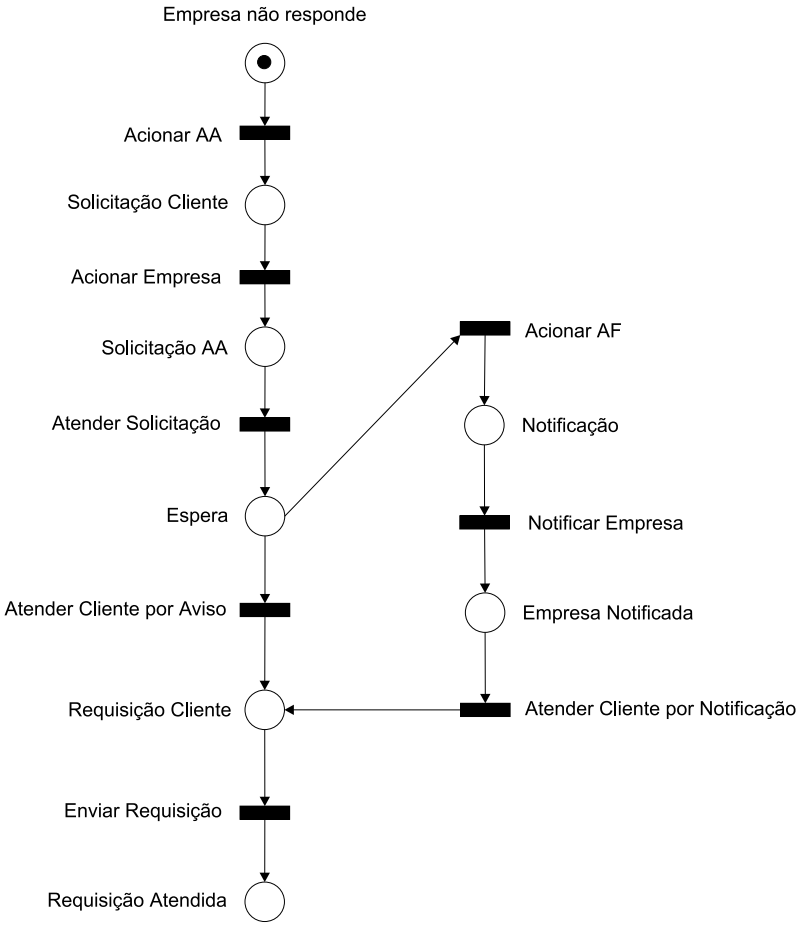

Figura 6.3: Empresa não responde ao cliente. Modelo da rede que trata da negação de resposta ou negligência da empresa ao atendimento ao cliente.

Transição *Acionar Cliente* - A AA tenta de todas as formas possíveis comunicar-se com o cliente gerando uma solicitação para o atendimento à empresa e marcando o lugar *Solicitação AA*;

Lugar *Solicitação AA* - Determina, quando marcado que o cliente recebeu uma solicitação da AA e que deve atendê-la respondendo para a empresa;

Transição *Atender Solicitação* - Essa transição é habilitada pela lugar *Solicitação AA*, representa a atitude do cliente em relação a solicitação feita e marca o lugar *Espera*;

Lugar *Espera* - Esse lugar, quando marcado acusa o aguardo da manifestação do cliente em relação a solicitação feita. Habilita as transições *Fechar OS* e *Decurso de Prazo*;

Transição *Decurso de Prazo* - Caso o tempo de resposta do cliente em relação a solicitação feita seja maior que o configurado no sistema, essa transição é disparada e o fechamento da OS ocorre;

Transição *Fechar OS* - Tendo o cliente se manifestado com relação ao aviso antes que o prazo de espera para o fechamento da OS se esgote, ele poderá analisar o serviço realizado e fechar a OS, marcando como saída o lugar *OS Assinada*;

Lugar *OS Assinada* - Determina quando marcado, que a ordem de serviço foi aceita e assinada pelo cliente e habilita o disparo da transição *Remeter Fechamento*;

Transição *Enviar Fechamento* - Realiza quando disparada, o despacho do recibo de fechamento para a empresa (RF), marcando como saída o lugar *OS Fechada*;

Lugar *OS Fechada* - Indica quando marcado que uma ordem de serviço foi fechada por intermédio da AA, dentro do prazo estipulado pelo sistema com a interação do cliente ou por decurso de prazo.

6.3.4 Litígio

Por último, porém não menos importante, a rede de Petri da figura 6.5, mostra o comportamento do SAC seguro quando, após o aceite de um serviço pela empresa e a emissão do recibo de requisição, a mesma não cumpre o prazo para atendimento da solicitação do cliente, ou ainda, exista qualquer outra divergência na transação realizada entre as partes. A seguir, são detalhados todos os lugares e transições dessa rede conforme mostrados na figura para uma melhor compreensão do modelo apresentado:

Lugar *Litígio* - É a marcação inicial da rede, representando a existência de um processo de reclamação e habilitando o disparo da transição de acionamento da autoridade fiscalizadora (AF);

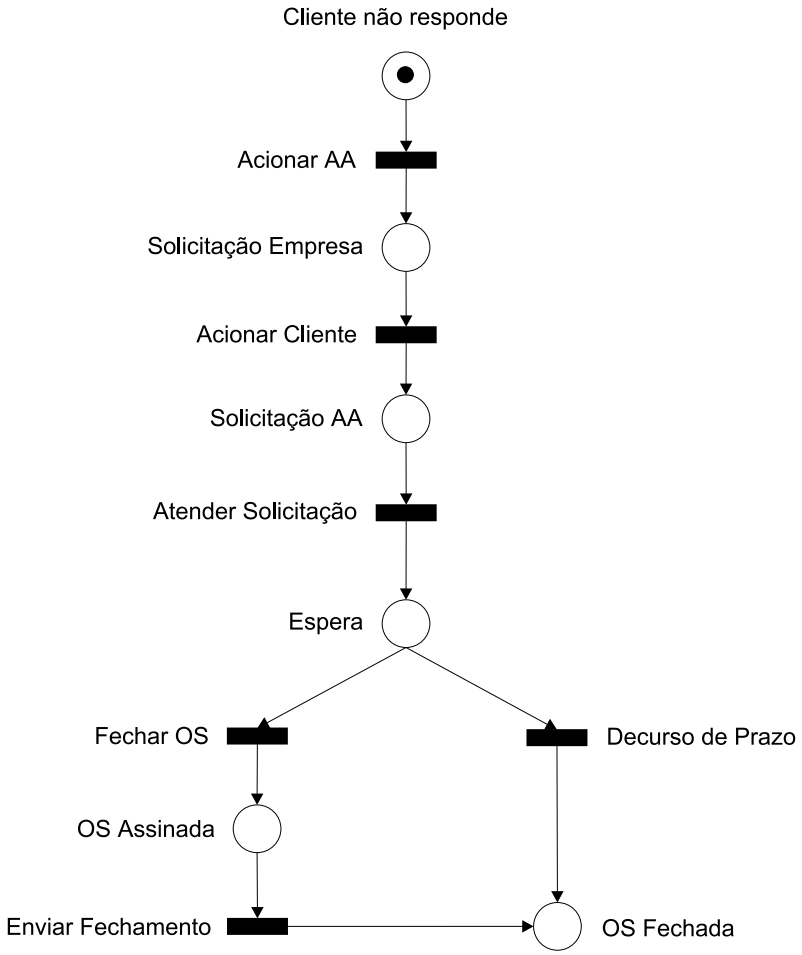

Figura 6.4: Cliente não responde à empresa. Modelagem da rede que contempla a notificação do cliente através da autoridade de aviso.

Transição *Acionar AF* - Representa quando habilitada, a geração de uma ocorrência de reclamação que dá origem à uma solicitação de um cliente;

Lugar *Solicitação Cliente* - Indica quando marcado que houve uma ocorrência de reclamação disparando o processo de acionamento da empresa;

Transição *Acionar Empresa* - É disparada pela marcação do lugar *Solicitação Cliente*, representando o contato da AF com a empresa e marca o lugar *Solicitação AF*;

Lugar *Solicitação AF* - Acusa quando marcado a existência de uma notificação da empresa por parte da autoridade fiscalizadora;

Transição *Atender Cliente* - Representa quando disparada o atendimento da solicitação

encaminhada pela AF. Pode ser a resolução de um problema com a ordem de serviço do cliente ou até mesmo o atendimento, caso esse ainda não tenha ocorrido. Marca o lugar *Fechamento OS* na saída;

Lugar *Fechamento OS* - Determina quando marcado que a pendência do litígio foi resolvida e habilita a transição do envio do fechamento para o cliente;

Transição *Enviar Fechamento* - Despacha quando disparada, o fechamento da solicitação do cliente;

Lugar *OS Fechada* - Acusa quando marcado, que ocorreu um litígio entre o cliente e a empresa, sendo resolvido com a intervenção da autoridade fiscalizadora.

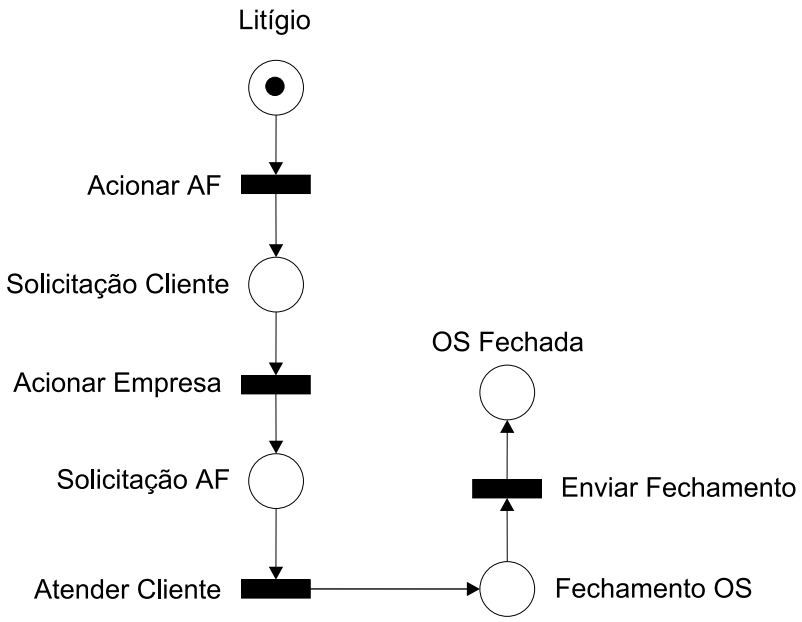

Figura 6.5: Litígio. Modelagem da rede que estuda o fluxo de informações e mensagens em questões litigiosas entre o cliente e a empresa.

6.4 Análise dos Resultados

As redes de Petri apresentadas na seção 6.3.1, tiveram suas propriedades analisadas no *software* ARP 2.4 que emitiu para cada uma delas um diagnóstico. Com a utilização deste programa pôde-se verificar a consistência e as características das

redes modeladas em todas as fases do protocolo proposto. As especificações das redes de acordo com a sintaxe do programa **ARP 2.4**, que geraram esses resultados estão no anexo B. As propriedades principais analisadas de cada rede estão descritas abaixo segundo o manual do programa [dCeML 89]:

Limitação - é calculado o número máximo de fichas (limite) em cada lugar da rede, para os estados alcançáveis. Os lugares podem ser nulos, quando nunca receberam fichas; binários, sempre possuindo uma ou nenhuma ficha; limitados, quando o número de fichas é sempre igual ou inferior a um limite finito maior que 1 ou não-limitados, quando o número de fichas tende ao infinito (simbolizado por w). Caso sejam detectados lugares não-limitados são indicadas as seqüências de disparos de transições que levam ao crescimento de fichas nesses lugares;

Conservação - é verificado se a soma total de fichas na rede é constante para qualquer marcação alcançável, indicando se a rede é estritamente conservativa ou não;

Vivacidade - este teste é relativo ao disparo das transições. Uma transição é viva se, a partir de qualquer estado do grafo gerado, existe uma seqüência de disparos que a contenha, ou seja, que leve a seu disparo. Uma transição é quase-viva se foi disparada ao menos uma vez durante a construção do grafo;

Reiniciação - a rede é reiniciável se todos os seus estados forem reiniciáveis. Um estado é reiniciável se, partindo dele, existe alguma seqüência de disparos de transições que leve de volta ao estado inicial;

Deadlock - um estado em deadlock está bloqueado, não possuindo nenhuma transição sensibilizada e portanto nenhum estado sucessor. Caso sejam detectados deadlocks na rede, são indicadas as seqüências de disparos de transições que levam aos mesmos.

6.4.1 Rede SAC Seguro modelado

Conforme a avaliação pelo software utilizado, a rede de Petri que representa o protocolo proposto como um todo, obteve os seguintes resultados:

```
State Enumeration : net Protocolo (20 reachable states).

Verified properties: *-----------------------------------*

Net under analysis is binary.
  Null places (M = 0): {aviso_cliente, empresa_aci,
                        espera, reclamacao, req_atraso,
                        req_prazo}
  Binary places      : {cliente, Web_site_disp, FEC,
                        FEC_banco_AF, FEC_cliente,
                        OS_concluida, OS_fechada,
                        OS_prod, OS_prot, req_cliente,
                        RF, RR, RR_banco_AF, RR_cliente}
  k-Bounded places   : {}
  Unbounded places   : {}

Net under analysis is not strictly conservative.

Net under analysis is not live.
  Live Tr.          : {}
  "Almost-live" Tr.: {assinar_FEC, executar_OS,
                      gerar_OS, protocolar_FEC,
                      protocolar_OS, remeter_FEC,
                      remeter_RF, remeter_RR,
                      requisitar_servico}
  Non-fired Tr.     : {acionar_AA, acionar_empresa,
                      concluir_req_atraso,
                      concluir_req_prazo,
                      disparar_reclamacao}

Net never can go back to M0.

No live-locks detected.

States (and fire sequencies) in deadlock:
  M9   :requisitar_servico gerar_OS executar_OS
        protocolar_FEC protocolar_OS remeter_FEC
        assinar_FEC remeter_RF remeter_RR
*-----------------------------------------*
```

Avaliando-se o apresentado pelo *software*, é possível observar algumas características da rede em questão conforme apresentado na tabela 6.1 abaixo:

6.4.2 Rede Empresa não responde

Conforme a avaliação pelo software utilizado, a rede de Petri que representa a ação do protocolo quando a empresa não responde ao cliente dentro do tempo determi-

nado, obteve os seguintes resultados:

```
State Enumeration : net Empresa_nao_responde (8 reachable states).

Verified properties: *-----------------------------------*

Net under analysis is binary.
  Null places (M = 0): {}
  Binary places      : {all}
  k-Bounded places   : {}
  Unbounded places   : {}

Net under analysis is strictly conservative.

Net under analysis is not live.
  Live Tr.          : {}
  "Almost-live" Tr.: {all}
  Non-fired Tr.     : {}

Net never can go back to M0.

No live-locks detected.

States (and fire sequencies) in deadlock:
  M7   :acionar_AA acionar_empresa atender_solicitacao
        acionar_AF notificar_empresa
        atender_cliente_not enviar_RR
*-------------------------------------------*
```

Avaliando-se o apresentado pelo *software*, é possível observar algumas características da rede em questão conforme apresentado na tabela 6.2 abaixo:

6.4.3 Rede Cliente não responde

Conforme a avaliação pelo software utilizado, a rede de Petri que representa a ação do protocolo quando o cliente não atende a solicitação de fechamento da ordem de serviço da empresa, obteve os seguintes resultados:

```
State Enumeration : net Cliente_nao_responde (6 reachable states).

Verified properties: *-----------------------------------*

Net under analysis is binary.
  Null places (M = 0): {}
  Binary places      : {all}
  k-Bounded places   : {}
  Unbounded places   : {}

Net under analysis is strictly conservative.

Net under analysis is not live.
  Live Tr.          : {}
```

```
  "Almost-live" Tr.: {all}
  Non-fired Tr.    : {}

Net never can go back to M0.

No live-locks detected.

States (and fire sequencies) in deadlock:
  M4   :acionar_AA acionar_cliente
        atender_solicitacao decurso_prazo
*-----------------------------------------*
```

Avaliando-se então o apresentado pelo *software*, é possível observar algumas características da rede em questão conforme apresentado na tabela 6.3 abaixo:

6.4.4 Rede Litígio

Conforme a avaliação pelo software utilizado, a rede de Petri que trata da resolução de litígios entre as partes, obteve os seguintes resultados:

```
State Enumeration : net Litigio (5 reachable states).

Verified properties: *-----------------------------------*

Net under analysis is binary.
  Null places (M = 0): {}
  Binary places      : {all}
  k-Bounded places   : {}
  Unbounded places   : {}

Net under analysis is strictly conservative.

Net under analysis is not live.
  Live Tr.         : {}
  "Almost-live" Tr.: {all}
  Non-fired Tr.    : {}

Net never can go back to M0.

No live-locks detected.

States (and fire sequencies) in deadlock:
  M4   :acionar_AF acionar_empresa atender_cliente
        enviar_fechamento
*-----------------------------------------*
```

Avaliando-se então o apresentado pelo *software*, é possível observar algumas características da rede em questão conforme apresentado na tabela 6.4 abaixo:

6.5 Conclusão

O emprego das redes de Petri proporcionaram um estudo matemático e determinístico do funcionamento do protocolo proposto. As propriedades estudadas das redes modeladas tornaram a proposta do SAC Seguro mais consistente.

Tabela 6.1: Principais características da rede do Sac Seguro modelado. Conforme os resultados apontados pelo programa utilizado para a análise da rede, pode-se destacar as características abaixo:

Característica Avaliada	**Observação**
Limitação	Binária, pois os lugares representam apenas valores booleanos
Conservação	Sim, pois seus lugares são limitados
Vivacidade	Não, pois a rede não é reiniciável
Reiniciação	Não, pois analisando o grafo da rede pode-se observar que as marcações iniciais **Cliente** e **Web site disponível** não recebem nenhuma entrada de outro caminho por se desejar verificar a rede com a entrada de apenas uma requisição
DeadLock	As transições **requisitar_servico, gerar_OS, executar_OS, protocolar_FEC, protocolar_OS, remeter_FEC, assinar_FEC, remeter_RF** e **remeter_RR** apresentam avisos da possibilidade de deadlock, entretanto, pela estrutura e características da rede eles não serão alcançados em nenhum momento

Tabela 6.2: Principais características da rede Empresa não responde. Conforme os resultados apontados pelo programa utilizado para a análise da rede, pode-se destacar as características abaixo:

Característica Avaliada	**Observação**
Limitação	Binária, pois os lugares representam apenas valores booleanos
Conservação	Sim, pois seus lugares são limitados
Vivacidade	Não, pois a rede não é reiniciável
Reiniciação	Não, pois analisando o grafo da rede pode-se observar que a marcação inicial **Empresa não responde**não recebe nenhuma entrada de outro caminho por se desejar verificar a rede com a entrada de apenas uma requisição
DeadLock	As transições **acionar_AA, acionar_empresa, atender_solicitacao, acionar_AF, notificar_empresa, atender_cliente_not** e **enviar_RR** apresentam avisos da possibilidade de deadlock, entretanto, pela estrutura e características da rede eles não serão alcançados em nenhum momento

Tabela 6.3: Principais características da rede Cliente não responde. Conforme os resultados apontados pelo programa utilizado para a análise da rede, pode-se destacar as características abaixo:

Característica Avaliada	**Observação**
Limitação	Binária, pois os lugares representam apenas valores booleanos
Conservação	Sim, pois seus lugares são limitados
Vivacidade	Não, pois a rede não é reiniciável
Reiniciação	Não, pois analisando o grafo da rede pode-se observar que a marcação inicial **Cliente não responde**não recebe nenhuma entrada de outro caminho por se desejar verificar a rede com a entrada de apenas uma requisição
DeadLock	As transições **acionar_AA, acionar_cliente, atender_solicitacao** e **decurso_prazo** apresentam avisos da possibilidade de deadlock, entretanto, pela estrutura e características da rede eles não serão alcançados em nenhum momento

Tabela 6.4: Principais características da rede Litígio. Conforme os resultados apontados pelo programa utilizado para a análise da rede, pode-se destacar as características abaixo:

Característica Avaliada	**Observação**
Limitação	Binária, pois os lugares representam apenas valores booleanos
Conservação	Sim, pois seus lugares são limitados
Vivacidade	Não, pois a rede não é reiniciável
Reiniciação	Não, pois analisando o grafo da rede pode-se observar que a marcação inicial **Litígio** não recebe nenhuma entrada de outro caminho por se desejar verificar a rede com a entrada de apenas uma requisição
DeadLock	As transições **acionar_AF, acionar_empresa, atender_cliente** e **enviar_fechamento** apresentam avisos da possibilidade de deadlock, entretanto, pela estrutura e características da rede eles não serão alcançados em nenhum momento

Capítulo 7

Considerações Finais

Com os estudos realizados para a elaboração deste trabalho, pôde-se observar uma nova perspectiva para o atendimento aos clientes através de um meio eletrônico que é a *Internet*. Por se tratar de uma tecnologia nova, se comparada com as formas tradicionais de relacionamento entre empresas e clientes, muitas questões ainda precisam ser avaliadas, entre elas, a segurança.

Uma revisão bibliográfica sobre a qualidade no atendimento aos clientes e métodos tradicionais utilizados foi de grande importância para que se pudesse estampar nas características do protocolo proposto tais qualidades.

Tratando-se de um ambiente eletrônico para a troca de mensagens e informações confidenciais, a infra-estrutura de chaves públicas e as técnicas de criptografia e segurança, permitiram definir um protocolo de atendimento ao cliente seguro.

Sabe-se que em muitos casos a implantação do protocolo será arbitrada para empresas que tenham suas atividades ou concessões de serviços controladas pelo governo. Entretanto, a utilização do mesmo é altamente recomendada para todas as empresas que tenham compromissos verdadeiros com a qualidade dos serviços prestados. Nesses casos, as autoridades fiscalizadoras poderão ser os setores de qualidade das próprias empresas.

Conforme os objetivos iniciais dessa dissertação, pode-se tecer os seguintes co-

mentários e conclusões:

- O entendimento dos modelos de relacionamento entre empresas e clientes, permitiu a compreensão de que o sucesso das empresas e satisfação dos clientes é diretamente proporcional ao compromisso com a qualidade;
- Muitos problemas no relacionamento entre clientes e empresas são resultantes da negligência, omissão e até mesmo da discriminação do cliente, o que compromete seriamente a qualidade do atendimento e a imagem da empresa;
- O estudo dos modelos empregados pelas empresas e disponibilizados para o cliente no atendimento, suporte e pós-venda demonstrou serem eficientes. Entretanto, a não continuidade ou falta de manutenção em tais serviços poderá ser um aspecto negativo;
- Os modelos de comércio foram estudados e os riscos do comércio eletrônico pela *Internet* foram avaliados do ponto de vista do cliente e do comerciante;
- O direito dos consumidores em transações eletrônicas e a legalidade das provas, assim como a legislação inerente à esses casos foram abordados e compreendidos;
- Foram realizados estudos sobre as tecnologias de segurança eletrônica de dados, protocolos criptográficos e de criptografia, sendo entendidas as vulnerabilidades, as ameaças e os riscos de ataques e ainda os requisitos de segurança;
- Foram estudadas as técnicas para a análise e especificação de protocolos, onde os padrões PKCS de chave pública e a linguagem ASN.1 foram destacadas como quesitos importantes para a implementação do protocolo proposto nesse trabalho;
- Foi proposto o SAC seguro para a aplicação no atendimento à clientes através de transações eletrônicas com garantias de qualidade de serviço e auditoria;
- Foram estudadas as fases do SAC seguro e avaliadas as mensagens trocadas entre os participantes para a garantia dos requisitos de segurança. Os proble-

mas de comunicação e o ataque do homem do meio foram também considerados dentro dos padrões de segurança inicialmente estabelecidos;

- Foram definidas as mensagens a serem trocadas entre os participantes, porém, uma definição formal das mesmas utilizando a linguagem ASN.1, se faz necessária para permitir a implementação do protocolo;
- O protocolo foi modelado utilizando-se as técnicas das redes de Petri para se verificar as suas propriedades e robustez.

Finalmente, sabe-se que atualmente muitos clientes que poderiam ser usuário de um SAC seguro como o proposto nesse trabalho, ainda não tem acesso a grande rede. Todavia, isso é apenas uma questão de tempo e cultura. Deve-se também considerar que o SAC seguro é mais uma ferramenta de apoio para o atendimento com garantia de qualidade aos clientes e que não substitui as outras já utilizadas pelas empresas.

A garantia dos diretos e a qualidade dos serviços prestados aos consumidores através de sistemas de atendimento seguro é um tema amplo e ainda há muito para ser discutido. Esse trabalho não tem a pretensão de esgotar o assunto acerca deste tema, pelo contrário, no decorrer de seu desenvolvimento pôde-se observar várias possibilidades de trabalhos futuros para complementá-lo. A partir das propostas apresentadas, pode-se vislumbrar alguns trabalhos futuros como:

- Implementação do protocolo proposto para uso comercial por empresas e repartições públicas;
- Estudo dos aspectos legais das relações de consumo entre clientes e empresas avaliando-se as características do protocolo;
- Propor a adoção do protocolo após a sua implementação como ferramenta oficial de órgãos governamentais para a monitoração de empresas concessionárias de serviços públicos com o estudo de caso de algumas instituições;

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.

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

[CAR 97] CARDOSO, J.; VALETTE, R. **Redes de Petri**. Editora da UFSC, 1.997.

[CAR 00] CARVALHO, D. B. **Segurança de Dados Com Criptografia: Métodos e Algoritmos**. Rio de Janeiro, RJ: Editora Book Express Ltda, 2000.

[CAR 01] CARVALHO, D.; CIANCIO, P. Mensagem para você. **INTERNET BUSINESS - A Revista de Negócios da Rede**, [S.l.], v.45, p.47–55, Maio, 2001.

[COR 94] CORTADA, J. W.; DE MEIRELLES QUINTELLA, H. L. M. **TQM: Gerência Da Qualidade Total**. Makron Books, São Paulo, SP, 1994.

[dCeML 89] DE CONTROLE E MICROINFORMÁTICA (LCMI), L. **ARP - Analisador/Simulador de Redes de Petri**. Departamento de Engenharia Elétrica Da Universidade Federal de Santa Catarina, 1989.

[DEN 90] DENTON, D. K. **Qualidade Em Serviços: O Atendimento Ao Cliente Como Fator de Vantagem Competitiva**. McGraw-Hill, São Paulo, SP, 1990.

[dHF 99] DE HOLANDA FERREIRA, A. B. **Novo Aurélio Século XXI: O Dicionário Da Língua Portuguesa**. 3ł. ed. Rio de Janeiro, RJ: Editora Nova Fronteira S.A, 1999.

[dM 94] DE MOURA, J. A. M. **Os Frutos Da Qualidade: A Esperiência Da Xerox Do Brasil**. 2ł. ed. Makron Books, São Paulo, SP, 1994.

[dR 00] DE ROLT, C. R. **O Desenvolvimento Da Comunidade Virtual: Uma Proposta Para a Melhoria Da Qualidade e Da Comercialização de Software**. Universidade Federal de Santa Catarina, 2000. Tese de Doutorado.

[FIL 99] FILHO, V. B. **ISO 9000 Em Serviços: Um Passo Para a Qualidade Total**. Makron Books, 1999.

[GAR 99] GARFINKEL, S.; SPAFFORD, G. **Comércio e Segurança Na Web**. Market Press, São Paulo, SP, 1999.

[GRI 99] GRITZALIS, S.; SPINELLIS, D.; GEORGIADIS, P. Security protocols over open networds and distributed systems: Formal methods for their analysis, design and verification. **Computer Communications - ELSEVIER**, [S.l.], v.22, p.697–709, 1999.

[JR. 93] JR., B. S. K. **An Overview of The PKCS Standards**. Definição de padrões para o emprego e implementação de diversas tecnologias de segurança, como assinaturas digitais, certificados digitais, troca de chaves públicas, etc...

[JUR 95] JURAN, J. M. **Juran Planejando Para a Qualidade**. Pioneira, 1995.

[LEE 97] LEE, G.-S.; LEE, J.-S. Petri net based models for specification and analysis of cryptographic protocols. **J. Systems Software**, [S.l.], v.37, p.141–159, 1997.

[PAE 99] PAESANI, L. M. **Direito de Informática : Comercialização e Desenvolvimento Internacional Do Software**. Atlas, 1999.

[PAL 00] PALADINI, E. P. **Gestão Da Qualidade: Teoria e Prática**. Atlas, 2000.

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

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

[SHI 93] SHIOZAWA, R. S. C. **Qualidade No Atendimento e Tecnologia Da Informação**. Atlas, São Paulo, SP, 1993.

[SOA 95] SOARES, L. F. G.; LEMOS, G.; COLCHER, S. **Redes de Computadores: Das LANs, MANs e WANs Às Redes ATM**. 7ł. ed. Campus, Rio de Janeiro, RJ, 1995.

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

[TAN 97] TANENBAUM, A. S. **Redes de Computadores**. 5ł. ed. Campus, Rio de Janeiro, RJ, 1997.

[WHI 99] WHITELEY, R. C. **A Empresa Totalmente Voltada Para O Cliente**. Campus, São Paulo, SP, 1999.

Apêndice A

Correspondências Eletrônicas

Durante o desenvolvimento do trabalho, ocorreram muitas trocas de informação com diversos profissionais das áreas estudadas e um desses contatos realizados foi com a ombudsman da Petrobrás (Sra. Vera Marelim) que tratou das questões relacionadas ao tema com muita propriedade. O documento apresentado por ela segue na íntegra abaixo:

"Prezado Amauri,

Excelente o tema escolhido para desenvolver como dissertação. A importância da escolha está no fato de representar uma contribuição científica inovadora para a área de Atendimento a Clientes, ainda pouco explorada academicamente. Constatamos que não há disciplina específica para a matéria, nas grades curriculares das universidades.

Encontramos obras publicadas sobre atendimento a clientes que se apresentam mais empíricas do que científicas. De fato, as experiências vêm se dando de forma bastante individualizada, caso a caso, e, então, transmitida por seus protagonistas, conforme suas peculiaridades.

Vejo o seu viés de pesquisa como uma das várias abas de um leque. Pois, pude verificar, ao longo desses dois anos à frente do Ombudsman da Petrobrás Distribuidora S.A., que a Internet tem se demonstrado um forte aliado da comunicação com os

clientes; entretanto, considerando a comunidade ainda restrita de internautas, é, via de conseqüência, um canal limitado.

Feitas as considerações acima, e à parte questões inerentes às especificidades tecnológicas da Internet (segurança, sigilo na transmissão de dados e confiabilidade de dados recebidos), passo a tecer alguns comentários quanto ao atendimento a clientes propriamente dito.

Alguns fatores são indispensáveis para que um serviço de atendimento a clientes funcione a contento. O critério para elencá-los num mesmo rol dá-se quando nos propomos estar, ainda que momentaneamente, no ”lugar do outro”. Assim, fica mais fácil identificar quais são as necessidades do cliente e procurar atendê-las, na medida do que se apresente razoável.

Dito isto, vamos analisar um caso hipotético (considerando que o cliente somente poderia contatar o Serviço de Atendimento ou o Ombudsman pela Internet), de modo a visualizar a exposição acima: um cliente encomenda determinado produto, mas, por questões alheias à vontade do fornecedor, o produto não será entregue. O fornecedor não sabe que alternativa apresentar ao cliente, que por falta de informação por parte do contato direto (vendedor= ”ponta da linha”) e por se considerar mal atendido, busca a última instância, entrando em contato com o Ombudsman (via Internet), onde pede ajuda para o caso, pois necessita do produto num prazo exíguo. Como se daria o atendimento, ou melhor, como se daria o tratamento dessa manifestação(*)?

Passemos à análise do caso, por partes:

1) O cliente contatou o Ombudsman pela Internet, através de um link mantido no sítio da empresa (FALE COM OMBUDSMAN).

O cliente necessita de um atendimento ágil porque tem prazo exíguo para receber seus insumos e cumprir os prazos de entrega da produção. Ora, haverá que se pensar em manter um monitoramento constante da entrada desse tipo de mensagem (*e-mails*).

Se a Internet é a única via de acesso, como poderia ser melhor divulgada. Um caminho seria manter banners em outras homepages, de modo a que mais internautas descobrissem a forma de acesso. Ou mesmo ostensiva propaganda de midia.

2) Após contatar, necessita confirmação de que foi ”ouvido”.

Como?

O cliente tem pressa em ser atendido, então, de plano, recebe um *e-mail* informando-lhe que sua manifestação foi recebida e que estará sob análise da área afim, para análise e resposta no prazo mais breve possível (= resposta automática).

Quando? Por quanto tempo deverá aguardar resposta?

Se a empresa optar por estabelecer prazo para resposta (p.e. 24 h), este deverá ser informado ao cliente e atentar para que seja rigorosamente respeitado, sob pena de perder a confiança dos clientes que buscam essa forma de acesso.

3) O cliente tem pressa.

Em quanto tempo a empresa é capaz de monitorar as entradas de manifestações e dar efetivo tratamento, de maneira a retornar com respostas concretas ao cliente?

A credibilidade no trabalho advém da capacidade de respostas ágeis e efetivas por parte da empresa. Não basta que a resposta seja dada em 24h ao cliente, mas que, principalmente, seja satisfatória ou tenda a ser.

Se não houver prazo estabelecido, ainda que a resposta automática tenha sido recebida, que a resposta efetiva ao cliente após o tempo necessário para sua análise e elaboração tente esgotar as questões colocadas pelo cliente.

4) A empresa responde ao cliente. Satisfatoriamente? Sim? Não?

A empresa responde satisfatoriamente e a manifestação pode ser dada por encerrada. Neste caso, não há desdobramentos. Encerra-se após o feedback positivo do cliente (que pode ser obtido pela solicitação de contato por meio eletrônico, ou contato telefônico - neste caso fugindo um pouco ao escopo do seu trabalho).

Entretanto, se a resposta for insatisfatória, há um novo input. A manifestação está

inacabada, sua solução está suspensa por conta de a primeira tentativa não ter logrado êxito.

Nesse caso, a manifestação dá novamente entrada como um novo case, o que possibilitará à empresa dar tratamento normal, inclusive, quanto ao prazo para solução, que será reaberto. Isso deverá estar claro para o cliente, a fim de que ele não perca a confiança no serviço, reputando-o de fachada.

A credibilidade do público é fundamental para o êxito dessa atividade. E credibilidade só se adquire transparecendo-a. Não há fórmula mágica para isso, ou se respeita o cliente de fato, ou não. Não há como se manter um meio termo. A resposta pública é imediata e pode ser implacável.

Se o serviço de atendimento não for bem conduzido e perder a credibilidade do público, dificilmente se manterá no mercado.

5) De quanto tempo o cliente dispõe para esperar?

Outra questão importantíssima, antes de se ”enquadrar”o cliente na burocracia cibernética da empresa é perqüirir qual a urgência e real necessidade do cliente e, de fato, de quanto tempo pode esperar pela solução a ser encontrada pela empresa.

Agilizar o retorno das respostas é procedimento padrão. Entretanto, dadas as características da demanda, a resposta deverá ser providenciada em tempo recorde. Isso é muito importante para o cliente. O tempo de resposta a um cliente é diretamente proporcional ao nível de importância que ele crê ser dado à sua manifestação. Muitas vezes a empresa pode até estar providenciando a solução do problema ou mesmo já o solucionou, contudo, é preciso que o cliente saiba disso, pois, caso contrário a empresa pode deixá-lo com a má impressão de que não está sendo dispensada a devida atenção ao seu caso. Esse feedback pode se dar por *e-mail*, haja vista que na hipótese em questão o único acesso é via Internet.

Questões de fundo

Deixo aqui alguns pontos para sua reflexão científica, vez que não me caberia argumentar numa área, cujo conhecimento não me é peculiar. Mas, diante de alguma

experiência que vimos acumulando, permito-me lançar os seguintes questionamentos que poderão ser respondidos, se pertinentes, por sua pesquisa científica:

1) Manter o acompanhamento em workflow? Apenas em meio magnético? Como fazer para manter o sistema 24 horas no ar, minizando panes e problemas de máquina, que geram as famosas frases ”desculpe, mas o nosso sistema está fora do ar”?

2) Como lidar com os solucionadores (=empregados responsáveis por providenciar a solução das manifestações registradas)? Manter contato com os solucionadores somente por meio magnético? E como registrar os andamentos (questão 1.ł - worflow)?

3) Como manter o feedback ao cliente?

4) Necessidade de apoio à atividade de serviço de atendimento a clientes por parte dos colegas (demais empregados) e da alta direção da companhia. Como é encarado o serviço de atendimento pelo público interno (empregados)? Qual o respaldo conferido pela alta direção ao trabalho desenvolvido pelo serviço de atendimento?

5) Qual a temática mais comum das demandas encaminhadas via Internet? Como quantificá-las? O programa elaborado para atender a esse tipo de atividade é capaz de gerar relatórios regulares (mensais, de preferência)?

6) Idoneidade da origem da demanda. Como medir a seriedade com que alguém nos escreve? *E-mails* ”laranjas”(= *e-mail* criado apenas para registrar determinada manifestação, normalmente em provedor gratuito, sem compromisso com a verdadeira identidade do demandante ou com a realidade dos fatos).

O trabalho que você propõe visa a atender clientes, via Internet, de forma segura e confiável e, assim, garantir a qualidade dos serviços prestados pelas empresas.

Baseada nisso, sugiro mais alguns pontos de reflexão, que poderiam estar contidos num capítulo de sua obra dissertativa, à medida que fossem sendo pesquisadas e evidenciadas, compondo a estrutura abaixo.

FATORES ENVOLVIDOS NO ATENDIMENTO A CLIENTES (A).

Vale a pena avaliar certas questões preliminares: um excelente serviço de atendimento a clientes (departamento integrante do organograma da empresa), por si só, garante a qualidade dos serviços prestados e/ou produtos fornecidos pela empresa? O atendimento ao cliente só se restringiria ao departamento responsável por isso ou se estenderia a todo aquele empregado que atendesse um cliente, gerando um compromisso do grupo, passando a transparecer a filosofia da empresa?

FATORES ENVOLVIDOS NA GARANTIA DE QUALIDADE DOS SEVIÇOS PRESTADOS PELAS EMPRESAS (B).

(A) (B)

OBS.: PROPOSTA DO QUADRO COMPARATIVO. Após cotejar as colunas em que estarão elencados os fatores que influem nos aspectos propostos, poder-se-á constatar algumas conclusões sobre a relação entre o setor de atendimento a clientes da empresa e a qualidade dos serviços prestados por ela, buscando extrair conclusões, sem exaurir possibilidades ou horizontes, apenas constatar, para então criar espaço para traçar perspectivas.

Quanto à indagação de quantitativos, pensamos que quantificar não se torna a questão principal, pois seja lá qual for o número de atendimentos, a qualidade destes deverá seguir um padrão pré-estabelecido.

Coloco-me à sua disposição para continuarmos a trocar idéias sobre seu projeto de pesquisa."

Apêndice B

Especificação das redes no ARP 2.4

Neste anexo são apresentadas as especificações das redes avaliadas no **ARP 2.4** de acordo com a sintaxe do *software*.

B.1 Rede Protocolo

```
Net Protocolo;

Nodes
  cliente,
  Web_site_disp             : Place (1);

  req_cliente,
  OS_prot,
  OS_prod,
  RR,
  RR_banco_AF,
  RR_cliente,
  req_prazo,
  req_atraso,
  OS_concluida,
  FEC,
  FEC_banco_AF,
  FEC_cliente,
  RF,
  OS_fechada,
  espera,
  reclamacao,
  aviso_cliente,
  empresa_aci               : Place;

  requisitar_servico,
  gerar_OS,
  protocolar_OS,
  remeter_RR,
```

```
  concluir_req_prazo,
  executar_OS,
  protocolar_FEC,
  remeter_FEC,
  assinar_FEC,
      remeter_RF,
  disparar_reclamacao,
  acionar_AA,
  acionar_empresa,
  concluir_req_atraso      : Transition;

Structure

  requisitar_servico  : (cliente,Web_site_disp) , (req_cliente);
  gerar_OS            : (req_cliente)           , (OS_prot,OS_prod);
  protocolar_OS       : (OS_prot)               , (RR);
  remeter_RR          : (RR)                    , (RR_banco_AF,RR_cliente);
  concluir_req_prazo  : (RR_cliente,espera)     , (req_prazo);
  executar_OS         : (OS_prod)               , (OS_concluida);
  protocolar_FEC      : (OS_concluida)          , (FEC);
  remeter_FEC         : (FEC)                   , (FEC_banco_AF,FEC_cliente);
  assinar_FEC         : (FEC_cliente)           , (RF);
  remeter_RF          : (RF)                    , (OS_fechada);
  disparar_reclamacao : (espera)                , (reclamacao);
  acionar_AA          : (reclamacao)            , (aviso_cliente);
  acionar_empresa     : (aviso_cliente)         , (empresa_aci);
  concluir_req_atraso : (RR_cliente,empresa_aci), (req_atraso);

endNet.
```

B.2 Rede Empresa não responde

```
Net Empresa_nao_responde;

Nodes
  cliente_sem_resposta       : Place (1);
  solicitacao_cliente,
  solicitacao_AA,
  espera,
  notificacao,
  empresa_notificada,
  req_cliente,
  RR                         : Place;

  acionar_AA,
  acionar_empresa,
  atender_solicitacao,
  atender_cliente_aviso,
  acionar_AF,
  notificar_empresa
  atender_cliente_not,
  enviar_RR                  : Transition;

Structure

  acionar_AA            : (cliente_sem_resposta) , (solicitacao_cliente);
  acionar_empresa       : (solicitacao_cliente)  , (solicitacao_AA);
  atender_solicitacao   : (solicitacao_AA)       , (espera);
```

```
  atender_cliente_aviso : (espera)               , (req_cliente);
  acioanr_AF            : (espera)               , (notificacao);
  notificar_empresa     : (notificacao)          , (empresa_notificada);
  atender_cliente_not   : (empresa_notificada)   , (req_cliente);
  enviar_RR             : (req_cliente)          , (RR);

endNet.
```

B.3 Rede Cliente não responde

```
Net Cliente_nao_responde;

Nodes
  empresa_sem_resposta      : Place (1);
  solicitacao_empresa,
  solicitacao_AA,
  espera,
  OS_assinada,
  OS_fechada                : Place;

  acionar_AA,
  acionar_cliente,
  atender_solicitacao,
  fechar_OS,
  enviar_RF,
  decurso_prazo             : Transition;

Structure

  acionar_AA            : (empresa_sem_resposta) , (solicitacao_empresa);
  acionar_cliente       : (solicitacao_empresa)  , (solicitacao_AA);
  atender_solicitacao   : (solicitacao_AA)       , (espera);
  fechar_OS             : (espera)               , (OS_assinada);
  enviar_RF             : (OS_assinada)          , (OS_fechada);
  decurso_prazo         : (espera)               , (OS_fechada);

endNet.
```

B.4 Rede Litígio

```
Net Litigio;

Nodes
  cliente_insatisfeito : Place (1);
  solicitacao_cliente,
  solicitacao_AF,
  fechamento_OS,
  OS_fechada           : Place;

  acionar_AF,
  acionar_empresa,
  atender_cliente,
  enviar_fechamento    : Transition;
```

```
Structure

  acionar_AF        : (cliente_insatisfeito) , (solicitacao_cliente);
  acionar_empresa   : (solicitacao_cliente)  , (solicitacao_AF);
  atender_cliente   : (solicitacao_AF)       , (fechamento_OS);
  enviar_fechamento : (fechamento_OS)        , (OS_fechada);

endNet.
```

Apêndice C

Recomendações e Padrões

C.1 Introdução

Para a definição do protocolo proposto neste trabalho, serão utilizados padrões e recomendações internacionais. Tais padrões, tornam a leitura universal, facilitando a compreensão e permitindo a implementação do protocolo a qualquer momento.

Para as técnicas criptográficas assimétricas com uso de chave pública citadas no capítulo anterior, existem padrões que determinam as formas de implementação. Esses padrões, chamados PKCS (*Public Key Cryptography Standards* ou Padrões Criptográficos de Chave Pública) são representados formalmente em uma linguagem de Notação para Sintaxe Abstrata chamada ASN.1.

Os padrões concebidos e a descrição dos mesmos em ASN.1 permitem a definição formal de protocolos para diversas finalidades e de leitura universal, facilitando a implementação dos mesmos.

Neste anexo, será abordada na seção C.2 a linguagem de notação ASN.1 com suas características. A seção C.3, apresenta os padrões PKCS com suas respectivas finalidades.

C.2 ASN.1

ASN.1 é um acrônimo para *Abstract Syntax Notation One*, e é utilizada como uma linguagem para a descrição abstrata de tipos de dados e definição de protocolos de comunicação. Com a abstração[1] proporcionada por esta linguagem, pode-se especificar uma parte de um sistema sem se preocupar como de fato ele será implementado ou representado. Isto simplifica a especificação e permite se determinar axiomas a respeito de uma parte de um sistema, que podem ser comprovados, quando esta for implementada.

Um dos mais complexos sistemas atuais e que também utiliza um grande volume de abstração, é o sistema *OSI* (*Open Systems Interconnection*). OSI é uma arquitetura internacional padrão que regimenta a interconexão de computadores desde a camada física até a camada de aplicação. Objetos nas camadas altas são definidos de forma abstrata e combinados para serem implementados com os objetos das camadas baixas. O modelo OSI utiliza ASN.1 para a especificação desses objetos.

No caso da especificação de protocolos, o emprego do ASN.1 é importante, pois, permite a verificação sem que a implementação deste ocorra. Esta especificação é padronizada e de leitura universal, o que prolonga a validade de qualquer proposta de implementação.

C.2.1 Tipos e Valores

Para se entender melhor como o ASN.1 descreve tipos e valores, é necessário primeiramente, entendê-los. Um tipo é um conjunto de valores. Para alguns tipos existe um número limitado de valores, já para outros, este número pode ser infinito.

Os tipos e valores são definidos em ASN.1 com a utilização do operador de atribuição (::=). Tipos e valores criados podem também ser usados para a definição de outros.

[1] Ato de separar mentalmente um ou mais elementos de uma totalidade complexa [dHF 99].

Algumas características para a expressão de tipos e valores em ASN.1 devem ser observadas, apesar de serem bastante flexíveis:

- Indentação ou alinhamentos não são considerados. Múltiplos espaços e linhas em branco são considerados como um simples espaço;
- Comentários são delimitados por um par de hífens, ou um par de hífens e uma quebra de linha;
- Identificadores de valores e tipos podem ser compostos por letras maiúsculas e minúsculas, dígitos, hífens e espaços. Os valores começam com letra minúscula e os tipos com letras maiúsculas.

Em ASN.1 existem quatro espécies de tipos:

Tipo *Simple*: São atômicos e não possuem componentes. Os tipos simples mais relevantes para a definição dos padrões PKCS são:

BIT STRING Uma *string* binária (uns e zeros);

IA5String Uma *string* de caracteres (ASCII);

INTEGER Um valor inteiro qualquer;

NULL Um valor nulo;

OBJECT IDENTIFIER Identificador de um objeto. É uma seqüencia de componentes inteiros que identificam o objeto;

OCTET STRING Uma *string* qualquer de octetos;

PrintableString Uma *string* de caracteres imprimíveis;

T61String Uma *string* de caracteres T.61;

UTCTime Uma *string* de caracteres com a coordenada universal de tempo (*Greenwich Mean Time - GMT*)

Tipo Structured: Estruturados com componentes. O ASN.1 define quatro tipos, os quais são importantes para os padrões PKCS:

SEQUENCE Um conjunto ordenado de um ou mais tipos;

SEQUENCE OF Um conjunto ordenado de nenhuma ou várias ocorrências de um determinado tipo;

SET Um conjunto não ordenado de um ou mais tipos;

SET OF Um conjunto não ordenado de nenhuma ou várias ocorrências de um determinado tipo.

Tipo Tagged: Derivado do tipo *other*, é utilizado para se distinguir tipos no interior de uma aplicação. É também usado para diferenciar tipos de componentes em tipos estruturados (*structure*). Aos componentes opcionais de um tipo estruturado SET ou SEQUENCE, por exemplo, são aplicadas etiquetas (*tags*) distintas para se evitar ambigüidades. Existem dois tipos em ASN.1:

Implícitos São derivados de outros tipos com a troca da etiqueta (*tag*). ASN.1 define esses tipos com a palavra chave *IMPLICIT*;

Explícitos São derivados de outros tipos com a adição de um *tag* externo. Na prática, esses tipos são estruturados contendo apenas um componente. ASN.1 define esses tipos com a palavra chave *EXPLICIT*;

A notação em ASN.1, seria então assim:

[***class number***] IMPLICIT ***Type***

ou

[***class number***] EXPLICIT ***Type***

Onde:

Class É um nome opcional da classe;

Number É um número inteiro não negativo que identifica a etiqueta dentro da classe.

Type É o tipo;

Tipo Other: São os tipos que incluem o tipo *CHOICE* e o tipo *ANY*. O tipo *CHOICE* consiste num conjunto de uma ou mais alternativas e o tipo *ANY* é um valor de um tipo qualquer que pode ser definido em um registro de um *object identifier* ou um *integer*.

C.2.2 BER

BER (*Basic Encoding Rules*), proporciona uma ou mais formas de se representar qualquer valor em ASN.1 em uma *string* de octetos, sendo considerado um padrão. Existem três métodos de codificação **BER** em ANS.1. A escolha depende do tipo do valor e se o tamanho do mesmo é conhecido ou não.

Primitive, definite length Tipos simples (*simple*) não *string* empregam este método;

Constructed, definite length Empregados por tipos estruturados (*structured)* e tipos simples *string* com tamanhos conhecidos;

Constructed, indefinite length Empregados por tipos estruturados (*structured)* e tipos simples *string* com tamanhos desconhecidos;

Cada um dos métodos apresentados acima são codificados em três ou quatro partes:

Identifier octets Identifica a classe e o número do *tag* do valor ASN.1 e indica se o método é *primitive* ou *constructed*;

Length octets Para os métodos de tamanho definido, este campo determina o número de octetos contidos. Para os métodos de tamanho indefinido, indica que o tamanho é indefinido;

Contents octets No caso dos métodos primitivos de tamanho definido, este campo contém o valor propriamente dito. Para os métodos do tipo *constructed*, possui a concatenação da codificação **BER** dos componentes do valor;

End-of-contents octets Este campo indica o fim do conteúdo para os métodos de tamanho indefinido. Para os outros métodos, é ausente.

C.2.3 DER

DER (*Distinguished Encoding Rules*), é um subconjunto de **BER** e proporciona uma forma de se representar algum valor em ASN.1 em uma *string* de octetos.

DER é indicado para aplicações onde uma codificação única para uma seqüência de octetos é necessária.

C.3 Padrões PKCS

Nesta seção, serão descritos os elementos da família de padrões PKCS para criptografia de chaves públicas. Conforme as tecnologias abordadas no capítulo anterior, os laboratórios RSA, com a sua divisão de segurança de dados, propuseram padrões que descrevem a implementação de cada uma delas. A descrição da sintaxe das mensagens é feita em ASN.1. A necessidade de se criar padrões é decorrente de duas situações independentes. A primeira delas diz respeito à determinação da sintaxe da mensagem e a outra, à especificação do algoritmo criptográfico a ser utilizado. Exemplificando, podemos dizer que a sintaxe do padrão de assinatura digital pode empregar qualquer algoritmo de chave pública e não somente o RSA[2]. Da mesma forma, o algoritmo RSA pode ser empregado por diversos padrões de sintaxe [JR. 93]. Uma outra razão forte para a criação de padrões, é sem dúvida, a garantia da interoperabilidade dos sistemas.

Para apresentar os padrões PKCS a seguir e também entender melhor a padronização proposta, faz-se necessária a explanação de algumas tecnologias de chave pública contempladas pelos mesmos.

- **Assinatura Digital** - A tecnologia de assinatura digital consiste na cifragem de uma mensagem por Alice com o uso de sua chave privada. Essa mensagem pode ser verificada por qualquer pessoa que a receba utilizando a respectiva chave pública de Alice, o que comprova a sua autoria, pois, somente ela conhece a chave privada.

[2]Acrônimo de Rivest, Shamir e Adleman, seus criadores. É um algoritmo forte de criptografia assimétrica, desenvolvido em 1.978 baseado na exponenciação aritmética modular. O ataque da força bruta é computacionalmente inviável, pois, o tamanho da chave utilizada é muito grande.

- **Envelope Digital** - Um envelope digital é assim chamado por se compor de duas mensagens, sendo a principal cifrada por uma chave simétrica gerada randomicamente por Alice e a outra, com a própria chave simétrica usada pela primeira mensagem, cifrada com a chave pública de Beto. Assim, ao receber as mensagens, Beto decifra a segunda com a sua chave privada, para conhecer a chave secreta que utilizará para decifrar a mensagem principal.
- **Certificado Digital** - Um certificado digital é uma mensagem assinada digitalmente por uma autoridade certificadora contendo a identificação de um usuário e a sua chave pública. Este certificado é então distribuído pelo usuário para as pessoas com as quais ele deseja se comunicar. Como todos conhecem a chave pública da autoridade certificadora, este método se torna bastante eficiente para a distribuição e autenticidade de chaves.

A seguir, serão descritos alguns dos padrões PKCS com as respectivas tecnologias de chave pública que os empregam:

- **PKCS #1 - Cifrar com o RSA** - O padrão PKCS #1 descreve um método chamado *rsaEncription*, para cifrar os dados utilizando o algoritmo RSA de chave pública. Este algoritmo é utilizado na construção de assinaturas e envelopes digitais conforme descrito no PKCS #7. No caso específico de assinaturas digitais, é gerado um resumo da mensagem a ser assinada com um algoritmo de hash[3]. Este resumo é então concatenado com a mensagem principal e ambos são cifrados. Este artifício permite se verificar a integridade da mensagem recebida. Decifrando-a, calcula-se novamente o resumo da mensagem recebida e compara-se com o resumo recebido. Se forem iguais, sabe-se que a mensagem não foi alterada no transporte, sendo então, confiável. Além disso, o padrão PKCS #1 ainda descreve a sintaxe de chaves públicas e privadas para

[3]Algoritmo criptográfico que, ao ser aplicado a mensagens de qualquer tamanho, produz um resultado de tamanho fixo e bem pequeno, não sendo possível, executar a operação de forma reversa para se chegar à mensagem original. Os algoritmos de função hash em uso atualmente são o MD5, SHA-1 e RIPEMD-160 [STA 99].

o algoritmo RSA e também três outros algoritmos de assinatura chamados: *md2withRSAEncription*, *md4withRSAEncription* e *md5withRSAEncription*;

– **PKCS #3 - Troca de chaves por Diffie-Hellman** - Este padrão, descreve o método para implementação do protocolo de troca de chaves por Diffie-Hellman, onde duas partes interessadas em se comunicar podem trocar chaves secretas sem mesmo terem combinado previamente. Essas chaves podem ser utilizadas para se estabelecer conexões seguras entre as partes;

– **PKCS #5 - cifração baseada em senha** - A cifração de chaves privadas se faz necessária para armazenamento e transferência de um computador para outro. O padrão PKCS #5 define dois algoritmos de cifração de chaves: pbeWithMD2andDEs-CBC e pbeWithMD5andDES-CBC. Eles empregam o bloco de cifragem DES[4], que utiliza como senha, o resultado das funções de resumo (hash) MD2[5] e MD5.

– **PKCS #6 - Sintaxe de certificado estendido** - Este padrão descreve a sintaxe para certificados estendidos. Um certificado estendido possui um conjunto de atributos, os quais, podem ser verificados com uma simples operação de chave pública. A finalidade de se incluir um conjunto de outros atributos no processo de certificação de uma entidade, é fornecer outras informações a respeito dela, além de simplesmente, sua chave pública.

– **PKCS #7 - Sintaxe de mensagem criptográfica** - O **PKCS #7** descreve uma sintaxe geral para dados que podem ser cifrados tais como assinaturas e envelopes digitais. Esta sintaxe admite recursividade, ou seja, um envelope pode estar contido em outro ou alguém pode assinar um dado previamente enve-

[4]Data Encryption Standard - algoritmo de criptografia simétrica, onde os dados são cifrados em blocos de 64 bits com uma chave de 56 bits.

[5]Message Digest - Algoritmo desenvolvido por Ron Rivest que gera um resumo de tamanho fixo de uma mensagem de qualquer tamanho. A mensagem inicial é dividida e processada pelo algoritmo em blocos. Segundo o autor do algoritmo, o MD4 é uma versão mais rápida que o MD2, porém, baixou o nível de segurança em alguns pontos. O MD5, por sua vez, apesar de mais lento, é mais seguro que o MD4. O tamanho do resumo gerado das mensagens é de 128 bits.

lopado. Este padrão, pode ainda suportar uma variedade de arquiteturas para o gerenciamento de chaves baseado em certificados, semelhante ao que está descrito para *Privacy Enhanced Mail (PEM)* no RFC[6] 1422. Os valores produzidos de acordo com o PKCS #7 deveriam seguir as regras básicas de codificação (BER), as quais representam estes valores em seqüencias de octetos.

– **PKCS #8 - Informação sobre a chave privada** - O PKCS #8, determina a sintaxe para informações sobre a chave privada. Nessas informações, além da chave privada para alguns algoritmos de chave pública, estão contidos também um conjunto de atributos. Algoritmos de criptografia baseados em senha que foram descritos no PKCS #5 podem ser usados para cifrar informações sobre chaves privadas. Tais algoritmos são eficazes e de fácil implementação.

– **PKCS #9 - Tipos de atributos selecionados** - Este padrão define os tipos de atributos selecionados para uso nos padrões PKCS #6 - certificados estendidos, PKCS #7 - mensagens assinadas digitalmente e PKCS #8 - informações sobre chave privada.

– **PKCS #10 - Requisição de certificado digital** - Neste padrão é descrita a sintaxe para a requisição de certificados digitais. Uma requisição de certificado digital compõem-se de uma identificação, uma chave pública, e como opcional um conjunto de atributos. Tudo isso é enviado para a autoridade certificadora que transforma a requisição inicial em um certificado X.509 ou, em um certificado estendido, caso um conjunto adicional de atributos tenha sido definido inicialmente.

– **PKCS #11 a PKCS #15** - Existem ainda outros padrões PKCS que determinam vários aspectos de comunicação e implementações de segurança em sistemas, entretanto, são de menor relevância para esse trabalho. São eles:

  PKCS #11: New Member of Public Key Cryptography

[6] *Request for Comments* - Formam uma série de notas a respeito da Internet, comunicação entre computadores e protocolos de redes desde 1.969.

PKCS #12 - Personal Information Exchange Syntax Standard

PKCS #13: Elliptic Curve Cryptography Standard

PKCS #14 - Pseudorandom Number Generation Standard

PKCS #15: Cryptographic Token Information Format Standard

Maiores informações sobre os padrões PKCS podem ser encontrados na Internet no endereço: http://www.rsasecurity.com/rsalabs/pkcs/.

C.4 Conclusão

Uma forma padronizada para a construção de objetos que venham a compor um protocolo é necessária para a transferência de dados através da rede [TAN 97]. A linguagem para a descrição de dados ASN.1, juntamente com os padrões de criptografia de chave pública (PKCS), permitem a construção de protocolos de modo que possam ser implementados a qualquer tempo. Além disso, a adoção de padrões para a representação de uma idéia, torna-a de fácil entendimento por se tratar de uma linguagem comum.

Apêndice D

Glossário

Ombudsman - Palavra de origem sueca que designa a pessoa encarregada de observar e criticar as lacunas de uma empresa, sempre colocando-se no lugar do cliente;

Ouvidor - O mesmo que Ombudsman;

Helpdesk - Fonte de suporte técnico. É composto por um grupo de técnicos de suporte para auxílio a usuários em geral;

Call Center - Centro de chamadas telefônicas para atendimentos aos usuários de um sistema ou clientes de uma empresa;

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;

Hacker - Grandes conhecedores de computação que objetivam a invasão de sistemas informáticos de empresas ou instituições em geral;

Web Site - O mesmo que sítio;

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

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

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*);

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

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;

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;

PKCS - Public Key Cryptographic Standards ou Padrões Criptográficos de Chave Pública;

ASN.1 - Abstract Sintaxe Notation One - é uma linguagem para a descrição abstrata de tipos de dados e definição de protocolos de comunicação;

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;

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.