JOÃO FÁBIO DE OLIVEIRA

MECANISMO DE AUTENTICIDADE NA CONTRATAÇÃO VIA INTERNET

Dissertação apresentada ao Programa de Pós-Graduação em Informática Aplicada da Pontifícia Universidade Católica do Paraná como requisito parcial para obtenção do título de Mestre em Informática.

CURITIBA

2009

JOÃO FÁBIO DE OLIVEIRA

MECANISMO DE AUTENTICIDADE NA CONTRATAÇÃO VIA INTERNET

Dissertação apresentada ao Programa de Pós-Graduação em Informática Aplicada da Pontifícia Universidade Católica do Paraná como requisito parcial para obtenção do título de Mestre em Informática.

Área de Concentração: *Computação Forense e Biometria*

Orientadora: Prof. Dr[a]. Cinthia Obladen de Almendra Freitas
Co-orientadores: Prof. Dr. Altair Olivo Santin e Prof. Dr. Antônio Carlos Efing

CURITIBA
2009

Oliveira, João Fábio de
Mecanismo de Autenticidade na Contratação via Internet. Curitiba, 2009. 91p.

Dissertação – Pontifícia Universidade Católica do Paraná. Programa de Pós-Graduação em Informática.

1. Segurança na *Web* 2. Mecanismo 3. Assinatura Digital 4. Autenticidade da Informação. I.Pontifícia Universidade Católica do Paraná. Centro de Ciências Exatas e de Tecnologia. Programa de Pós-Graduação em Informática II-t

Para minha querida e amada esposa, *Vanessa*.

Agradecimentos

O sentir-se desafiado por uma evolução constante é algo que me fascina a todo tempo e quando encontramos e nos relacionamos com pessoas que alimentam o desejo pelo aprendizado, tornando-o um desafio, flora a motivação para vencer os obstáculos e mostrar para si mesmo que é possível, que a cada passo dado torna-se uma realização gratificante rumo à própria evolução do ser.

A Deus, por permitir que os desafios me fossem colocados a frente e que, com alegria, saúde, apoio familiar e muita motivação, pudesse vencê-los a cada dia deste percurso da vida.

À minha querida e amada esposa Vanessa, que sempre me apoiou e dedicou seu precioso tempo em me ajudar a vencer mais esta etapa de nossa maravilhosa vida.

Às minhas filhas, Gabriela e Rafaela, que me apoiaram em todo o tempo deste trabalho e suportaram as ausências dos diversos finais de semana de árduo trabalho.

A minha mãe Maura, especial carinho pelo constante apoio e alegria de ver a realização os filhos.

Ao meu querido irmão Guilherme, que sempre me motivou neste trabalho e me mostra constantemente a realização da vida nas coisas mais simples, na alegria de viver sempre.

Aos meus sogros Samuel e Edite, cujo apoio e ajuda tornou mais fácil vencer mais este desafio.

Tenho especial gratidão e carinho ao amigo Luciano Johnson, que muito tem feito para que cresçamos juntos na amizade, e neste trabalho me ensinou as maravilhas da linguagem Java.

À minha orientadora Cinthia Freitas, que tornou possível e desafiador este trabalho, e que com sua especial habilidade de dosar os temas críticos nos momentos certos, juntamente com o apoio dos co-orientadores Carlos Efing e Altair Santin, permitiu-me chegar ao fim deste maravilhoso trabalho.

Agradeço aos demais amigos pelo incentivo, e que tenhamos força para continuar na busca da realização do conhecimento, sempre.

Sumário

Lista de Figuras

Lista de Tabelas

Lista de Abreviaturas

TCP/IP	*Transmission Control Protocol/Internet Protocol*
WWW	*World Wide Web, ou simplesmente Web*
HTTP	*Hypertext Transfer Protocol*
Hash	Função matemática aplicada sobre uma string (texto)
SSL	*Secure Sockets Layer*
TLS	*Transport Layer Security*
Log	Registro de eventos relevantes em um sistema computacional
CPU	*Control Process Unit*
SNMP	*Simple Network Management Protocol*
ICMP	*Internet Control Message Protocol*
NAT	*Network Address Translation*
NTP	*Network Time Protocol*
DNS	*Domain Name System*
RFC	*Request For Comments*
PHP	*Hypertext Processor*
XML	*eXtensible Markup Language*
KDD	*Knowledge Discovery in Databases*
B2B	*Business to Business*
B2C	*Business to Consumer*
C2C	*Consumer to Consumer*
B2G	*Business to Government*
B2E	*Business to Employee*

Resumo

Este trabalho apresenta um estudo sobre os problemas de segurança nas transações de contratação realizadas na Internet apresentados em Garfinkel (1997) e propõe um método de verificação de autenticidade aplicado nestas contratações, definida como um mecanismo de autenticidade que irá manter diversos registros das atividades realizadas, durante todo o processo de contratação, em arquivos armazenados digitalmente no servidor do fornecedor, e oferecido para arquivo ao consumidor no final da transação comercial. Entende-se que o papel do fornecedor é garantir o registro das operações realizadas na Internet, até porque o consumidor não tem obrigação legal de armazená-las, visto que em situações de litígio deve ocorrer a inversão do ônus da prova, conforme definido Art. 6º, Inciso VIII, da Lei 8.078/90 – Código de Defesa do Consumidor. Neste caso, o mecanismo proposto garante a autenticidade da transação realizada, registrando informações relevantes que auxiliam na identificação das partes, do objeto, da forma de pagamento, entre outros, caracterizado como Instrumento Contratual. Este trabalho define um mecanismo que garante a autenticidade das operações de contratação realizadas no ambiente Internet, especificamente através de transações via *Web*, no qual o registro de itens críticos da operação deverá servir como base jurídica, satisfazendo as premissas de aceitação legal de um documento digital.

Palavras-Chave: Segurança na *Web*; Mecanismo; Assinatura Digital; Autenticidade da Informação.

Abstract

This proposal discusses the security problems on the contracts hired by Internet and describes an authenticity mechanism that will keep log files from the activities during the *Web* hiring, throughout the process of recruitment. These log files will be stored digitally, either on the side of the supplier and offered to consumer as a cipher file. It is understood that it is legal obligation of the supplier to register and ensure the integrity of the operations on the Internet, because in situations of dispute can occur a reversal of the burden of proof, as defined in art. 6, section VIII, of the Law 8.078/90 - Brazilian Consumer Code. Thus, the authenticity mechanism ensure confidence on the Internet contracts, registering relevant information that will help in the identification of the parties, of the objects, of the bill payments and others, defined like Contractual Instrument. Moreover, it is important to remind that security in hiring by Internet is an essential feature because it allows the consumer a guarantee of contract award, since it maintains the integrity of the document, and also can be presented as evidence to the Judiciary, helping in litigation and satisfying the premises of the legal acceptance of a digital document.

Keywords: Law and Internet; Consumer Protection; Authenticity.

Capítulo 1

Introdução

O crescimento do uso da Internet na rotina diária das pessoas já se concretizou como ferramenta para realização de diversas tarefas do dia-a-dia da sociedade, tais como: pagamento de contas bancárias, consulta das condições meteorológicas, consulta a catálogos telefônicos e mapas, relacionamento entre pessoas, mensagens eletrônicas e, ainda, compras de produtos e contratação de serviços.

Segundo o Centro de Estudos sobre as Tecnologias da Informação e da Comunicação[1], cerca de 18% dos domicílios brasileiros já possuem acesso a Internet, contabilizados na última pesquisa em 2008[2], o que representa um crescimento de 5,89% sobre os 17% do ano de 2007[3]. Este universo crescente de usuários e potenciais consumidores de produtos e serviços através da Internet representa uma grande preocupação do ponto de vista computacional e jurídico, pois potencializa a cada ano o volume de problemas a serem tratados no âmbito de cada ciência relacionada.

Como meio de acesso digital, a Internet traz algumas preocupações no aspecto de segurança da informação uma vez que os registros não são mais feitos em meio físico, como o papel, e sim arquivados eletronicamente em meios digitais, como o disco rígido dos computadores. Ao mesmo tempo em que são simplificadas as operações comerciais realizadas no meio digital, insere-se um fator restritivo, como exemplo o nível de conhecimento da tecnologia envolvida no meio digital, e aponta-se para um universo de estudo sobre os

---

[1] Comitê Gestor da Internet Brasil, Centro de Estudos sobre Tecnologias da Informação e da Comunicação, disponível em: http://www.cetic.br/, acesso em 20 de junho de 2009.
[2] Pesquisa disponível em: http://www.cetic.br/usuarios/tic/2008-total-brasil/rel-geral-04.htm, acesso em 20 de junho de 2009.
[3] Pesquisa disponível em: http://www.cetic.br/usuarios/tic/2007/rel-geral-04.htm, acesso em 20 de junho de 2009.

aspectos da segurança, confiabilidade, autenticidade. Sem esquecer, ainda, da regularidade jurídica dessas operações frente a fatos duvidosos e questionados por qualquer parte envolvida na transação, conforme apresentado em Mattos (2007).

Assim, torna-se importante esclarecer o entendimento dos termos usualmente aplicados no ambiente eletrônico que estão diretamente correlacionados com o desenvolvimento deste trabalho, que são vulnerabilidades e ameaças, sendo esta última também caracterizada pela exploração das limitações existentes nos softwares que são executados em determinados ambientes. Para Mackenzie (1997), uma ameaça (*threat*) é caracterizada por um conjunto de ações explorando circunstâncias, condições ou conhecimentos sobre um sistema que expõem as propriedades de segurança ao risco (possibilidade de ocorrência de comportamento não esperado do sistema). Uma ameaça, quando posta em ação, é identificada como um ataque (*attack*) à segurança do sistema. Por outro lado, entende-se por vulnerabilidade (*vulnerability*) a existência de debilidade, fraqueza ou imperfeição em procedimentos, serviços ou sistemas. Estas vulnerabilidades podem ser oriundas de falhas de concepção, implementação ou de configuração de serviços ou aplicações, expondo os recursos de um sistema computacional aos ataques [Shirley, 2000].

As principais vulnerabilidades e ameaças existentes na Internet, como mensagens eletrônicas indesejadas, invasão de sites, vírus em computadores, entre outras[4], tem crescido nos acessos a Internet, porém o esforço em busca de soluções técnicas para a segurança da informação trafegada, como a criptografia e assinatura digital definida em [Behrens, 2005] [Garfinkel, 1997] [Denning, 1982], permite propor mecanismos mais robustos para o tráfego e armazenamento das informações, principalmente para torná-las confiáveis do ponto de vista da veracidade do conteúdo registrado.

De acordo com Boiago Júnior (2005), os contratos provêm dos negócios jurídicos que são realizados em virtude de acordos de vontades bilaterais ou plurilaterais, e a diferenciação está caracterizada na convergência de dois ou mais consentimentos para que sejam produzidos efeitos jurídicos. Assim, se uma pessoa através de e-mail se compromete a cumprir

[4] Segundo o Centro de Tratamento de Incidentes de Segurança da Rede Nacional de Pesquisa, disponível em: http://www.rnp.br/cais/alertas/2007/cais-res-20071106.html, "*No terceiro trimestre de 2007 a equipe do CAIS tratou 8.080 incidentes de segurança na sua totalidade. Destes, 49,12% referem-se ao envio de spam em grande escala, 18,57% a tentativas de invasão de sistemas e 13,89% a propagação de vírus e worms através de botnets (computadores infectados e controlados à distância por atacantes). Também foram tratados 225 casos de troca de páginas, em que o atacante substitui o conteúdo original de uma página web ou inclui conteúdo não autorizado na página atacada, e ainda 88 casos de phishing, ataques que têm por objetivo básico obter dados confidenciais de usuários.*", acesso em 20 de junho de 2009.

determinada obrigação para com outras duas pessoas que aceitam a execução da obrigação, certamente ocorreu um negócio jurídico, pois houve a convergência de três vontades para a consecução de um determinado negócio jurídico, por conseqüência a realização de um contrato.

Neste sentido, torna-se necessário buscar alguma maneira de tratar as características técnicas da rede Internet usada para comércio eletrônico, com os aspectos jurídicos das contratações de produtos e serviços, de forma a aumentar o nível de confiabilidade sobre este meio que vem crescendo anualmente, aumentando o consumo e potencializando problemas.

1.1. Problema de Segurança na *Web*

A base de transporte das informações na Internet é o protocolo TCP/IP *(Transmission Control Protocol/Internet Protocol*), conforme definido em Comer (1991), e este, em sua versão 4, é o consolidado para uso na Internet. Este protocolo não prevê mecanismos de segurança em nível do transporte das informações, deixando, para as aplicações que são desenvolvidas para interação com os usuários finais, o papel da preocupação com critérios relativos à proteção do conteúdo trafegado. Isto significa que o transporte das informações entre dois pontos na Internet, independente de sua localização física, poderá ser capturado por um analisador de protocolo[5], tornando-se conhecido o conjunto de informações ali capturadas.

Na especificação do protocolo TCP/IP definida nas RFC 781[6] e RFC 793[7], e também referenciada em Comer (1991), existe a divisão conceitual de cinco camadas ou níveis, conforme mostrado na Tabela 1.1. As camadas mais baixas (1-4) preocupam-se em fazer com que a informação saia da origem e chegue ao destino através da rede, seja ela Internet pública ou mesmo uma rede privada[8]. A camada 5, também chamada de aplicação, especifica e implementa softwares aplicativos que interagem com os usuários finais. É justamente neste nível que todas as preocupações relativas à segurança da informação deverão ser implementadas, ou seja, as aplicações no nível do usuário devem ter mecanismos de tratamento que sejam considerados seguros o suficiente para, de um lado dar a percepção ao

---

[5] O analisador de protocolo Wireshark é o mais popular conhecido e distribuído livremente na Internet, disponível em: http://www.wireshark.org/, acesso em 20 de junho de 2009. Outros aplicativos disponíveis são o CommView e Norton Ghost, ambos com licença através de pagamento.

[6] *Request For Comment* definida em http://www.ietf.org/rfc/rfc0781.txt?number=781, acesso realizado em 20 de junho de 2009.

[7] *Request For Comment* definida em http://www.ietf.org/rfc/rfc0793.txt?number=793, acesso realizado em 20 de junho de 2009.

usuário final que sua transação na rede está segura, sem riscos de adulterações de conteúdo, e por outro lado promover condições técnicas comprovadas de mecanismos considerados seguros, como o uso de algoritmos criptográficos no nível da aplicação, conforme definido e apresentado por Schneier (1996).

O tráfego na Internet conhecido como WWW (*World Wide Web*), ou simplesmente *Web*, é uma aplicação de software, modelo cliente-servidor, que é executada como interface direta com o usuário através do ambiente conhecido como navegador ou *browser*. Neste ambiente, diversas aplicações são escritas no formato do protocolo de nível de aplicação do TCP/IP conhecido como HTTP (*hypertext transfer protocol*) [Garfinkel, 1997]. Em não havendo mecanismos ou métodos específicos para tratativas de segurança definidos no próprio protocolo TCP/IP, cabe então as aplicações definirem e implementarem seus algoritmos adicionais de segurança para minimizar os impactos das ameaças ou limitações existentes na rede.

Tabela 1.1 – Modelo em Níveis do TCP/IP

Camada	Protocolo
5 – Aplicação	HTTP, DNS, SMTP, ...
4 - Transporte	TCP, UDP
3 – Rede	IP, IGMP
2 – Enlace	Ethernet, 802.11 WiFi, FR, ...
1 – Física	Modem, RS232, USB, ...

Os problemas de segurança na *Web* consistem em três grandes categorias, conforme definido em Garfinkel (1997):

[8] Redes Privadas são as que usam endereçamentos IPs reservados e distintos dos usados na Internet pública, conforme definição disponível em: http://www.ietf.org/rfc/rfc1918.txt, acesso em 15 de abril de 2009.

- Segurança no servidor *Web* e nos dados que estão ativos e arquivados nele: o usuário deve ter garantias de que suas informações estão confiáveis e seguras, e que não foram modificadas ou distribuídas sem sua autorização;
- Segurança da informação que trafega entre o servidor e o cliente pela rede de computadores: o usuário deve ter garantias de que a transmissão das informações entre o servidor e seu navegador *Web* tem um nível de proteção baseado em critérios tidos como confiáveis, tal qual a criptografia ou a assinatura digital [Behrens, 2005];
- Segurança da informação na própria máquina do usuário: o usuário deve ter garantias de que seu computador está o mais protegido possível através do uso de ferramentas associadas ao seu ambiente operacional[9]. Neste ponto, a mensuração do quanto à máquina do usuário está protegida fica comprometida pela própria autoridade do usuário sobre seu ambiente, pois, no nível de autonomia sobre gestão de sua máquina, o usuário pode autorizar, indevidamente, a instalação de softwares maliciosos que irão atuar em contravenção ao seu uso. Estes aspectos dependem do conhecimento e esclarecimento do usuário sobre segurança, tendo-se pouco, ou quase nenhum domínio sobre isto quando da implementação de aplicações para Internet.

Transpondo as definições dos protocolos envolvidos na Internet e suas características de limitações, já tratadas anteriormente, sobre as contratações realizadas na Internet, o paradigma da confiança do contrato de consumo eletrônico, apresentado em Mattos (2007), levanta aspectos jurídicos de despersonalização extrema baseado em massa de contrato por adesão e cláusulas gerais, em que há pluralidade de consumidores e fornecedores organizados em cadeia, dificultando as identificações e relação de responsabilidades sobre o contrato. Isto se agrava quando a tecnologia usada oferece riscos de alterações de conteúdo, quebra de autoridade, plágio, ou mesmo acessos indevidos e mau uso do conteúdo para fins ilícitos[10].

Neste sentido, a Internet torna-se foco de atenção quanto aspecto de segurança por uso de características em sua estrutura, a exemplo do protocolo TCP/IP visto anteriormente, que propicia cenários de uso indevido de informações. Como há riscos no aspecto de segurança da

[9] Cartilha sobre segurança para Internet recomenda uso e configurações adequadas para o usuário final, disponível em: http://cartilha.cert.br/, acesso em 20 de junho de 2009.
[10] De 1999 até 2007, o número de incidentes de segurança registrado no Brasil tem crescido anualmente, conforme demonstrado em: http://www.cert.br/stats/incidentes/, acesso em 18 de janeiro de 2009.

informação sobre as operações realizadas nas contratações via Internet onde, além da estrutura de funcionamento da rede mundial, aspectos operacionais de uso por parte do próprio usuário colocam em risco a confiabilidade da operação realizada. Portanto, torna-se necessário agregar algum mecanismo que melhore o nível de segurança da informação no âmbito do usuário da rede.

1.2. Objetivo Geral

A proposta deste trabalho é estudar as principais necessidades de segurança envolvendo a contratação na Internet, utilizando-se do ambiente *Web* como base referencial para esta contratação e, assim, correlacioná-los com aspectos jurídicos dessas contratações no sentido da materialização do fato realizado para compor o contexto da comprovação do fato e elaboração da prova frente situações de litígio. Deste modo, o presente projeto de pesquisa propõe e descreve um método, definido como mecanismo de autenticidade do relacionamento entre o fornecedor, aqui definido como contratado, e consumidor, aqui definido como contratante, o qual define parâmetros técnicos e rastreáveis da operação realizada, e disponibiliza informações seguras armazenadas no servidor do contratado, e, ao final da transação comercial, oferecê-lo ao contratante em formato digital de maneira que o mesmo tenha posse das informações comprobatórias de sua participação na transação comercial realizada.

Também, definir o mecanismo de autenticidade em seus detalhes técnicos de conteúdo de informações, processos de atualizações, inserção no contexto do portal de comércio eletrônico hospedeiro, rastreabilidade das informações armazenadas e de maneira íntegra e confidencial (armazenamento com criptografia), seguindo os algoritmos definidos em Schneier (1996). Estas informações têm fundamentação jurídica para aceitação legal de um documento digital, onde, de fato, o documento eletrônico, por possuir os elementos da autoria, conteúdo e meio, configura-se perfeitamente como documento para fins de prova no processo civil [Dias, 2004].

1.3. Objetivos Específicos

Confirmar e correlacionar às limitações existentes nas redes TCP/IP que suportam as transações de contratação via Internet, principalmente as limitações inerentes ao protocolo

HTTP (*hypertext transport protocol*) e correlacionados as transações na *Web*, com aspectos jurídicos do comércio eletrônico, propostos em Mattos (2007) e Behrens (2005).

Trabalhar o desenvolvimento da proposta de um mecanismo de autenticidade, que permite o armazenamento de informações críticas sobre a transação de contratação comercial realizada, número IP do contratante e contratado, data e hora da realização da operação, portas dos serviços utilizadas no protocolo TCP/IP da Internet (cliente e servidor), entre outras informações técnicas. Este conjunto de informações tem o objetivo de garantir a veracidade da operação nas informações trafegadas entre o servidor do contratado e a máquina do contratante, sendo que ao final da transação comercial, o contratante terá a sua disposição um arquivo encriptado, conforme definido em Schneier (1996), oferecido pelo servidor do contratado para ser armazenado na máquina do contratante e, ao mesmo tempo, enviado a ele através de e-mail, contendo as informações técnicas formatadas em um documento denominado "Instrumento Contratual", as quais estarão disponíveis para uso comprobatório do acesso realizado e servirá de informação digital para sustentação jurídica em caso de litígio.

Incluir, também, o desenvolvimento de um protótipo de software, que permite testar e avaliar o método proposto, de forma a medir sua eficiência e eficácia quanto ao objetivo proposto. Os dados obtidos durante a realização do presente projeto foram de ambiente controlado em laboratório, porém representarão uma amostragem estatística extraída do ambiente real executando-se diversas interações do protótipo em cenário de simulação da realidade. Foram coletadas informações quantitativas dos usuários que aceitaram participar do uso do mecanismo de autenticidade, medidos no servidor do contratado, e foi considerada a montagem de um cenário de litígio jurídico com base nos dados de um contratante, no qual a amostragem da base legal das informações coletadas foi gerada pelo software do mecanismo de autenticidade e disponibilizada como prova através de documento eletrônico.

1.4. Estrutura do Trabalho

O Capítulo 1 apresenta o contexto geral do uso da Internet para comércio eletrônico, seus aspectos de limitação na parte de rede, protocolos, falhas existentes nas aplicações, e destaca os aspectos jurídicos de impacto nas contratações via Internet, ressaltando a base legal existente para suporte às definições do mecanismo de autenticidade proposto.

O Capítulo 2 apresenta o estado da arte dos problemas relacionados à segurança nos diversos conceitos envolvidos na tecnologia da informação, correlacionando com os elementos chaves que compõem o cenário das transações eletrônicas nas contratações realizadas na Internet, bem como, apresenta outros trabalhos desenvolvidos na área, tanto no aspecto técnico quanto apontamentos jurídicos na legislação brasileira.

O Capítulo 3 define e propõe o mecanismo de autenticidade, considerando seu detalhamento teórico e técnico, bem como caracterizando sua implementação no ambiente do servidor *Web* do contratado e todos os procedimentos junto ao contratante.

O Capítulo 4 descreve a execução de testes do protótipo em ambiente controlado de laboratório e analisa os resultados obtidos a partir da prototipação laboratorial do mecanismo de autenticidade proposto. Também conclui esta dissertação dentro da abordagem do portal de comércio eletrônico e apresenta os trabalhos futuros.

Capítulo 2

Estado da Arte

Este capítulo apresenta os conceitos de segurança, com destaque aos contratos através da Internet que impactam na legalidade das operações realizadas. Destaca também seus elementos principais, como o fornecedor, consumidor, produtos e serviços.

2.1. Segurança da Informação

A segurança da informação pode ser definida como uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade [Sêmola, 2003]. Neste sentido, o interesse por segurança em sistemas computacionais tem crescido muito nos últimos anos. Em geral, as ações danosas executadas por invasores[11] geram prejuízos tanto para a imagem quanto perdas financeiras, fatos estes que também apresentam a segurança da informação com mecanismos de defesas e prevenção aos ataques para evitar perdas e prejuízos de alguma natureza [Santin, 2004].

Segurança em sistemas computacionais não é exclusivamente um meio para permear fins, mas é antes de tudo, uma disciplina que através de seus conceitos, metodologias e técnicas, tenta manter as propriedades de um sistema, evitando ações danosas de entidades não autorizadas sobre as informações e os recursos do mesmo. Nas definições da segurança da informação apresentadas neste capítulo, ou mesmo outras encontradas na literatura, em quase todas é caracterizada a necessidade de se manter no sistema um conjunto de propriedades [Denning, 1982], apresentadas a seguir:

[11] Hackers, crackers, spies e outros tipos de malfeitores.

- Confidencialidade: garante a revelação da informação só a sujeitos[12] autorizados;
- Integridade: assegura a não modificação indevida – seja acidental ou intencionalmente – das informações do sistema;
- Disponibilidade: garante que as informações e recursos num sistema computacional estarão desimpedidos e prontos para serem usados quando requisitados por sujeitos autorizados.

De acordo com Landwehr (2001), consideram-se ainda como propriedades de segurança, a autenticação e não-repúdio.

- Autenticidade: garante que o sujeito usando uma identificação é seu verdadeiro detentor;
- Não-repúdio: garante que o participante de uma comunicação não possa negá-la posteriormente.

Em toda operação de contratação em ambiente eletrônico realizada na Internet, os elementos acima definidos compõe a parte essencial da análise da relação de confiança sobre o procedimento realizado.

A interoperabilidade entre aplicações nos negócios eletrônicos (*e-business*) é um contexto que exige eficiência para o ganho em escala no mundo digital. Bracher (2008) propõe um modelo de infra-estrutura baseado em uma arquitetura segura de documentos, em um contexto de fluxo inter-organizacional de trabalho, de forma que as organizações possam relacionar-se de maneira segura na troca de seus documentos digitais.

O modelo apresentado por Bracher (2008) implementa um protótipo no qual a arquitetura a ser implementada possui três componentes principais: engenharia do fluxo de trabalho, identidade do provedor, e o ambiente de processamento do documento. Neste modelo, as entidades participantes são reconhecidas e autenticadas para que tenham seus documentos validados dentro da arquitetura de trabalho, e o fluxo de relacionamento entre elas é estabelecido por regras definidas no contexto de trabalho entre as organizações. Os documentos trocados entre as entidades são validados digitalmente e compartilhados entre elas, o que garante um único e seguro ambiente de troca de documentos digitais.

[12] Entende-se por sujeito uma entidade ativa (programa, processo, sistema, etc.) cujas ações se refletem em recursos do sistema.

Para (Watanabe, 2008), a credibilidade nos ambientes baseados em *Web*, em especial os sites de comércio eletrônico, podem ser julgados incorretamente quanto aos aspectos de confiança pelo baixo conhecimento ou referência dos usuários em relação a ele. Muitos usuários acabam avaliando o site com base em sua estrutura visual, sua beleza ou mesmo aspectos irrelevantes do ponto de vista técnico para a segurança da informação, para tanto, o mesmo propõe uma análise técnica mais profunda do site de forma a prover informações aos usuários para sua análise de credibilidade e confiança sobre os acessos ao site de e-commerce.

2.2. Contratos Eletrônicos

O consumo em sites eletrônicos através do comércio eletrônico tem crescido a taxas na ordem de 42% ao ano[13], o que escala um nível na mesma proporção de problemas a serem tratados, desde aspectos computacionais quanto aos aspectos jurídicos da própria contratação.

Em pesquisa realizada pelo Procon-SP no período de junho a julho de 2007 sobre uma amostragem de 3 mil usuários de computadores, 59,11% destes usuários praticaram comércio eletrônico, ou seja, geram aceitação sobre os contratos eletrônicos. Nesta mesma pesquisa, 35,46% apontam para a falta de confidencialidade e segurança neste tipo de contrato, e 36,42% apontam para a falta de segurança no processo de contratação, destacando este fator como restritivo ao maior crescimento e confiabilidade em todo o processo de contratação pela Internet[14].

Em sua essência, o contrato eletrônico não se descaracteriza em qualquer aspecto que componha a idéia de contrato como principal fonte do direito das obrigações, apenas sua forma é diversa, e é necessária a análise de sua natureza para se determinar os elementos formativos em face do novo ambiente em que ele se realiza sem perder de vista os interesses que devem estar presentes em qualquer abordagem jurídica [Relvas, 2005].

---

[13] Segundo a FOLHAOnline, disponível em http://www1.folha.uol.com.br/folha/informatica/ult124u435247.shtml, temos: "O comércio eletrônico no Brasil somou, no primeiro semestre de 2008, um faturamento de R$ 3,8 bilhões, resultado 45% superior ao obtido no mesmo período do ano passado, segundo estudo divulgado pela consultoria e-bit. Já o número de consumidores cresceu 42% se comparado a 2007, totalizando 11,5 milhões de pessoas que já compraram pela rede no Brasil. Os dados fazem parte da 18ª edição do estudo "Relatório WebShoppers", realizado pela e-bit com o apoio da Câmara Brasileira de Comércio Eletrônico". Acesso realizado em 20 de junho de 2009.

[14] Pesquisa realizada pelo Procon-SP, disponível em http://www.procon.sp.gov.br/pdf/comercio_eletronico.pdf, acesso realizado em 14 de janeiro de 2009.

Na composição dos elementos contratuais no ambiente da Internet, tal qual Relvas (2005) pode-se relacionar os seguintes itens fundamentais em sua estrutura:

- Consumidor (contratante): diz respeito à pessoa física ou jurídica que adquire ou utiliza produto ou serviço, pela via eletrônica, como consumidor final;
- Fornecedor (contratado): 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 (Código de Defesa do Consumir, art. 3º.);
- Contratos eletrônicos: são contratos formais ou informais, expressos ou tácitos, individuais ou por adesão, realizados através da rede mundial de computadores (Internet);
- Local do contrato: é o local de residência habitual ou sede do contratante, que deve ser considerado para efeitos jurídicos.

O princípio fundamental da autonomia da vontade, apresentado em Relvas (2005), destaca particularidades na contratação eletrônica, a saber:

a) Faculdade de contratar ou não contratar, ou seja, liberdade de escolha do contratante em aceitar ou não o contrato;
b) Liberdade de escolha do contratante em relação ao contratado, ou seja, no mundo virtualizado[15] da Internet, ter a liberdade de escolha de quem contratar;
c) Liberdade de fixar e/ou negociar o conteúdo dos contratos, a exceção dos contratos por adesão[16].

A assinatura de um contrato tradicional é a confirmação explícita da vontade entre as partes. Já nos contratos eletrônicos, a assinatura eletrônica torna-se cada vez mais imprescindível para a validade e legalidade do contrato [Behrens, 2005]. A grande parte das contratações em ambiente eletrônico não considera o uso de mecanismos de assinatura digital,

[15] Entende-se que o termo "virtualizado" refere-se ao mundo digital ou eletrônico provido pela Internet.
[16] No Código de Defesa do Consumidor sobre os contratos de adesão, disponível em http://www.procon.go.gov.br/artigodoutrinario/artigo_dout_19.htm, temos: "Os contratos de adesão são os contratos já escritos, preparados e impressos com anterioridade pelo fornecedor, nos quais só resta preencher os espaços referentes à identificação do comprador e do bem ou serviços, objeto do contrato. As cláusulas são preestabelecidas pelo parceiro contratual economicamente mais forte, sem que o outro parceiro possa discutir ou modificar substancialmente o conteúdo do contrato escrito. É evidente que esses tipos de contrato trazem vantagens as empresas, mas ninguém duvida de seus perigos para os contratantes hipossuficientes ou consumidores. Estes aderem sem conhecer as cláusulas, confiando nas empresas que as pré-elaboraram e na proteção que, esperam, lhes seja dada por um Direito mais social.". Acesso realizado em 14 de janeiro de 2008.

porém estes mecanismos estão disponíveis publicamente na Internet e garantem o mesmo valor jurídico de uma assinatura convencional[17], conforme Medida Provisória 2.200-2/2001, que estabelece: “"*Art. 1o Fica 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, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras.*"[18].

Isto significa que, toda a contratação realizada na Internet, se confirmada com uma assinatura digital, possui o valor jurídico necessário para confirmar a vontade das partes, bem como, identifica as partes que o assinam, tornando o fato verdadeiro sob os olhos da justiça.

2.3. Assinatura Digital

A assinatura digital é um método de autenticação que usa uma técnica adicional no processo de criptografia. Esta técnica é uma função matemática chamada de função *hash* e possuiu um algoritmo que determina um resultado exclusivo sobre o texto original, garantindo sua exclusividade e unicidade [Schneier, 1996] [Efing & Freitas, 2008].

A assinatura digital origina-se no processo de criptografia [Maia, 2005] [Behrens, 2005], a qual é definida como sendo a arte de escrever em códigos, visando esconder a informação através de um texto incompreensível, denominado de texto cifrado. Este processo denomina-se cifragem, e o processo inverso, ou seja, a partir do texto criptografado transformá-lo no formato original, compreensível, chama-se decifragem. Tanto a cifragem quando a decifragem são tarefas que podem ser realizadas computacionalmente, sendo que este software recebe o texto a ser codificado e uma informação adicional chamada chave, que é utilizado para definir a forma de trabalho do software no processo de cifragem ou decifragem. A chave passa a ser um elemento fundamental na solução criptográfica, sendo parte indispensável para tal procedimento funcionar, por isto seu sigilo torna-se importante no contexto da segurança do arquivo encriptado.

A Figura 2.1 ilustra o processo de cifragem e decifragem de um texto digital com base em chave simétrica (mesma chave para cifrar e decifrar o conteúdo).

---

[17] Conforme definição e disponibilização em http://www.contratosdigitais.com/oque/valorLegal.html: “As assinaturas eletrônicas têm o mesmo valor jurídico da assinatura convencional, desde que sejam realizadas por meio de um processo que assegura todos os elementos de prova jurídica em conformidade com a legislação vigente.”. Acesso em 14 de janeiro de 2009.

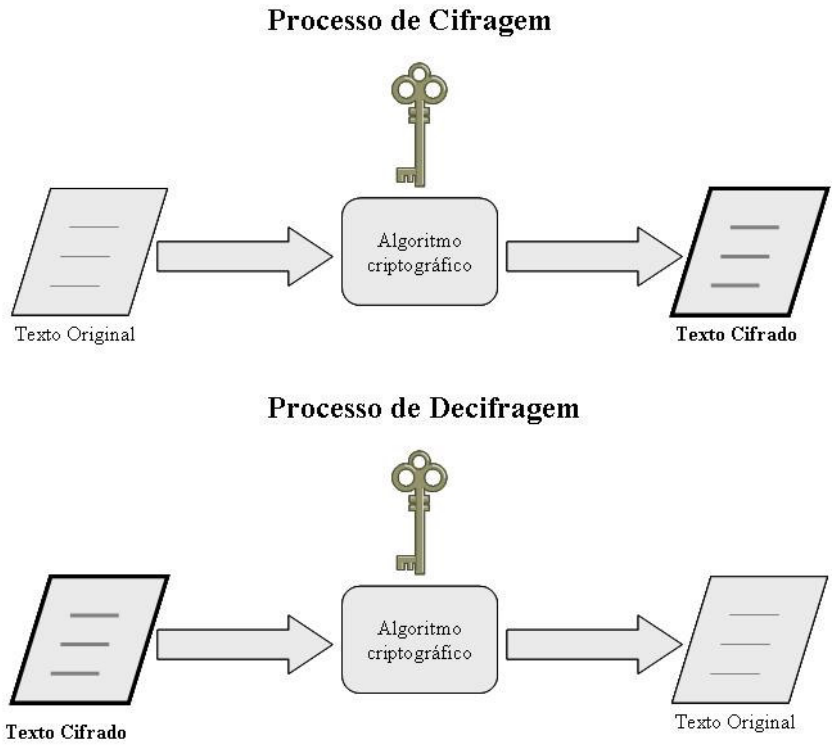

Figura 2.1 – Cifragem e Decifragem Simétrica

Em Efing & Freitas (2008), a assinatura digital resulta de uma função matemática aplicada sobre uma entrada original, representada por um conjunto de caracteres alfanuméricos (*string*) com a associação de uma chave do proprietário da informação original, sendo esta função conhecida também como função *hash*. Assim, é possível converter a entrada original em algo inteligível e aplicar o processo inverso, de forma a recuperar a originalidade da respectiva informação de entrada com a possibilidade de reconhecimento de propriedade do mesmo. Neste contexto, a assinatura digital também tem sua aplicabilidade jurídica justamente pelo mecanismo de verificação e identificação da autenticidade.

Há dois tipos de criptografia: a simétrica e a assimétrica [Garfinkel, 1997]. Na criptografia simétrica, a chave é a mesma usada pelo algoritmo de cifragem e decifragem da informação, como mostrado na Figura 2.1. A chave, por ser única, deve ser compartilhada entre as partes envolvidas no processo de encriptação e decriptação para atender os quesitos de funcionamento do algoritmo.

---

[18] Maiores informações disponível em http://www.icpbrasil.gov.br/twiki/bin/view/Certificacao/CertificadoConceitos, acesso realizado em 20 de junho de 2009.

Para Garfinkel (1997), os algoritmos simétricos são divididos em duas categorias: blocos e *stream*[19]. Os algoritmos em blocos encriptam os dados de uma única vez sobre o bloco da informação, enquanto que os algoritmos em *stream* trabalham byte a byte.

Existem muitos algoritmos com chave simétrica disponível para uso em âmbito de programação de computadores. A seguir, é apresentada uma relação dos principais algoritmos utilizados em aplicações na *Web*:

- DES: O *Data Encryption Standard* foi adotado como um padrão de criptografia pelo governo dos Estados Unidos em 1977 e como um padrão ANSI[20] em 1981. O DES é um encriptador em bloco que utiliza uma chave com tamanho de 56 bits e tem muitas formas diferentes de operar de acordo com o propósito que foi desenvolvido. Em sua forma básica de operação, utiliza-se da chave para encriptar o bloco de dados, gerando o arquivo protegido. De forma inversa, utiliza-se da mesma chave para abrir o arquivo em seu formato original;
- DESX: É uma simples modificação proposta no algoritmo DES que constrói uma inteligência em passos adicionais de encriptação. Estes passos adicionais (interações de encriptação) melhoram a segurança do algoritmo e o torna mais robusto em relação ao anterior[21];
- Triple-DES: É uma forma de construir um algoritmo mais robusto, utilizando-se do DES em repetições de encriptação com três chaves distintas, o que torna o texto encriptado mais difícil de ser decriptado;
- Blowfish: É um algoritmo criado por Bruce Schneier[22], que permite variação do tamanho da chave usando o tamanho máximo de 448 bits, tendo sido otimizado em sua execução de código para processados de 32 e 64 bits, o que o torna um algoritmo rápido e compacto. Não é patenteado e é de domínio público;

---

[19] Processo de encriptação com chave simétrica com o método de *stream*, significa que a encriptação acontece byte a byte ao invés de todo o bloco do arquivo, conforme detalhes apresentado na RFC2405, disponível em http://www.ietf.org/rfc/rfc2405.txt, acesso em 23 de abril de 2009.

[20] Instituto Nacional de Padrões dos Estados Unidos, disponível em http://www.ansi.org/, acesso em 20 de junho de 2009.

[21] Outras informações sobre este algoritmo estão disponíveis no site da *RSA Data Security* sob o título "*Cryptography FAQ*", disponível em http://www.rsa.com/rsalabs/node.asp?id=2152, acesso em 28 de fevereiro de 2009.

[22] O autor Bruce Scheneier possui muitos estudos sobre criptografia, disponíveis em http://www.schneier.com/, acesso em 20 de junho de 2009.

- IDEA: O *International Data Encryption Algorithm* (IDEA) foi desenvolvido em Zurique, Suíça, e publicado em 1990. Ele usa chaves de 128 bits em seu algoritmo de encriptação/decriptação e é utilizado pelo programa PGP[23] para encriptação de e-mails sobre a Internet, o qual se tornou um padrão na Internet, tendo sua RFC 2440 especificada pelo IETF – *Internet Engineering Task Force* e divulgada de forma pública.

Algoritmos assimétricos, também chamados de algoritmos de chave pública, operam com duas chaves distintas: chave privada e chave pública. Essas chaves são geradas simultaneamente e são relacionadas entre si, o que possibilita que a operação executada por uma chave seja revertida pela outra chave. A chave privada deve ser mantida em sigilo e protegida pela origem, enquanto que a chave pública é divulgada abertamente para que seja usada no processo de encriptação do conteúdo que será destinado ao proprietário desta chave pública, o qual usará sua chave privada para poder decifrar a informação. Desta forma, quando alguém (usuário A) quer encriptar uma informação e enviá-la a outra pessoa (usuário B), deverá utilizar a chave pública da outra pessoa (usuário B) e enviar o arquivo. Esta outra pessoa (usuário B), ao receber o arquivo, deverá utilizar-se de sua chave privada para poder abrir o arquivo. A Figura 2.2 mostra o processo de encriptação e decriptação das informações utilizando-se um algoritmo assimétrico.

Comparativamente, algoritmos simétricos trabalham sobre um único contexto de chave sobre o objeto encriptado, tornando-se mais ou menos robusto de acordo com o critério de encriptação e chaves utilizadas. Já os algoritmos assimétricos utilizam-se de técnicas envolvendo os dois lados de interesse no processo criptográfico de envio e de recebimento das informações, considerando a troca de chaves destas partes sobre os algoritmos definidos. Isto os tornam mais complexos em sua utilização e implementação, porém o nível de robustez e confiabilidade é superior ao dos algoritmos simétricos. Os dois principais sistemas definidos como de chaves públicas tem seu resumo funcional apresentado a seguir:

[23] O OpenPGP especifica os detalhes do protocolo e padrão utilizado, disponível em http://www.openpgp.org/, acesso em 20 de junho de 2009.

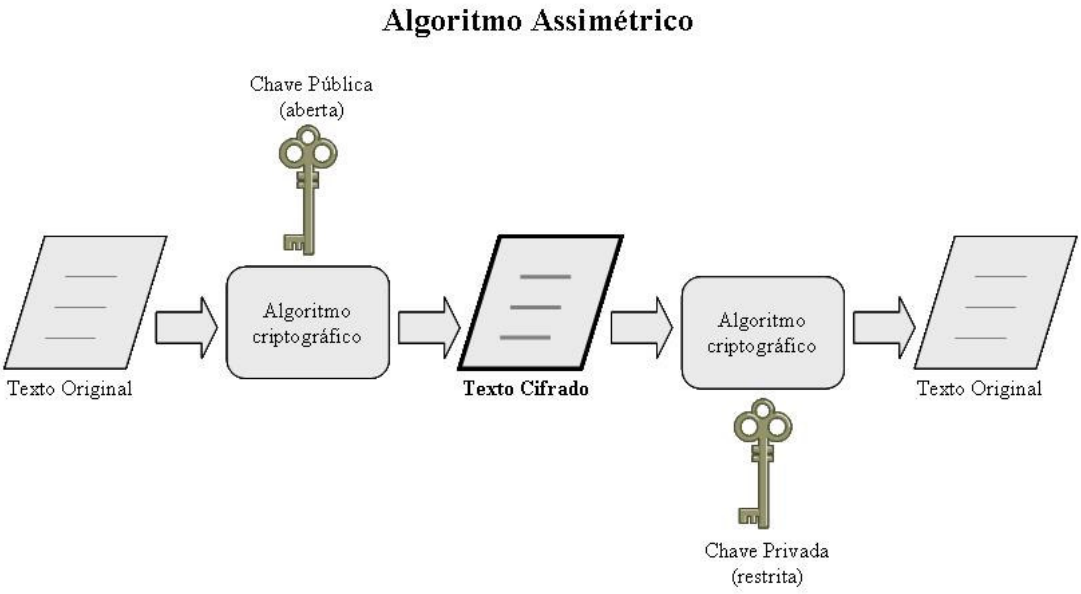

Figura 2.2 – Algoritmo Criptográfico Assimétrico

- Diffie-Hellman (DH) Key Exchange: É um sistema para troca de chaves criptográficas entre partes ativas. Não é um processo de encriptação e decriptação, mas um método de distribuição de chaves sobre um canal comum. Isto é, as partes aceitam trocar algumas informações numéricas para que seja criada uma terceira chave entre as partes através de um mecanismo matemático aplicado sobre estes números compartilhados. Após esta fase, os participantes da troca terão um meio seguro de envio da chave que protegerá futuras interações;
- RSA: É um sistema de chaves públicas desenvolvido por professores do MIT - *Massachussets Institute of Technology* - EUA, chamados, respectivamente, Ronald Rivest, Adi Shamir, e Leonard Adlaman. RSA pode ser usado como algoritmo criptográfico e também é proposto como base para assinatura digital, conforme definido mais adiante neste capítulo.

Além dos dois sistemas apresentados [Preneel, 2008], há uma variação do DH (Diffie-Hellman), conhecida como ElGamal, que implementa o algoritmo criptográfico e também serve como base para assinatura digital, conforme mostrado no RSA. Seu nome se deve a seu autor e criador Taher ElGamal.

Outro padrão usado para assinaturas digitais chama-se DSS (*Digital Signature Standard*), em português Padrão de Assinatura Digital, foi desenvolvido e proposto pela

Agência Nacional de Segurança dos Estados Unidos (NSA) e adotado como padrão nos processamentos de documentos federais pelo Instituto Nacional de Padrões e Tecnologia (*National Institute for Standars and Technology*). Permite o uso de chaves de qualquer tamanho e está direcionado apenas ao uso com o algoritmo de assinatura digital.

Existe, portanto, uma função usada em assinaturas digitais que é chamada de *hash*[24]. Este mecanismo tem a função de obter uma *string* (texto) com tamanho fixo com base no arquivo de entrada. O mecanismo de *hash* é usado computacionalmente para vários propósitos, mas em criptografia, serve para extrair uma *string* única com base na análise do arquivo fornecido que representa um valor único sobre a análise deste arquivo, ou seja, o algoritmo *hash* garante que a *string* extraída do arquivo é único de acordo com o formato, conteúdo e tamanho original [Preneel, 2008].

A assinatura digital é, por sua vez, um método de autenticação que usa um algoritmo de criptografia assimétrica em conjunto com a função *hash*. A Figura 2.3 ilustra o mecanismo de assinatura digital utilizando algoritmo assimétrico, conforme exposto anteriormente.

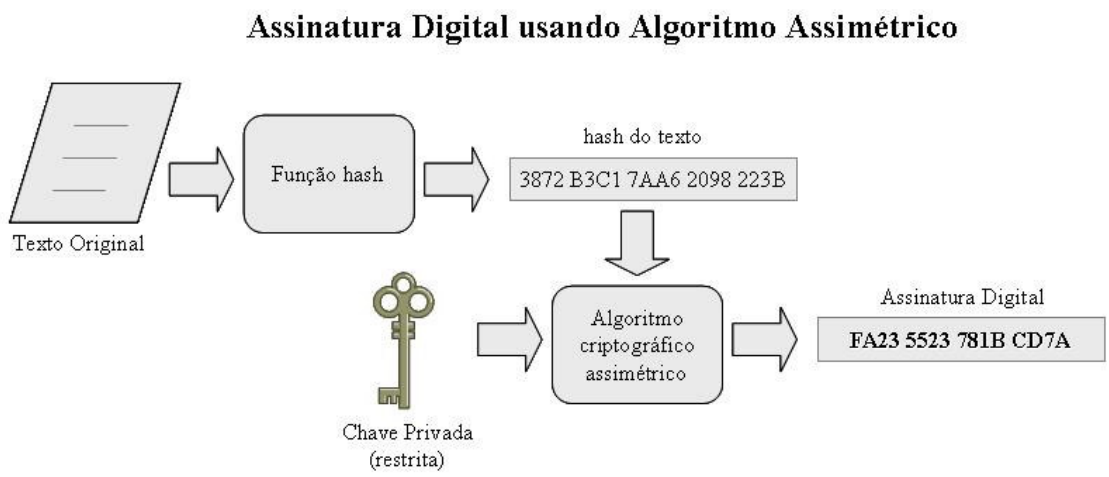

Figura 2.3 – Assinatura Digital com Algoritmo Assimétrico

A assinatura digital, em associação com a criptografia assimétrica, apresenta um conjunto de propriedades básicas que a caracterizam, conforme apresentado em Efing & Freitas (2008) e abaixo relacionadas:

[24] O *hash* é amplamente usado em computação e, especificamente para criptografia, tem um papel importante na extração da *string* (texto) que define a "impressão digital" do arquivo, conforme apresentado em http://www.ietf.org/rfc/rfc2104.txt, acesso em 23 de abril de 2009.

- Autenticidade: a assinatura é autêntica, pois quando um “usuário A” usa a chave pública do “usuário B” para decifrar um documento eletrônico, ele confirma que foi o “usuário B” e somente o “usuário B” quem assinou o documento;
- Integridade: a assinatura não pode ser forjada, pois somente o “usuário A” conhece sua chave privada e pode aplicá-la. Esta propriedade é garantida pela aplicação da função *hash*;
- Confiabilidade: o documento assinado não pode ser alterado, pois se houver qualquer alteração no texto criptografado este não poderá ser restaurado com o uso da chave pública. A assinatura é uma função *hash* do documento, porque ela não geraria o mesmo sumário se aplicada em outro documento;
- Veracidade: a assinatura tem a presunção de veracidade, pois o “usuário B” não precisa de nenhuma ajuda do “usuário A” para reconhecer à assinatura do “usuário A”;
- Não-repúdio: é a não recusa, ou seja, é a garantia de que o “usuário A”, que executou determinada transação de forma eletrônica, não poderá posteriormente negar sua autoria, visto que somente a sua chave privada poderia ter gerado aquela assinatura digital. Deste modo, a menos de um uso indevido da chave privada, fato que não exime de responsabilidade, o “usuário A” não pode negar a autoria da assinatura.

Um ponto importante é a verificação de um documento assinado digitalmente, ou seja, a validade do documento assinado eletronicamente. Para isto, duas tarefas são realizadas: uma aplicando-se o *hash* sobre o texto original, e outra buscando o resultado do *hash* utilizando-se a chave pública do algoritmo assimétrico utilizado. Comparando-se os dois resultados, o *hash* deverá ser idêntico nestas duas tarefas, o que garante a autenticidade do documento assinado, caso contrário, o documento não é verdadeiro. A Figura 2.4 mostra o processo de confirmação da assinatura digital sobre um documento eletrônico.

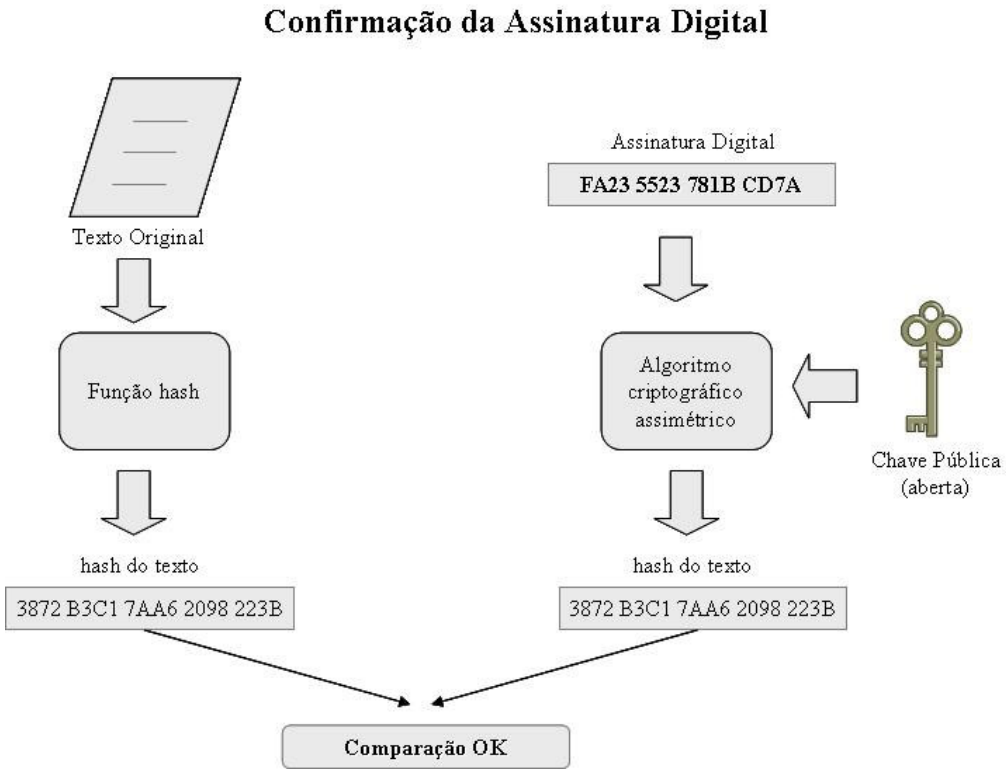

Figura 2.4 – Confirmação da Assinatura Digital

2.4. Considerações Finais

Este capítulo apresentou os aspectos fundamentais da segurança da informação, destacando os elementos essenciais na composição da informação considerada segura. Apresentou elementos de um contrato, transpondo-o para o ambiente digital no qual a assinatura eletrônica o valida juridicamente no padrão convencional dos contratos impressos, e, ao mesmo tempo, aponta para as necessidades de mecanismos de segurança para garantir a autenticidade das informações nas contratações via Internet.

Capítulo 3

Mecanismo de Autenticidade

Este capítulo especifica os detalhes do mecanismo proposto, considerando aspectos de sua implementação e detalhamento computacional. Apresenta como está especificado no servidor *Web* a lógica envolvendo os procedimentos de captura, tratamento, geração do instrumento contratual, encriptação, e envio ao usuário final (contratante ou consumidor), procurando ilustrar de maneira clara e objetiva o fluxo dos detalhes relacionados com o desenvolvimento do referido mecanismo de autenticidade.

3.1. Introdução

A Figura 3.1 ilustra o cenário geral proposto pelo mecanismo de autenticidade no qual o contratante tem disponível para baixar em sua máquina o registro técnico das transações efetuadas sobre *Web* do site do contratado, de forma a poder extrair um relatório com as informações pertinente a estes acessos, denominado de instrumento contratual. Do lado do contratado, tal mecanismo permite que o mesmo conteúdo seja armazenado e resgatado através de relatório de forma a confrontar as informações trafegadas entre as partes.

O instrumento contratual gerado é um arquivo digital com informações de identificação das partes envolvidas na contratação, ou seja, informações detalhadas do contratado e contratante, como nome completo, endereço, telefone, entre outros, e reúne também um conjunto de outras informações técnicas que identificam as máquinas envolvidas na operação através de informações providas pelo protocolo TCP/IP e o sistema que hospeda o portal de comércio eletrônico do contratado, bem como adiciona os elementos técnicos capturados durante todo o processo de interação do contratante com o portal de comércio eletrônico em sua aquisição do produto e/ou serviço. Sobre este arquivo digital, é aplicado um

método criptográfico desde sua geração inicial no servidor do contratado, usando uma senha única fornecida pelo contratante, de maneira que o arquivo fique encriptado em seu armazenamento e trâmite pela Internet, ou seja, quando este arquivo for enviado do fornecedor para o consumidor, de forma que somente o consumidor, com posse do arquivo instrumento contratual, possa abri-lo usando sua senha pessoal para tal operação.

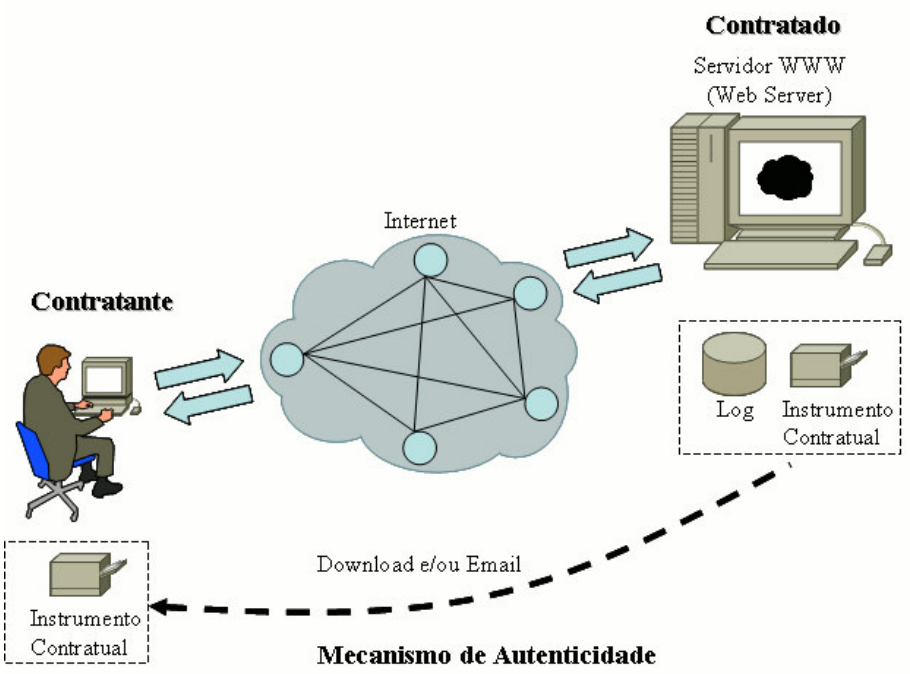

Figura 3.1 – Ambiente do Mecanismo de Autenticidade

3.2. Tráfego *Web* na Internet

As contratações realizadas no âmbito da Internet contemplam desde uma simples aceitação de um acordo estipulado em e-mail, até os mais complexos contratos postados em sites *Web* com aceitação por adesão por parte do contratante [Boiago Júnior, 2005]. Isto aponta para que, especificamente no contexto do tráfego *Web*, o nível de segurança das informações trafegadas através do protocolo HTTP na rede Internet garanta um mínimo de segurança através de mecanismo de criptografia. De fato, o uso do protocolo SSL[25] *(Secure Sockets Layer*) [Garfinkel, 1997] nas aplicações *Web* aplica criptografia entre o nível de

[25] O protocolo SSL foi desenvolvido pela Netscape para uso com seu navegador *Web*. O IETF (*Internet Engineering Task Force*) o utiliza como protocolo de criptografia básica em sua especificação TLS (*Transport Layer Security*), que é a recomendação de uso para o TCP/IP, conforme apresentado na RFC 2246, disponível em http://www.ietf.org/rfc/rfc2246.txt, acesso em 20 de junho de 2009.

sessão da pilha de protocolos TCP/IP de um lado e do outro da comunicação, evitando que as informações sejam trafegadas na rede Internet de forma aberta.

Nos diversos níveis do protocolo TCP/IP, há características que podem ser exploradas de forma maliciosa por *hackers* [Atkins at al, 1997] ou outros usuários mal intencionados. A exemplo do nível 2 da camada do protocolo TCP/IP (nível de enlace), o endereço da placa de rede de um computador em rede local pode ser adulterado por um outro usuário com intenções de redirecionar o tráfego para outra máquina naquela mesma rede local, gerando fraude para os usuários envolvidos neste problema. No nível 3 da camada do protocolo TCP/IP (nível de rede), o endereçamento IP também pode ser adulterado de forma maliciosa, desviando o tráfego agora não no contexto da rede local, mas sim ultrapassando as barreiras do ambiente do usuário e envolvendo o tráfego na rede Internet, conforme mostrado em Atkins at al (1997).

As aplicações desenvolvidas para o ambiente da Internet, seguindo a arquitetura cliente-servidor, utilizam-se da infra-estrutura padronizada do protocolo TCP/IP, estando, todavia, vulneráveis aos diversos problemas característicos deste ambiente.

Nas contratações via Internet, a exemplo de compras de produtos de consumo em sites eletrônicos de vendas[26], o contratante estará utilizando-se de toda a infra-estrutura de comunicação definida na rede Internet, ou seja, desde seu computador com o seu navegador *Web*, linhas de comunicação, provedor do serviço Internet, seguindo a comunicação até o servidor do contratado. Quando o contratante realiza uma operação de compra sobre o servidor do contratado através do seu navegador *Web*, está desprovido de mecanismos que comprovem a evidência da operação em sua relação contratual no nível computacional da operação realizada, ou seja, não há registros efetivos em seu computador que armazene e recupere o histórico realizado entre contratante e contratado. Assim, mesmo que haja embasamento jurídico, a ausência de mecanismos de comprovação da relação contratual (com os seus elementos: partes; objeto e demais condições ajustadas), certamente dificultará a viabilização dos direitos das partes (em juízo e extrajudicialmente).

3.3. Definição do Mecanismo de Autenticidade

No contexto do desenvolvimento do algoritmo de coleta e tratamento das informações, o mecanismo de autenticidade define um módulo de software (programa) instalado no servidor do contratado, integrado ao servidor *Web* do portal de comércio eletrônico, e está dividido em duas partes:

a) Servidor: programa que é instalado junto ao servidor *Web* do contratado e segue os padrões do protocolo HTTP, PHP e linguagem Java para suporte a extensões de software nas aplicações *Web*, sendo configurado como uma extensão dos serviços do servidor e oferecido ao cliente durante o procedimento de venda de produtos e/ou serviços daquele portal eletrônico;

b) Cliente: programa disponibilizado ao cliente, instalado em sua máquina, necessário para abertura do arquivo encriptado contendo o instrumento contratual gerado em sua operação de compra junto ao servidor. O ambiente do portal de comércio eletrônico está estruturado com páginas *Web* desenvolvido em linguagem HTML e PHP[27], de forma a atender a lógica de início, captura de dados e finalização de captura, conforme mostrado na Figura 3.2.

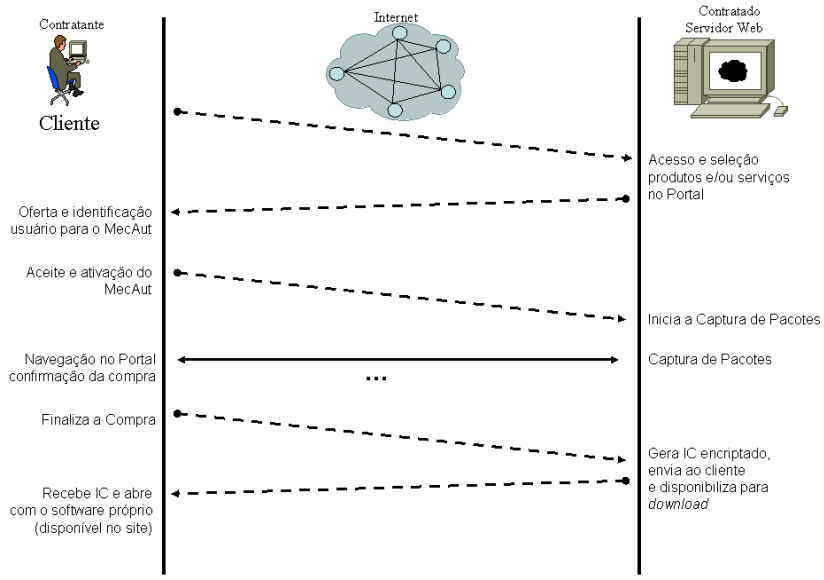

Figura 3.2 - Servidor e Cliente de Captura

[26] Como referência de site de comércio eletrônico, há o http://www.submarino.com.br, entre outros de mesma natureza. Acesso em 20 de junho de 2009.

Para efeito das avaliações do protótipo desenvolvido, foi utilizado o portal de comércio eletrônico chamado osCommerce[28], distribuído livremente na Internet e amplamente utilizado na maioria dos portais de comércio eletrônico.

Assim o mecanismo proposto define que o contratante, ao acessar o site *Web* do contratado através de seu navegador, tem a sua disposição um ícone com informativo sobre o mecanismo de autenticidade disponível para que o mesmo possa, com sua autorização e vontade explicitada [Boiago Júnior, 2005], ativá-lo para captura de pacotes para criação do instrumento contratual e, a partir desta aceitação, obter o registro de todas as informações propostas pelo mecanismo arquivadas e disponíveis a ele ao final de sua transação comercial.

Este procedimento inicial de navegação no site do contratado prevê uma verificação na qual, não havendo o aceite do contratante, o mesmo será avisado textualmente em janela *Web* sobre a continuidade dos acessos, porém sem a autenticidade garantida pelo mecanismo.

Tal como apresentado na Figura 3.2, a Figura 3.3 ilustra a integração necessária entre a lógica do programa do mecanismo de autenticidade para ativação e desativação do procedimento de captura de pacotes, bem como todos os demais recursos envolvidos no software desenvolvido, juntamente com as páginas *Web* do servidor do portal de comércio eletrônico. Ou seja, define-se o melhor ponto dentro do portal para se oferecer o uso e ativação do mecanismo de autenticidade e, ao final da transação comercial, interage-se com o portal para desativar a captura e executar o processamento das atividades envolvidas no mecanismo de autenticidade.

No caso do protótipo desenvolvido do mecanismo de autenticidade, integrado ao osCommerce, foi definido que o momento ideal a se oferecer o uso do mecanismo ao contratante seria no momento de sua finalização da compra, ou seja, quando o mesmo for executar o procedimento de confirmação de compra dos itens (produtos) selecionados, confirmação dos endereços de cadastro e entrega, e o pagamento final da compra (este processo também é definido como *Checkout*).

---

[27] Linguagem de desenvolvimento para ambiente *Web* integrado com HTML Maiores informações disponível em http://www.php.net/. Acesso realizado em 03 de maio de 2009.

[28] Pacote de software disponibilizado para uso livre como Portal de Comércio Eletrônico, sob licença GNU (General Public Licence), conforme disponível em http://www.oscommerce.com/. Acesso realizado em 03 de maio de 2009.

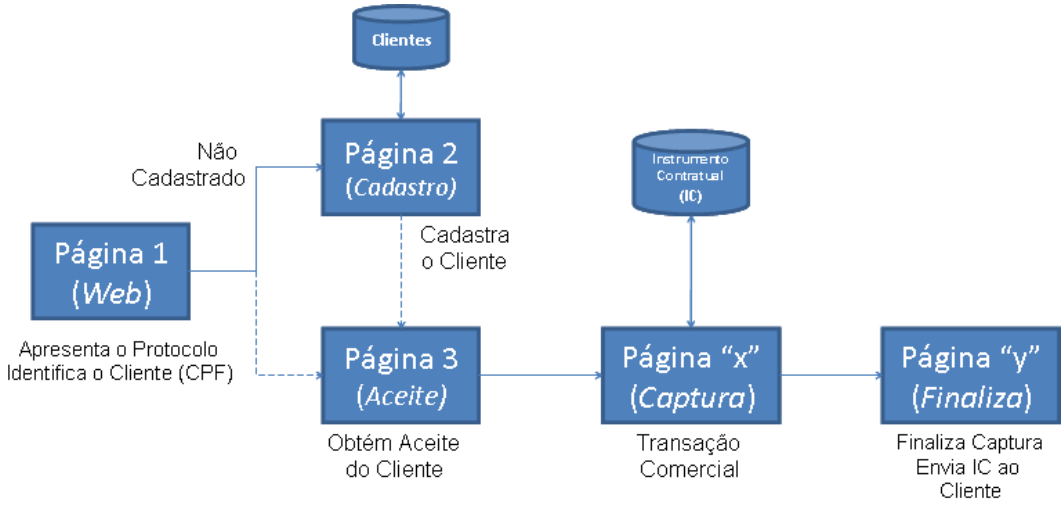

Figura 3.3 – Lógica de Início e Finalização da Captura

Esta lógica de controle do início e finalização[29] da captura das informações foi inserida nas páginas *Web* do portal de comércio eletrônico conforme as definições do ambiente do próprio portal em sua estrutura de início de relacionamento com o seu cliente no momento do *checkout*, ou seja, neste ponto estabelece-se a identificação do cliente e/ou seu cadastro, ativando-se o início das capturas de informações, uma vez que se tenha o seu aceite do uso do mecanismo de autenticidade por parte do contratante.

A partir deste ponto (ativação da captura), as informações-chave[30], que estão detalhadas no Capítulo 4, serão capturadas e armazenadas em uma estrutura própria de dados no servidor até a sua finalização, que também é comandada por uma instrução de código do mecanismo de autenticidade, escrita no padrão HTML e inserida na página *Web* que finaliza o procedimento de relacionamento com o cliente (contratante) do portal eletrônico.

Portanto, o controle de ativação das capturas das informações (início e fim) é administrado pelo fornecedor, ou seja, o mantenedor do portal de comércio eletrônico, de acordo com as instruções de configuração oferecidas pelas definições do mecanismo de autenticidade.

---

[29] O mecanismo de autenticidade define como "início e finalização" do processo de captura de informações na interface de rede o uso das respectivas frases (*Strings*): "PROTAUT:ATIVA" e "PROTAUT:FINALIZA". Estas frases são inseridas nas páginas do código-fonte do Portal de Comércio Eletrônico de forma a trafegarem na rede entre o servidor *Web* e o cliente final onde o analisador de captura é sensibilizado conforme estas instruções.

[30] A "**informação-chave**" é extraída dos dados trafegados na rede entre o servidor *Web* e o cliente com base em um conjunto de informações-chave definidas no mecanismo de autenticidade que permite selecionar os pontos importantes a tratar como informação capturada entre as partes.

3.4. Interfaces e Informações Armazenadas

O algoritmo desenvolvido define a captura de informações do contratante através de um processo inicial de interação com o mesmo na primeira vez que ele aceita a ativação e uso do mecanismo de autenticidade, e também a captura de informações técnicas referente aos acessos diretamente no site *Web* do contratado. Ou seja, na primeira interação do contratante, há um questionário a ser respondido por ele que define um cadastro inicial com seus dados próprios[31], que ficarão armazenadas no servidor, conforme definido na Tabela 3.1.

Após o processo inicial de cadastro, o contratante confirma a ativação do uso do mecanismo de autenticidade para que se iniciem as capturas das informações-chave nas páginas seguintes de navegação do portal eletrônico.

A partir deste ponto, as operações realizadas pelo contratante no site *Web* do contratado têm suas informações armazenadas em um arquivo de *log*[32], registrando estas informações no servidor do contratado para posterior geração do instrumento contratual. A Tabela 3.2 mostra as informações complementares que são armazenadas em cada interação do contratante no site do contratado.

Tabela 3.1 - Informações do Contratante no Cadastro Inicial

Informações do Contratante no Cadastramento Inicial	
Campo	**Descrição**
nome_contr	nome do contratante
cpf_contr	número do CPF do contratante
endereco_contr	endereço completo do contratante
telefone_contr	telefone de contato do contratante
senha_contr	senha do contratante para uso no processo criptográfico do instrumento contratual
email_contr	email do contratante para envio do instrumento contratual

[31] Dados principais do Contratante para registro nos arquivos de captura (base de dados do Cliente), que serão informados uma única vez no processo inicial de aceite do mecanismo de autenticidade. Estes dados são a base de identificação legal do Contratante.

[32] Em computação, *log* de dados é o termo utilizado para descrever o processo de registro de eventos relevantes num sistema computacional, normalmente armazenado para posterior análise.

Tabela 3.2 - Informações da Operação no Arquivo de *Log*

Informações da Operação no Arquivo de Log	
Campo	**Descrição**
numero_serie_ic	número sequencial de controle do instrumento contratual
Dados do Servidor (Contratado)	
nome_empresa_contratado	nome da empresa do contratado
CNPJ_empresa_contratado	número do CNPJ do contratado
endereco_contratado	endereço completo do contratado
MAC_address_contratado	número do MAC address do servidor do contratado
numero_IP_contratado	número IP do servidor do contratado
mascara_IP_contratado	máscara de rede da máquina do contratado
broadcast_IP_contratado	broadcast de rede da máquina do contratado
nome_servidor_contratado	nome do servidor do contratado
Dados do Cliente (Contratante)	
numero_IP_contratante	número IP da máquina do usuário contratante
nome_contratante	nome do contratante
CPF_contratante	número do CPF do contratante
endereco_contratante	endereço completo do contratante
telefone_contratante	telefone do contratante
Informações do Pacote Capturado	
data_pacote	data do pacote
hora_pacote	hora do pacote
ip_origem_pacote	número IP do pacote origem
ip_destino_pacote	número IP do pacote destino
porta_origem_pacote	número da porta TCP/IP (serviço) do pacote origem
porta_destino_pacote	número da porta TCP/IP (serviço) do pacote destino
dados_pacote	informações carregadas pelo pacote TCP/IP

Uma vez ativado, o mecanismo de autenticidade captura os pacotes sobre a interface de rede do servidor *Web* com base na seleção definida por um arquivo de informações-chave[33], cujo detalhamento deste procedimento está apresentado no Capítulo 4, que são lidas no início da execução do programa. Este procedimento torna flexível a seleção dos pacotes que irão compor o instrumento contratual gerado, pois permite ao administrador do site de comércio eletrônico definir informações-chave relacionadas ao negócio especificado no portal, de maneira a selecionar as capturas direcionadas aos interesses específicos do negócio, evitando assim uma captura excessiva de outros pacotes existentes na rede, muitas vezes relacionadas com controles do próprio protocolo Internet.

[33] Este arquivo está definido como texto seqüencial de palavras, a exemplo: http, get, post, pagamento, prazo, entre outros, ou seja, simples palavras texto que serão usadas para busca seletiva de conteúdo dentro dos pacotes

As informações capturadas não alteram ou danificam qualquer conteúdo trafegado pelo usuário, ou seja, o mecanismo de autenticidade provê um conjunto de informações que garantem a verificação da veracidade da operação realizada, porém sem invadir ou desrespeitar o sigilo do conteúdo trafegado. Isto, todavia, também é garantido pelo próprio recurso adicional do protocolo HTTP, chamado HTTPS[34], que, caso ativado como recurso do portal de comércio eletrônico, inclui a encriptação dos dados trafegados entre a máquina do contratante e o site *Web* do contratado, não sendo possível a abertura do conteúdo dos dados trafegados.

As informações de data e hora são consideradas fundamentais e essenciais em qualquer arquivo de armazenamento de *log*, principalmente no confronto entre dois arquivos que devem armazenar informações idênticas. Neste caso, o servidor do contratado deve garantir o sincronismo de relógio utilizando-se do serviço de rede NTP (*Network Time Protocol*)[35], no qual a data e hora do servidor *Web* do contratado estará sincronizado com a rede mundial de computadores, considerando também os ajustes de localização física do servidor (*time zone*), onde esta informação será usada em cada pacote capturado pelo mecanismo de autenticidade.

A informação relativa ao número IP da máquina do contratante capturada pelo mecanismo de autenticidade e armazenada no instrumento contratual contempla o seu IP público usado na Internet, ou seja, seu IP real que o unifica dentro da rede mundial de computadores. A *Request For Comments* (RFC) 1918[36] é amplamente usada nas redes corporativas e/ou residenciais, na qual o número IP usado no ambiente local do usuário é um número privado não válido na Internet pública. Associadamente faz-se o uso de técnicas de

---

capturados na rede, ou seja, para cada pacote capturado, só serão aceitos os pacotes que possuírem alguma das palavras listadas no arquivo das informações-chave.

[34] *Hypertext Transfer Protocol Secure* (HTTPS) é uma combinação do *Hypertext Transfer Protocol* e um protocolo de criptografia. O HTTP opera na camada de aplicação da arquitetura TCP/IP e, juntamente com um protocolo criptográfico, encripta e decripta as mensagens deste nível. Em 1994, a Netscape Communications definiu o uso do *Secure Sockets Layer* (SSL) como protocolo criptográfico para uso com seu navegador, porém tornou-se obsoleto pela definição e uso do *Transport Layer Security* (TLS), adotado como padrão nos navegadores *Web* desde o ano de 2000 e definido pela RFC 2818, conforme definição disponível em http://www.ietf.org/rfc/rfc2818.txt, acesso realizado em 20 de junho de 2009.

[35] O NTP é um protocolo para sincronização dos relógios dos computadores, ou seja, ele define um jeito para um grupo de computadores conversarem entre si e acertar seus relógios, baseados em alguma fonte confiável de tempo, como os relógios atômicos do Observatório Nacional, que definem a Hora Legal Brasileira. Disponível em http://ntp.br/, acesso realizado em 20 de junho de 2009.

[36] A RFC 1918 recomenda o uso de faixas de endereçamento IP para uso interno nas organizações, sem ter vínculo com a Internet Pública. Maiores informações disponível em http://www.ietf.org/rfc/rfc1918.txt, acesso realizado em 20 de junho de 2009.

firewall e NAT (*Network Address Translation*)[37] para permitir que usuários destas redes privadas acessem a Internet, o que mapeia diversas máquinas em um mesmo ambiente de rede local usando um único IP na Internet. No caso do mecanismo de autenticidade, para diferenciar o usuário atrás de uma rede privada que normalmente usa um único IP público, adicionalmente utiliza-se o número da sessão[38] *Web* que o usuário está conectado ao portal de comércio eletrônico de maneira a unificá-lo no seu acesso ao portal, garantindo que as informações capturadas e tratadas naquela sessão sejam únicas e exclusivas deste usuário.

Com as informações do servidor (contratado), do cliente (contratante) e todos os pacotes armazenados no arquivo de *log*, o mecanismo de autenticidade define a formatação de apresentação dos dados de saída em uma estrutura definida pelo XML[39] (*Extensible Markup Language*), os quais compõem o instrumento contratual disponibilizado ao contratante.

O arquivo XML é encriptado utilizando-se DES (*Data Encryption Standard*) que referencia os padrões de diversos protocolos utilizados mundialmente na Internet, conforme descrito em Schneier (1996). Este protocolo de criptografia trabalha com blocos de 64 bits, sendo um algoritmo simétrico[40]. Assim, ao ser simétrico, a chave usada para encriptação e decriptação do arquivo é a mesma, possuindo tamanho de 56 bits, tornando o algoritmo de rápido processamento considerando o arquivo XML a ser processado e garantido no âmbito do mecanismo proposto.

Desta forma, o contratante terá condições de gerar seu relatório diretamente a partir de sua máquina sem depender de outras informações do contratado, a exemplo de utilização de outros critérios de encriptação com uso de chaves assimétricas (dependência da troca de chaves públicas e privadas entre as partes). Apesar de o algoritmo simétrico exigir o compartilhamento da senha pessoal do contratante junto ao contratado para que ambos possam encriptar e desencriptar as informações do arquivo XML, esta senha está armazenada

---

[37] Consiste em reescrever os endereços IP origem que atravessam um Firewall ou roteador, com objetivo de conectar uma rede privada a Internet pública. Maiores informações disponível em http://tools.ietf.org/html/draft-ietf-nat-traditional-04, acesso realizado em 03 de maio de 2009.

[38] No exemplo do protótipo do Mecanismo de Autenticidade junto ao portal osCommerce, utilizou-se o controle de sessão do PHP conforme definido em http://br.php.net/manual/pt_BR/function.session-id.php. Acesso realizado em 03 de maio de 2009.

[39] O XML é uma linguagem definida como o formato universal para dados estruturados na *Web*. Esses dados consistem em tabelas, desenhos, parâmetros de configuração, etc. A linguagem então trata de definir regras que permitem escrever esses documentos de forma que sejam adequadamente visíveis ao computador. Maiores definições estão disponíveis em http://tools.ietf.org/html/rfc3688. Acesso realizado em 03 de maio de 2009.

[40] Há diversas técnicas de encriptação propostas em [Scheneier, 1996], como Lúcifer, Madryga, NewDES, IDEA, entre outras, que trabalham com conceitos próprios de chaves privadas ou públicas, aplicando técnicas simétricas ou assimétricas para encriptação dos respectivos arquivos.

no servidor do contratado de forma restrita, encriptada pelo método MD5[41], conforme ilustrado pela Figura 2.1, Capítulo 2.

Assim sendo, este procedimento garante que as informações armazenada durante a captura, ativada pelo contratante em sua navegação no portal de comércio eletrônico, estejam com o nível básico de segurança garantida pela criptografia aplicada no arquivo, o que impede que qualquer pessoa possa tomar posse do conteúdo das informações armazenadas.

Com posse do arquivo XML encriptado, o contratante poderá utilizar-se de um software adicional disponibilizado pelo contratado no próprio portal de comércio eletrônico para que o mesmo consiga abri-lo (desencriptar), utilizando-se de sua senha pessoal. Estas informações definem o instrumento contratual, que poderá ser visualizado em sua máquina local através de seu *browser* e impresso para efeitos documentacionais.

No âmbito jurídico, o instrumento contratual com as informações sobre as operações realizadas pelo contratante sobre o portal de comércio eletrônico do contratado permite ao mesmo comprovar o fato realizado, podendo solicitar elaboração de ata notarial em cartório, conforme apresentado em Rezende (1999). Neste instrumento jurídico, o tabelião relata aquilo que vê, ouve, verifica e conclui, com seus próprios sentidos. É o testemunho oficial de fatos narrados pelos notários no exercício de sua competência em razão de seu ofício. Neste momento, há a confirmação jurídica do mecanismo de autenticidade que registrou e relatou as operações de transação no âmbito da contratação via Internet, em que o instrumento contratual validado em ata notarial, juridicamente será tratado como prova contundente das operações do contratante sobre o sítio *Web* do contratado [Ayoub, 2009]. Este instrumento também confirma que as informações ali relatadas são resultados das operações entre o navegador do contratante e o servidor *Web* do contratado, e que a Internet é, porém, apenas um meio de comunicação entre os dois pontos, não havendo possibilidades de envolvimentos ou adulterações das informações por terceiros uma vez que o arquivo XML está protegido por criptografia e o mesmo conteúdo também é armazenado na máquina do contratado, podendo, em situações de litígio, ser solicitada a verificação de seu conteúdo conforme especificação do mecanismo de autenticidade.

---

[41] O MD5 (*Message-Digest Algorithm* 5) é um algoritmo de hash de 128 bits unidirecional desenvolvido pela RSA Data Security Inc., descrito na RFC 1321. No mecanismo de autenticidade, está sendo usado uma função em Java que aplica o hash para o armazenamento seguro das senhas do contratante. Maiores informações disponível em http://java.sun.com/j2se/1.4.2/docs/api/java/security/MessageDigest.html. Acesso realizado em 03 de maio de 2009.

3.5. Algoritmo de Captura e Armazenamento

O processo de captura das informações utiliza as facilidades disponíveis na estrutura da linguagem Java com as bibliotecas de interface com o nível do protocolo TCP/IP, que são recursos de software que disponibilizam informações do tráfego de rede, contemplando todas as camadas definidas por este protocolo. Isto permitirá a captura e visualização das informações técnicas definidas no mecanismo de autenticidade de forma aberta, possibilitando o armazenamento conforme definição do arquivo de *log*.

Os dados capturados seguem a estrutura definida na Tabela 3.3, que é um exemplo de captura de dados utilizando-se o pacote de software JPCAP[42], um conjunto de classes em Java que permite interagir com a interface de rede capturando pacotes sobre a interface física, mantendo-se a referência ao modelo didático do protocolo TCP/IP. As informações necessárias para atender aos campos definidos no mecanismo de autenticidade estão disponíveis no conjunto de dados capturados no *frame Ethernet*[43], conforme mostrado na Figura 3.4. As informações extraídas desta captura são armazenadas no arquivo de *log* de forma seqüencial e logicamente estruturado em um arquivo de dados no formato texto, sendo posteriormente processado para o formato XML e encriptado para proteção dos dados ali armazenados.

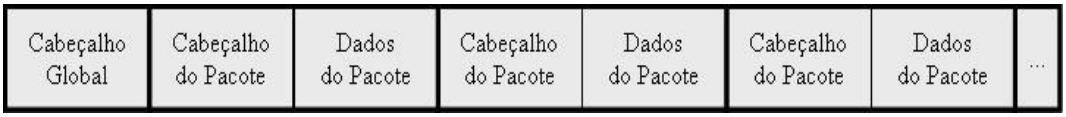

Figura 3.4 – Formato do Pacote Capturado

A técnica a ser usada na captura de pacotes baseia-se no uso da biblioteca *libpcap/winpcap*[44], que são bibliotecas de software de baixo nível disponível para desenvolvimento de código de programação, as quais provêem informações do tráfego de rede

[42] JPCAP é um pacote de software em Java com diversas classes que interage diretamente no nível de interface de rede permitindo capturar e enviar pacotes sobre a mesma. Pacote disponível em http://netresearch.ics.uci.edu/kfujii/jpcap/doc/. Acesso realizado em 07 de maio de 2009.

[43] O Frame *Ethernet* é a composição lógica de transmissão do pacote de dados em uma rede local usando o padrão IEEE 802.3 (http://www.ieee.org/web/standards/home/index.html), onde os computadores do contratado e contratante estão conectados. Nesta rede local, em cada um das respectivas máquinas, são capturados os pacotes de dados para análise e armazenamento do Mecanismo de Autenticidade.

[44] As bibliotecas Winpcap e Libpcap estão disponíveis para desenvolvimento de código de captura de pacotes em suas diversas interfaces de rede, conforme disponível em http://www.winpcap.org/ e http://www.tcpdump.org/, acesso realizado em 20 de junho de 2009.

de acordo com a interface utilizada, a exemplo para este trabalho, redes baseadas em protocolo *ethernet* e *wireless wifi*.

Esta biblioteca fornece funções que capturam pacotes no formato básico de rede, nas quais possuem um cabeçalho e um conjunto de dados separados de forma distinta. Dentro do protocolo TCP/IP, em sua classificação didática [Comer, 1991], é possível separar os diversos níveis de informações, separando os níveis do protocolo e as informações do usuário, possibilitando assim a gravação destas informações em arquivo de *log*. A Tabela 3.3 mostra o formato do pacote capturado na interface de rede, que é disponibilizado pelas classes da biblioteca JPCAP para a aplicação do mecanismo de autenticidade, o qual já separa os dados em seus níveis de informações técnicas, conforme definição da estrutura de dados armazenadas nos arquivos de dados o mecanismo de autenticidade.

Tabela 3.3 – Captura do Pacote de Dados

```
Sun May 03 19:54:32 GMT-03:00 2009 -> 192.168.15.52 -> 192.168.15.100 ->
80 -> 3313 -> Dados do Pacote:
..q.....}.....E...].@.@.;....4...d.P..(..}...wP..P.a..HTTP/1.1 302
Found..Date: Sun, 03 May 2009 22:54:32 GMT..Server: Apache/2.2.9
(Fedora)..X-Powered-By: PHP/5.2.6..Expires: Thu, 19 Nov 1981 08:52:00
GMT..Cache-Control: no-store, no-cache, must-revalidate, post-check=0,
pre-check=0..Pragma: no-cache..Location: http://py5jo.no-
ip.org/osc/catalog/checkout_payment.php..Content-Length : 0..Connection:
close..Content-Type: text/html; charset=iso-8859-1....
```

3.6. Processamento dos Dados – Geração do XML, Encriptação e Envio

Quando da finalização da compra pelo contratante, o que é apontado ao mecanismo de autenticidade pelo servidor do contratado logo após a fase de pagamento, encerra-se o processo de captura de pacotes sobre o arquivo de *log*. Este arquivo de *log* é serializado, ou seja, há um controle seqüencial feito pelo mecanismo de autenticidade que garante unicidade de cada arquivo a sessão executada pelo contratante, de maneira a ter individualizado os dados capturados para o posterior processamento e geração do instrumento contratual, detalhado no Apêndice A.

A Figura 3.5 ilustra o fluxo lógico do início, captura e finalização dos pacotes e posterior processamento, no qual é gerado o arquivo XML, aplicado criptografia simétrica e

enviado ao contratante via e-mail ao mesmo tempo em que é disponibilizado no site do contratado para que o contratante possa executar um *download* diretamente em sua máquina.

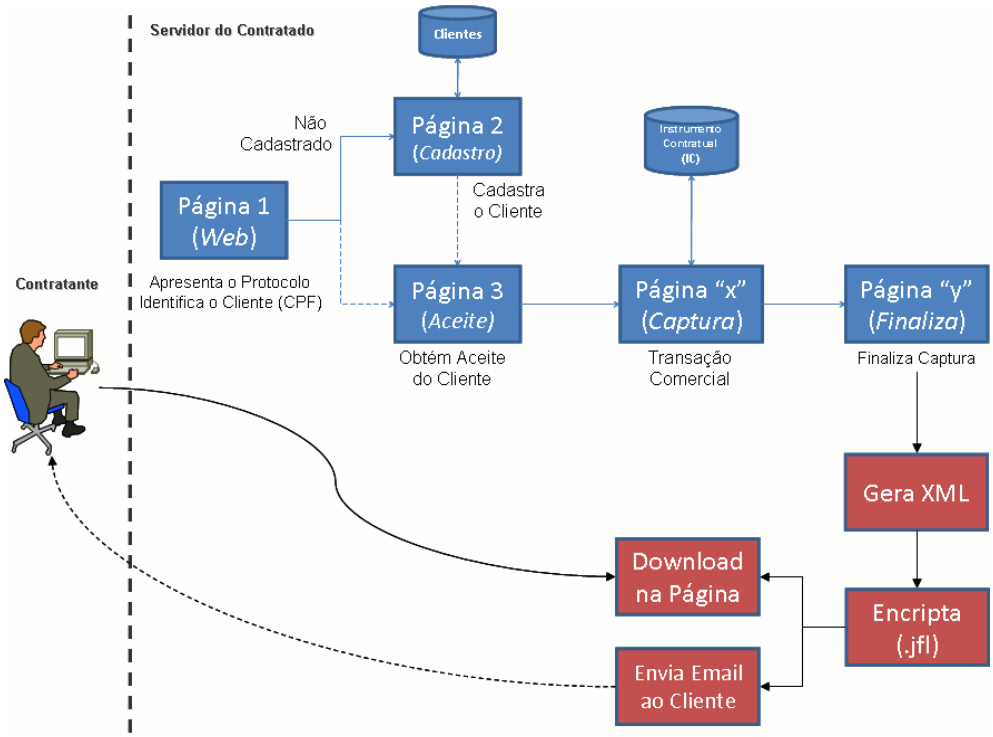

Figura 3.5 – Processamento dos Dados

O processo de geração do arquivo XML associa o uso da estrutura de estilos denominada XSL[45], que é um padrão para formatação de estilo que permite o transporte de variáveis de conteúdo, flexibilizando a construção do formato final do instrumento contratual com as variáveis associadas ao contratante, tais como: data, horário de acesso, site acessado, entre outras informações que são campos atribuídos ao documento gerado e transportado como informação entre o site do contratado e a máquina do contratante. Com isto, o arquivo XML gerado já contém todas as informações necessárias para a construção do instrumento contratual a ser mostrado ao contratante. A Tabela 3.4 ilustra um exemplo do arquivo XML gerada pelo mecanismo de autenticidade.

[45] O Extensible Stylesheet Language (XSL) especifica a apresentação de um conjunto de classes de documentos do XML trabalhando na definição de como os dados serão apresentados, considerando também o uso de campos variáveis para associar à conteúdos diversos. Maiores definições disponível no endereço http://www.w3.org/TR/xsl/. Acesso realizado em 09 de maio de 2009.

Tabela 3.4 – Exemplo de Arquivo XML

```
<?xml version='1.0' encoding='ISO-8859-1' ?>
<?xml-stylesheet type='text/xsl' href='mecaut.xsl' ?>
<mecaut>
<primeiro_texto>
<evento_data>
03/05/2009
</evento_data>
<evento_cidade>
Curitiba
</evento_cidade>

... (CONTINUA) DIVERSAS OUTRAS VARIÁVEIS NO FORMATO XSL ...

<site_responsavel_endereco_cidade>
Curitiba
</site_responsavel_endereco_cidade>
<site_responsavel_endereco_uf>
Parana
</site_responsavel_endereco_uf>
<site_responsavel_endereco_cep>
80.730-090
</site_responsavel_endereco_cep>
</primeiro_texto>
<segundo_texto>
<ic><![CDATA[Numero de Serie do Instrumento Contratual: 268
-------------------------------------------------
Dados do Servidor (Contratado):
Nome da Empresa: xxxxxxxxx <nome_empresa Ltda> xxxxxxxx
CNPJ da Empresa: xx.xxx.xxx/xxxx-xx
Endereco da Empresa: Rua xxxxxxxxxx,numero xx  - CEP: xxxxx-xxx - Curitiba-
Parana

..... (CONTINUA) ... DADOS CAPTURADOS PARA O INSTRUMENTO CONTRATUAL .....
```

Já no processo criptográfico, em que se considera o uso de mecanismo simétrico com senha única compartilhada entre o contratante e o contratado, foi usado um algoritmo de

criptografia simétrica disponível em Java baseado no DES (*Data Encryption Standard*), conforme apresentado no Capítulo 2, que faz parte de um conjunto de classes disponível no JCA (*Java Cryptography Architecture*)[46], uma biblioteca adicional de classes e métodos para programação de alto nível em Java para tratativa de segurança de informações.

O algoritmo segue a definição básica de uso na qual o arquivo de entrada está definido como o arquivo XML criado pelo mecanismo de autenticidade, sendo que a chave utilizada para a encriptação é a definida pelo contratante no momento inicial de seu cadastro no mecanismo de autenticidade junto ao site de comércio eletrônico. Com base no arquivo de entrada e a senha, aplica-se a criptografia simétrica e gera-se um novo arquivo de saída utilizando-se uma extensão definida pelo mecanismo de autenticidade chamada "JFL". Esta extensão é única e exclusiva para uso no mecanismo de autenticidade, e define o arquivo encriptado com as informações processadas individualmente para o contratante. Como há o mecanismo de controle seqüencial das informações de cada sessão (operação de compra) realizada pelo contratante, está definido que o nome do arquivo encriptado segue a estrutura: IC_xxxx.JFL, sendo "xxxxx" o número seqüencial.

Com base no algoritmo definido para execução do programa, logo após a encriptação do arquivo XML, o novo arquivo encriptado é armazenado no servidor do contratado e também enviado ao e-mail do contratante cadastrado na base de dados do mecanismo de autenticidade. Este procedimento tenta garantir que o contratante terá posse do arquivo encriptado com as informações de seu acesso ao site do contratado de maneira que possa abri-lo (desencriptá-lo) a qualquer momento de sua necessidade.

Como parte do mecanismo de autenticidade, o contratante deverá ter posse também do programa para abertura (desencriptação) do arquivo encriptado com extensão "JFL". Este programa é oferecido ao contratante para *download* na página do comércio eletrônico e também junto à página de *download* do arquivo encriptado ao final da transação comercial, de forma a garantir que o contratante tenha opções para a posse do arquivo.

Este programa possui a mesma rotina de encriptação e desencriptação usada no servidor do contratante para gerar o arquivo encriptado e o contratante, com posse deste programa em sua máquina, do arquivo encriptado, e de sua senha pessoal (a mesma

[46] O JCA é uma extensão da linguagem Java, também conhecido como JCE (Java Cryptography Extension) que amplia as funcionalidades de programação, incluindo facilidades para enriptação e desencriptação de dados, troca de chaves, autenticação de mensagens, verificação de conteúdo com funções HASH, entre outros. Maiores informações estão disponíveis no endereço http://java.sun.com/j2se/1.4.2/docs/guide/security/CryptoSpec.html. Acesso realizado em 09 de maio de 2009.

cadastrada no mecanismo de autenticidade e usada pelo servidor para encriptação), o contratante terá total condição de abrir o arquivo e ter o instrumento contratual relativo ao seu acesso junto ao portal de comércio eletrônico. Torna-se necessário este procedimento para garantir que o conteúdo gerado no servidor seja exatamente o mesmo entregue e visualizado pelo contratante.

3.7. Considerações Finais

Neste capítulo foram contextualizados os aspectos de segurança envolvidos nas operações realizadas na *Web* conforme apresentado em Garfinkel (1997). Também são tratados os aspectos jurídicos envolvidos nas provas no direito do consumidor [Nogueira, 1998] que realiza sua transação de contratação via Internet [Dias, 2004].

Também foi descrito a lógica definida para o mecanismo de autenticidade no qual o algoritmo descrito armazena as informações cadastrais do contratante, que servem de base jurídica para compor o documento final a ser apresentado como prova[47] (instrumento contratual), juntamente com os dados complementares das operações realizadas pelo contratante, o que comprovará, em situações de litígio, a autenticidade jurídica dos acessos entre a máquina do contratante e o site *Web* do contratado, relacionados por data, hora, número IP dos envolvidos, entre outras informações definidas na Tabela 3.2, as quais comprovam o fato realizado.

[47] Entendem-se como prova a comprovação do fato realizado na operação de contratação eletrônica entre o contratante (consumidor) e o contratado (fornecedor), materializado nas informações técnicas providas pelo documento gerado pelo mecanismo de autenticidade chamado Instrumento Contratual, que, em situações de litígio, tem o papel fundamental de tornar claro, irrefutável o fato realizado as vistas do decisor (Juiz). Segundo [Costa, 2008], "*não podemos perder de vista, entretanto, que o conceito de prova pode ser visto também por uma ótica menos objetivista, como aliás foi encarada no direito romano. Obviamente não nos interessa tentar embasar o comportamento arbitrário do juiz, mas sim evidenciar o papel retórico da prova e registrar que são possíveis dois pontos de vista: um ligado à demonstração do fato e outro ligado à persuasão do decisor*.".

Capítulo 4

Protótipo do Mecanismo de Autenticidade

Este capítulo apresenta os detalhes do protótipo desenvolvido, seus resultados e interações entre contratado e contratante.

4.1. Introdução

O contexto técnico do servidor do portal de comércio eletrônico considera o ambiente operacional Linux como suporte ao servidor *Web* do contratado e que o mesmo permite disponibilização de extensões de software ao usuário remoto, a exemplo do servidor *Web* Apache[48], bem como rotinas de criptografia e envio de e-mails, disponível na maioria dos sistemas operacionais Linux.

Já no ambiente do cliente, o mesmo necessitará executar um programa para abrir o instrumento contratual encriptado. Este programa está desenvolvido em linguagem Java, convertido para execução direta em ambiente Windows, de maneira que o contratante possa fazer o *download* diretamente em seu computador e tê-lo disponível localmente para abrir os arquivos contendo os Instrumentos Contratuais recebidos.

A linguagem de programação Java foi definida por apresentar a flexibilidade de tratamento das informações no ambiente de navegação Internet utilizando-se uma plataforma IDE[49] (*Integrated Development Environment*) NetBeans 6.1[50] para apoio do desenvolvimento

[48] O servidor Apache é um dos mais populares servidores HTTP para *Web* disponível na Internet para diversos sistemas operacionais. Maiores detalhes disponível em http://www.apache.org/, acesso em 20 de junho de 2009.
[49] **IDE**, do inglês ***Integrated Development Environment*** ou **Ambiente Integrado de Desenvolvimento**, é um programa de computador que reúne características e ferramentas de apoio ao desenvolvimento de software com o objetivo de agilizar este processo. Conforme apresentado em http://www.netbeans.org/kb/index.html, acesso realizado em 03 de maio de 2009.
[50] Platafoma IDE disponível em http://www.netbeans.org/index.html. Acesso realizado em 07 de junho de 2009.

integrado com ambiente de programação, verificações, testes e execução do código, o que fornece um ambiente robusto e consistente, e que melhora os resultados obtidos quanto a clareza, ausência de erros, modularidade e robustez do software desenvolvido.

A plataforma física de suporte ao desenvolvimento, execução e testes do contratado (servidor) é um PC com sistema operacional Linux Fedora 10[51] em ambiente de rede, executando as funcionalidades de servidor *Web* e portal de comércio eletrônico para as simulações de oferta de produtos e serviços no contexto do contratado (fornecedor), conforme definições do mecanismo de autenticidade.

A fase de prototipação deste trabalho para demonstração de conceitos considera a execução do mecanismo de autenticidade em ambiente controlado, no qual foi realizado sua integração a um portal de compras na *Web* (contratado), implementando o mecanismo entre o servidor instalado e as diversas máquinas clientes rodando o navegador do cliente (contratante).

O servidor, com o pacote de software osCommerce instalado, permitiu a integração do mecanismo de autenticidade e a experimentação em ambiente real de compras sobre o portal de comércio eletrônico, gerando os arquivos de *log* para que fossem verificados de acordo com os relatórios de acessos mapeados nas máquinas clientes, garantindo a confrontação real das informações auditadas no mecanismo proposto.

Isto mostrou que, em situações de litígio, nas quais o reclamante (contratante) emitirá o relatório de acessos de sua máquina sobre o referido site reclamado, o contratado deverá ter condições de validar as informações relatadas pelo cliente. De fato, isto estará mapeado no arquivo de *log* de seu servidor de forma a confirmar a operação frente ao instrumento contratual apresentado pelo contratante.

4.2. Estrutura Lógica do Protótipo

O protótipo usa as definições de orientação a objetos suportada pela linguagem Java, implementando diversas classes, objetos e relacionamentos entre eles. Em sua estrutura principal, o código considera a leitura dos arquivos de configuração inicial e um *loop* central (repetição) que analisa todos os pacotes que trafegam na interface de rede do servidor *Web*, conforme mostrado na Figura 4.1.

[51] Software de domínio público disponível em http://fedoraproject.org/. Acesso realizado em 20 de junho de 2009.

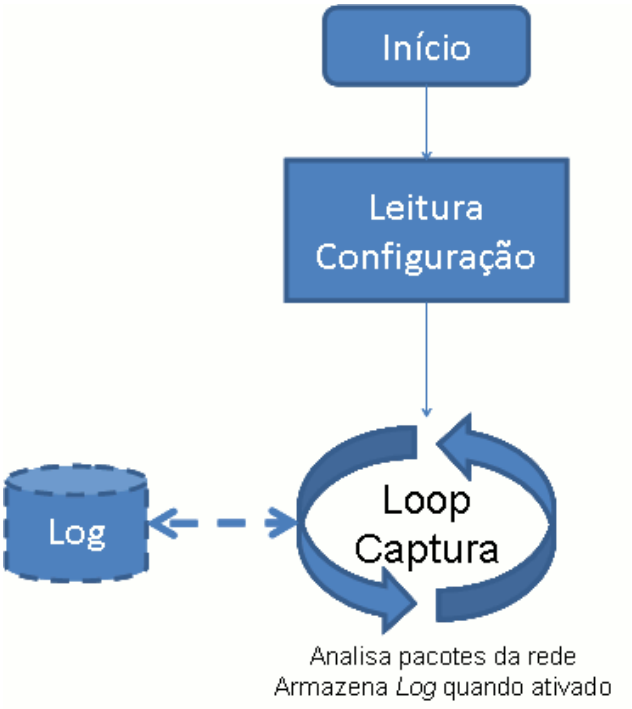

Figura 4.1 – Lógica Principal

Os arquivos de configuração do protótipo são flexíveis para permitir a especificação dos dados do fornecedor (contratado), informações técnicas de uso do próprio mecanismo, como portas do serviço *Web*, interface de rede para captura, entre outras que são necessárias para o funcionamento esperado do mecanismo. A Tabela 4.1 apresenta a estrutura básica das informações de configuração do servidor *Web* carregada no início da execução do protótipo.

Conforme apresentado no Capítulo 3, existe um arquivo de configuração que define um conjunto de informações-chave que são usadas como referência para a captura das informações trafegando na rede. Este arquivo também é lido em tempo inicial de execução e carregado em uma estrutura de dados (objeto) que serve como filtro para os pacotes capturados. Isto permite ao administrador do portal eletrônico do contratado aplicar um conjunto de palavras relacionadas ao conteúdo oferecido aos seus clientes de forma a otimizar as informações capturadas na rede entre o contratante e o portal eletrônico, ou seja, só serão capturados pacotes entre o servidor *Web* e o contratante que contenham informações-chaves do arquivo de configuração. A Tabela 4.2 mostra o arquivo de informações-chaves definidas no protótipo.

Tabela 4.1 - Configuração do Servidor *Web*

```
# Arquivo de configuracao do Mecanismo de Autenticidade
# Razao Social Fornecedor
xxxxxxxxxxxxxxx<nome_fornecedor>xxxxxxxxxxx

# CNPJ do Fornecedor
xx.xxx.xxx/xxxx-xx
```

... continua ...

```
# interface de captura
0

# diretorio do log do IC
/var/protaut/ticket

# diretorio de log
/var/log

# arquivo de log
protaut.log

# Porta Web do Servidor
80

# Porta SSL do Servidor
443
```

... continua ...

```
# SMTP Server
smtp.dominio.com.br

# User SMTP
usuario%dominio.com.br

# Senha SMTP
senhasenha

# E-mail Origem Envio IC SMTP
mecaut@dominio.com.br

# Nome SMTP
Mecanismo de Autenticidade
```

As palavras definidas neste arquivo estão relacionadas com o conteúdo das páginas *Web* que são trafegadas entre o servidor e o cliente, páginas estas que compõe a estrutura do portal de comércio eletrônico que é composto pela linguagem HTML, ou seja, estão relacionadas com o contexto do negócio jurídico. Estas palavras, em geral, são composições do código-fonte das páginas do portal eletrônico, que são escritas em uma linguagem textual, a exemplo do HTML, Java, PHP, Perl, Phyton, entre outras, em que, analisadas pelo

mecanismo de autenticidade, definem um filtro de seleção daqueles pacotes que serão processados e incluídos no instrumento contratual.

Tabela 4.2 - Informações-chave de seleção de captura

get
http
post
html
href
url
php
index
body
end
img
image
frame
java
javascript
applet
+++FIM+++

Como há a flexibilidade do administrador definir outras palavras, o mesmo pode correlacionar estas informações-chaves com o tipo e propósito dos produtos vendidos pelo portal, influenciando diretamente nos pacotes capturados pelo mecanismo de autenticidade que comporão o resultado final apresentado pelo instrumento contratual, ou seja, pelo menos uma das palavras definidas no arquivo estará contida no pacote capturado pelo mecanismo de autenticidade.

4.3. Base de Dados

O mecanismo de autenticidade utiliza-se de três estruturas de dados baseadas em arquivo seqüenciais e não relacionais[52]. Estes arquivos são trabalhados no momento da execução do protótipo (objetos) e alimentados conforme lógica do programa. São eles:

a) Cadastro dos clientes: é uma base de dados cadastrais dos clientes que aceitam a utilização do mecanismo de autenticidade. Nesta base, ficam armazenadas as informações de cadastro de cada cliente, tais como: nome, CPF, endereço, telefone, senha e e-mail, que são utilizados para composição da estrutura final dos dados de acessos de cada interação daquele cliente ao portal eletrônico, ou seja, a

[52] Estes arquivos são do tipo texto, gravados seqüencialmente no disco do servidor do fornecedor.

geração do *log* de acesso. A Tabela 4.3 apresenta um exemplo do arquivo de cadastro dos clientes, que é composta pela seguinte estrutura seqüencial separado por dois pontos (":"): CPF do cliente, nome, endereço, telefone, senha e e-mail;

Tabela 4.3 - Base de dados de cadastro dos clientes

```
22222222222:Joao Fabio Oliveira:Rua Carlos Benato, 750, 02:41 2222-2222:
rG6$V9MK51j7$iHIZ3uVBbyMrEQWHoD:joao.fabio@gvt.com.br
99999999999:Usuario Virtual:Rua da Paz, 123 - apto 1223:41 9999-9999:
&6$V9K1j7$iIZ3uVBbswrSDeEQWHoWeT:jose.maria@hotmail.com
33333333333:Teste de Usuario:Rua da Gloria, 25 - apto 11220:41 3333-9888:
$6$V9M1j7$iHIZ3uVBbyMrEQWHoD:usuario@pucpr.br
11111111111:Mais um teste:Rua da Vitoria, 2565 - casa 2:41 3333-4444:
9&#$V9MK7$iHIZ3uVBbyMaseqDh%:coelho@hotmail.com
```

b) "*Log*": é um arquivo criado em tempo de execução do mecanismo de autenticidade que possui todos os dados que identificam e individualizam o acesso de um cliente ao portal eletrônico. O "*log*" é criado somente quando o cliente aceita utilizar o mecanismo de autenticidade. Neste momento, é gerado um arquivo com nome único, com identificação seqüencial no nome[53], que possui informações técnicas de identificação do servidor, tais como: nome, CNPJ, endereço, número IP, máscara, endereço MAC; e também possui informações do cliente, tais como: número IP e os dados da base cadastrais do cliente. Neste mesmo arquivo, são armazenados seqüencialmente os dados capturados na interface de rede do servidor, conforme os filtros estabelecidos pelas informações-chave, que correspondem aos acessos do respectivo cliente daquela sessão. A Tabela 4.4 mostra a estrutura de informações existente dentro do *log* do cliente;

c) Controle seqüencial do *log*: é um controle numérico seqüencial de geração do *log* dos clientes, utilizado para a formação do nome e identificação individual de cada *log* correspondente ao acesso individualizado de cada cliente ao portal eletrônico.

[53] Exemplo: *log_268.txt*, onde o número 268 corresponde a um controle seqüencial e crescente do servidor para os acessos dos clientes para individualizá-los.

Tabela 4.4 - Estrutura de informações do *log* do cliente

```
Identificação Seqüencial do Instrumento Contratual

-----------------------------------------------

Dados do Servidor (Contratado)

-----------------------------------------------

Dados do Cliente (Contratante)

-----------------------------------------------

Pacotes Capturados

Data/Hora -> IP_Origem -> IP_Destino -> Porta_Origem -> Porta_Destino ->
Dados do Pacote (Texto)

INSTRUMENTO CONTRATUAL ENCERRADO---------------------------------------
```

4.4. Interação Contratado e Contratante

O mecanismo de autenticidade compõe-se de duas partes essenciais: a) código de captura, geração de *log,* processamento das informações (XML e Encriptação), e envio/disponibilização ao contratante, que roda no servidor *Web* do contratado; b) relacionamento entre contratado e contratante via interface *Web* através do portal eletrônico.

A primeira parte (código de captura) visa garantir que as informações trafegadas na rede entre o fornecedor e cliente sejam armazenadas, enviadas e disponibilizadas ao mesmo no final do processo, comandado pelo portal eletrônico.

Já a segunda parte (relacionamento com o cliente via *Web*), está relacionada à inserção dos comandos de identificação e cadastro do cliente, bem como ativação e desativação do processo de captura de pacotes uma vez tendo o aceite do cliente. O administrador do portal eletrônico deve colocar estes comandos no local apropriado de seu portal, ou seja, nas páginas iniciais e finais de maneira a obter-se uma interface clara com o usuário final.

No Apêndice A, é apresentado um exemplo de um instrumento contratual gerado a partir de uma compra executada sobre o portal de comércio eletrônico usado no protótipo do mecanismo de autenticidade.

Já no Apêndice B, segue a ilustração do início e finalização do procedimento do mecanismo de autenticidade junto ao protótipo desenvolvido que tem como base o portal eletrônico osCommerce, conforme apresentado no Capítulo 3.

4.5. Indicadores de Performance e Impactos

Para a execução do protótipo mecanismo de autenticidade, foi definido o uso do ambiente operacional Linux Fedora 10[54] rodando suas instalações de software padrão[55], ou seja, sem qualquer customização especial de parâmetros que modificasse o cenário após a instalação deste ambiente operacional. O suporte ao portal está sobre o servidor Apache[56] disponível também na instalação padrão do ambiente operacional. A máquina física utilizada baseia-se em um processador Pentium Core2Duo E4600[57], com dois processadores, possuindo 2 Gigabytes de memória física instalada, com dedicação exclusiva à execução do portal de comércio eletrônico osCommerce instalado para suporte aos testes do mecanismo de autenticidade.

Com este cenário definido, os indicadores de sucesso baseiam-se na performance da máquina frente ao processamento exigido pelo impacto do código em Java para captura de pacotes, processamento, encriptação e envio ao contratante, principalmente em se projetando um volume de acessos simultâneos de usuários executando compras e interações sobre o portal.

O método de captura das informações de performance estão baseados no protocolo SNMP[58] (*Simple Network Management Protocol*) habilitado no servidor e integrado ao portal de gerência Cacti[59], o qual disponibiliza um ambiente de visualização gráfica com capturas realizadas no padrão definido na ferramenta com sua instalação padrão (5 minutos a cada coleta de informações).

A Figura 4.2 ilustra o processamento da máquina servidor com o código em Java sendo executado para captura das informações. No pico de processamento destacado no

---

[54] Sistema Operacional de uso livre disponível em http://fedoraproject.org/. Acesso realizado em 10 de maio de 2009.

[55] A versão do ambiente operacional instalado é: "Linux version 2.6.27.9-73.fc9.i686 (mockbuild@) (gcc version 4.3.0 20080428 (Red Hat 4.3.0-8) (GCC)) #1 SMP Tue Dec 16 15:25:05 EST 2008".

[56] Servidor *Web* usado no ambiente do protótipo e disponível no endereço http://www.apache.org/. Acesso realizado em 10 de maio de 2009.

[57] Informação dos dois Processadores obtidos através do comando de console "dmesg": CPU0: Intel(R) Core(TM)2 Duo CPU E4600 @ 2.40GHz stepping 0d; e, CPU1: Intel(R) Core(TM)2 Duo CPU E4600 @ 2.40GHz stepping 0d.

[58] O SNMP (*Simple Network Management Protocol*) é um protocolo que roda no nível da aplicação da pilha TCP/IP, sendo executada nos diversos sistemas operacionais disponíveis na atualidade. Ele provê informações sobre diversos dispositivos do ambiente operacional, como uso de CPU, memória, ocupação de disco, etc. Maiores informações disponível em: http://www.ietf.org/rfc/rfc1157.txt. Acesso realizado em 10 de maio de 2009.

[59] Cacti é um pacote de software que disponibiliza um portal de gerência gráfica com inúmeros recursos de gestão de objetos com base em coletas de informações através do protocolo SNMP. Maiores informações disponíveis no endereço http://www.cacti.net/. Acesso realizado em 10 de maio de 2009.

gráfico, o percentual medido foi de 2,5% em cada processador no momento de realização de testes de execução junto ao portal. Estes testes foram realizados executando-se duas compras em paralelo em dois momentos distintos, conforme apresentado na Figura 4.2. Este parâmetro determina a carga de processamento do servidor em momento de navegação junto ao portal, ativação do mecanismo de autenticidade, captura de pacotes, finalização, processamento dos dados e envio ao contratante, etapas que definem o teste completo do protótipo e seu impacto sobre a máquina servidor.

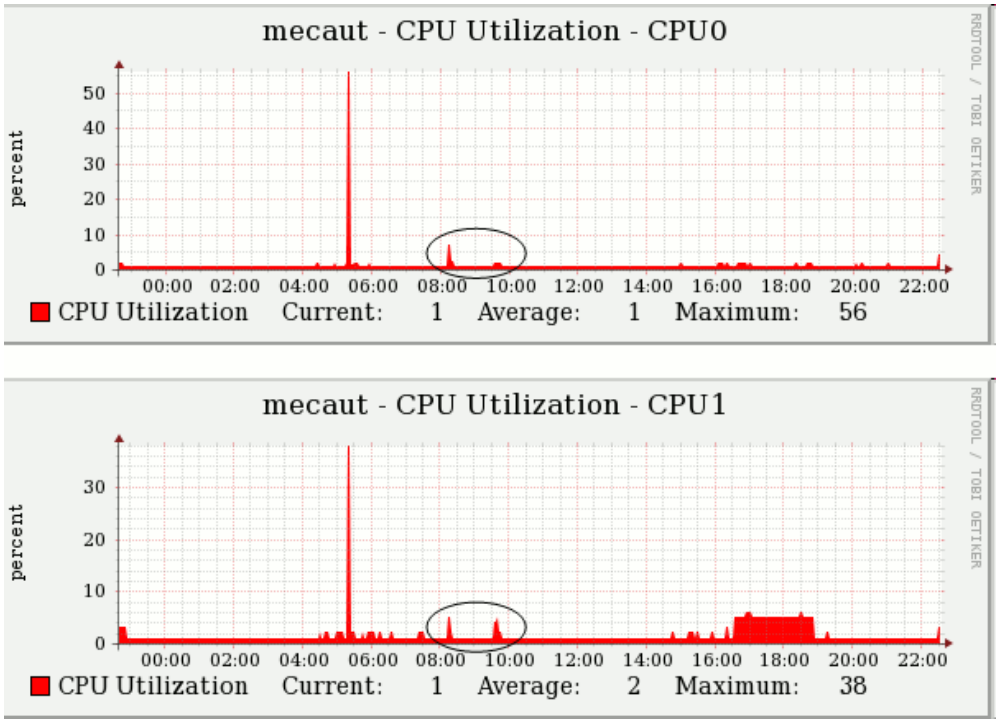

Figura 4.2 – Processamento no Servidor

A Figura 4.3 ilustra a projeção de carga para se determinar o limite de quantidade de acessos simultâneos de usuários ao servidor, o que determina o ponto de ampliação de processamento necessário para que os recursos computacionais dedicados a execução do mecanismo de autenticidade sejam aumentados.

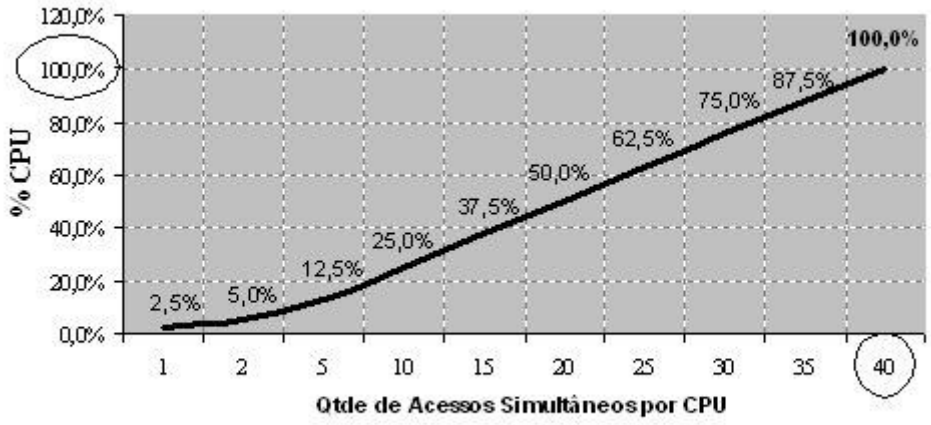

Figura 4.3 – Projeção de Carga de CPU do Servidor

Como conclusão, este percentual de processamento para o contexto de execução do protótipo não inviabiliza o uso do mecanismo no ambiente instalado.

4.6. Evolução e Trabalhos Futuros

O trabalho desenvolvido até este ponto, no qual há a concretização do instrumento contratual com informações técnicas comprobatórias do acesso realizado pelo contratante ao portal eletrônico do contratado, mostrou que há outros pontos a evoluir para melhoria de aspectos computacionais e jurídicos do mecanismo de autenticidade.

No teor da captura de pacotes e apresentação dos dados no formato do instrumento contratual, poder-se-ia trabalhar a técnica de mineração de dados, conforme apresentado em Silva (2007), para inferir informações mais específicas para a construção detalhada do documento comprobatório do objeto acessado, de maneira a ter um filtro sobre os pacotes técnicos e formatar os dados de maneira objetiva e associada a conceitos jurídicos dentro do instrumento contratual construído.

Silva (2007) define que a técnica de mineração de dados é um dos componentes do processo de descoberta do conhecimento, conhecido como *Knowledge Discovery in Databases* (KDD), no qual a mineração de dados é a etapa em KDD responsável pela seleção dos métodos a serem utilizados para localizar padrões nos dados, seguida da efetiva busca por

padrões de interesse numa forma particular de representação, juntamente com a busca pelo melhor ajuste dos parâmetros do algoritmo para a tarefa em questão.

De fato, para o mecanismo de autenticidade, há uma base rica de informações construída a partir da captura dos dados de rede, na qual a informação referente ao procedimento de aquisição do bem de consumo e/ou serviço pelo contratante está disponível em um conjunto de dados estruturados dentro do padrão definido pelo protocolo TCP/IP. Executar um processo de KDD sobre esta base, extraindo os dados essenciais e mais específicos para a construção do instrumento contratual é um processo evolutivo futuro e possível para enriquecer este trabalho.

Outro avanço pertinente para se estabelecer como evolução do mecanismo de autenticidade é a aplicação de criptografia assimétrica ao invés de simétrica. Neste processo, que compõe a Certificação Digital[60], o procedimento de troca de senhas deixa terem o compartilhamento único entre o contratante e contratado para o processo de criptografia e evolui para um mecanismo de chaves públicas e privadas, conforme apresentado no Capítulo 2, e garante que somente o contratante consegue abrir suas informações encriptadas.

Associado a aplicação do Certificado Digital, a gestão do instrumento contratual através de um Cartório Digital torna-se um ponto interessante a se investigar para evoluir o mecanismo de autenticidade associado ao procedimento de validação jurídica através do reconhecimento do instrumento com fé pública, possibilitando ao contratante ter o mecanismo de autenticidade integrado digitalmente desde o processo inicial de geração da informação até seu reconhecimento legal junto ao cartório, bem como demais facilidades de gestão de documentos digitais na Internet que podem ser providas pelo ambiente do cartório digital como serviço prestado ao usuário.

[60] A gestão de certificados digitais no Brasil possui estrutura definida pelo governo brasileiro em Medida Provisória (MP-2.200-2 de 24 de agosto de 2001), onde: "O **Instituto Nacional de Tecnologia da Informação - ITI** é uma autarquia federal vinculada à Casa Civil da Presidência da República, cujo objetivo é manter a **Infra-Estrutura de Chaves Públicas Brasileira – ICP-Brasil**, sendo a primeira autoridade da cadeia de certificação – AC Raiz.". Maiores informações disponíveis no endereço http://www.iti.gov.br/. Acesso realizado em 12 de maio de 2009.

4.7. Comentários Finais

A evolução do relacionamento entre pessoas, empresas, governos, entre outros, no ambiente Internet, caracteriza-se atualmente por um conjunto didático de classificação para qualificar os grupos que praticam comércio entre si, que são:

- B2B (*Business to Business*):

  São as transações de comércio entre empresas. Uma empresa vendendo para outra empresa é B2B. É a sigla mais conhecida e representam todas as outras abaixo quando generalizada. Um exemplo é a venda de material de escritório para empresas ou a compra de insumos para a produção de bens;

- B2C (*Business to Consumer*):

  É o comércio entre a empresa e o consumidor. Este é o mais comum, a exemplo do portal Amazon[61] que vende para o mundo todo [Baptista, 2008];

- C2C (*Consumer to Consumer*):

  Este é o comércio entre consumidores. Ele é intermediado normalmente por uma empresa (o dono do portal). O exemplo são os sites de leilão como o e-Bay[62] ou classificados como o Mercado Livre[63];

- B2G (*Business to Governement*):

  São as transações entre empresa e governo. Os exemplos comuns de B2G são licitações e compras de fornecedores;

- B2E (*Business-to-Employee*):

  Normalmente relacionado aos portais (Intranets) que atendem aos funcionários. Tem por objetivo de ser uma área central de relacionamento com a empresa. Através dele os funcionários podem, por exemplo, pedir material para sua área, gerir todos os seus benefício ou até utilizar processos de gestão dos funcionários (faltas, avaliações, inscrições em treinamentos, entre outros).

Como campo de estudo para aplicação do mecanismo de autenticidade, o comércio eletrônico baseado no conceito B2B (*Business to Business*) e B2C (*Business to Consumer*), são modelos de relacionamento que envolve o consumidor no qual o mecanismo de

---

[61] Portal de comércio eletrônico no modelo B2C, disponível em http://www.amazon.com/. Acesso realizado em 01 de novembro de 2009.
[62] Portal de comércio eletrônico no modelo C2C, disponível em http://www.ebay.com/. Acesso realizado em 01 de novembro de 2009.
[63] Portal de comércio eletrônico no modelo C2C, disponível em http://www.mercadolivre.com.br/. Acesso realizado em 01 de novembro de 2009.

autenticidade tornar-se uma interessante ferramenta para tratar os aspectos de segurança técnica e jurídica nas contratações eletrônicas, reforçando aspectos de segurança e confiança do fornecedor para o consumidor.

Como elemento comum, o portal *Web* é o componente existente em qualquer um dos modelos, seja na venda fornecedor-fornecedor (B2B), ou mesmo entre fornecedor-consumidor (B2C) [Marca, 2008], sendo o ponto de aplicação do mecanismo de autenticidade.

Há, portanto, um campo fértil de estudos a se desenvolver para detalhar os principais itens técnicos do mecanismo de autenticidade aplicado ao B2B e B2C, correlacionando-o também com aspectos jurídicos nas tratativas de litígio dentro deste contexto.

Capítulo 5

Conclusão

O comércio eletrônico, como prática de consumo, representa uma forma crescente de operação em que, de um lado o consumidor exercendo seu direito de consumo frente às opções disponíveis, e de outro o fornecedor buscando atender as necessidades do consumidor frente às oportunidades de negócio, desenvolvem entre si um fato jurídico através de Contrato Eletrônico que tem suas bases de relacionamento respaldada no Código de Defesa e Proteção do Consumidor (CDC), conforme apresentado no Capítulo 2 deste trabalho.

Fato este em que o mecanismo de autenticidade, através da geração do instrumento contratual com as informações técnicas da operação realizada pelo contratante sobre o portal de comércio eletrônico do contratado, propõe em sua essência, dar condições ao contratante de ter em sua posse um documento formatado, fornecido pelo próprio contratado, com forma e teor de uma estrutura de contrato entre as partes de maneira a explicitar tecnicamente o fato realizado no momento da contratação do serviço ou compra do produto. Há de se considerar o fato da boa vontade explicitada pelo fornecedor (contratado) em adotar este mecanismo junto ao seu portal de comércio eletrônico em que ele está fornecendo informações detalhadas ao seu cliente (contratante) sobre a operação realizada, reforçando aspectos de credibilidade e confiança entre as partes. Da mesma forma, o cliente, ao aceitar o uso do mecanismo, está reforçando os aspectos de segurança eletrônica em sua contratação, pois o instrumento contratual proverá a ele todos os dados comprobatórios da operação realizada, independentemente do seu nível de relacionamento com o fornecedor, o que o respalda, técnica e juridicamente sobre a operação de contratação registrada no documento digital.

Do ponto de vista jurídico, o contratante de posse do instrumento contratual terá condições de, frente à situação de litígio com o contratado, solicitar validação jurídica a um

cartório de notas e gerar o instrumento jurídico Ata Notarial, validando com fé pública o instrumento contratual e tornando comprovação legal do fato realizado.

Como apresentado neste trabalho, às garantias tecnológicas aplicadas no mecanismo de autenticidade, como as capturas, geração do XML, procedimento de encriptação e desencriptação dos dados, proporcionam a veracidade das informações geradas no portal do contratado e disponibilizadas ao contratante, o que valida o uso do mecanismo em qualquer portal de comércio eletrônico disponível na rede mundial de computadores.

Com a implementação do protótipo de software junto ao servidor *Web* do contratado, foi possível comprovar e viabilidade computacional dos objetivos propostos no Capítulo 1, onde os resultados esperados foram atingidos. O procedimento de captura dos dados, processamento (geração do instrumento contratual, formatação em XML, encriptação) e envio ao contratante, implementados em Java e executado junto ao servidor *Web*, resultou em um impacto de processamento de CPU que, em projeção de volume de acessos de usuários simultâneos ao portal de comércio eletrônico usado no protótipo, torna-se viável sua implementação pela escalabilidade de crescimento de infra-estrutura de hardware do servidor.

O aspecto prático de inserção do mecanismo de autenticidade junto ao portal de comércio eletrônico, definição do início e finalização da interação com o contratante para aceite do uso e recebimento do instrumento contratual, bem como a flexibilidade de configuração para parâmetros necessários à sua execução, torna-o simples e objetivo, realizando os resultados esperados.

O aspecto inovador deste trabalho, bem com as evoluções apontadas no Capítulo 4 para o mecanismo de autenticidade, o qualifica como diferenciado no contexto de soluções para portais de comércio eletrônico, as mesmo tempo que determina uma linha de pesquisa inédita no sentido de agregar critérios jurídicos às especificações técnicas, propiciando a sinergia entre duas linhas da ciência e evoluindo o conhecimento humano nos temas abordados.

Este trabalho foi desenvolvido através do projeto CNPq, "Segurança Jurídica nas Contratações Via Internet", Proc. No. 471627/2006-2 - Apoio a Projetos de Pesquisa/Edital MCT/CNPq 02/2006 – Universal, sob coordenação do Prof. Dr. Antônio Carlos Efing. Resultou deste projeto o registro no INPI (Instituto Nacional de Propriedade Industrial) sob o número 0000220806983610/2009, com patente de invenção (PI) número 0901094-7 sob o título “Protocolo de Autenticidade em Transações Eletrônicas”.

Houveram publicações relacionadas com o referido trabalho, uma no contexto internacional sendo apresentado artigo no *International Joint Conference on e-Business and Telecommunications* – ICETE, no ano de 2008[64], e outro artigo no XVII Encontro Preparatório do CONPEDI, no ano de 2008 em Salvador, Brasil[65].

Como interação e integração entre as áreas do conhecimento científico, através deste trabalho foi possível dar um importante passo em direção ao uso da tecnologia aplicada ao direito, principalmente nas discussões da validade técnica das informações sobre aspectos jurídicos com foco no consumidor final. Neste sentido, o mecanismo de autenticidade mostrou-se viável como uma ferramenta inovadora e de ampla aplicação nos portais eletrônicos B2C e C2C, reforçando a segurança jurídica através de elementos tecnológicos disponíveis dentro do próprio ambiente transacional usado na Internet.

[64] Artigo publicado na conferencia de 2008 com título "PROTOCOL OF AUTHENTICITY TO PROVIDE LEGAL SECURITY IN E-CONTRACTS - A Prototype", sendo seu *Abstract* disponível em http://www.ice-b.icete.org/Abstracts/2008/abstracts.htm. Acesso realizado em 01 de novembro de 2009.

[65] Artigo publicado na conferência de 2008 com título "A Adoção de Protocolo de Autenticidade para a Promoção da Segurança Jurídica na Contratação via Internet", disponível em http://www.conpedi.org/manaus/arquivos/anais/salvador/joao_fabio_de_oliveira.pdf. Acesso realizado em 01 de novembro de 2009.

Referências Bibliográficas

[Atkins at al, 1997] Atkins, Derek; Buis, Paul; Hare, Chris; Kelley, Robert; Nachenberg, Carey; B. Nelson, Anthony; Phillips, Paul; Ritchey, Tim; Sheldon, Tom; Snyder, Joel. *Internet Security Professional Reference, Second Edition*. New Riders Publishing, 1997.

[Behrens, 2005] Behrens, Fabiele. *A Assinatura Eletrônica como Requisito de Validade dos Negócios Jurídicos e a Inclusão Digital na Sociedade Brasileira*. Curitiba, 2005. 134 p., Dissertação de Mestrado, Centro de Ciências Jurídicas e Sociais, Pontifícia Universidade Católica do Paraná, 2005.

[Boiago Júnior, 2005] Boiago Júnior, José Wilson. *Contratação Eletrônica: Aspectos jurídicos*. Juruá Editora, Curitiba, 2005.

[Comer, 1991] Comer, Douglas E., *Internetworking With TCP/IP, Vol I: Principles, Protocols, and Architecture, Second Edition*. Prentice-Hall International, Inc., 1991.

[Dias, 2004] Dias, Jean Carlos. *Direito contratual no ambiente virtual*. Juruá Editora, 2ª. Edição. Curitiba, 2006.

[Garfinkel, 1997] Garfinkel, Simson; Spafford, Gene. *Web Security & Commerce*. O'Reilly & Associates, Inc., 1997.

[Mattos, 2007] Mattos, Analice Castor de; EFING, Antônio Carlos, *Aspectos relevantes dos contratos de consumo eletrônicos*. Curitiba, 2007. 156 p. Dissertação de Mestrado – Programa de Pós-graduação em Direito Econômico e Social, Pontifícia Universidade Católica do Paraná.

[Maia, 2005] Maia, Luis Paulo; Pagliusi, Paulo Sérgio, *Criptografia e Certificação Digital*. Disponível em: http://www.training.com.br/lpmaia/pub_seg_cripto.htm, Acesso em 26 de fevereiro de 2008.

[Nogueira, 1998] Nogueira, Tânia Lis Tizzoni. *A prova do direito do consumidor*. Juruá Editora, 1ª. Edição, Curitiba, 2003.

[Rezende, 1999] Rezende, Afonso Celso Furtado de. *Tabelionato de notas e o notário perfeito: direito de propriedade e atividade notarial*. Copola Livros, Campinas, 1997.

[Relvas, 2005] Relvas, Marcos. *Comércio Eletrônico*. Juruá Editora, Curitiba, 2006.

[Sêmola, 2003] Sêmola, Marcos. *Gestão da Segurança da Informação: visão executiva da segurança da informação*. Elsevier, Rio de Janeiro, 2003.

[Schneier, 1996] Schneier, Bruce, *Applied Cryptography Second Edition: protocols, algorithms , and source code in C*. John Wiley & Sons, Inc., 1996.

[Efing & Freitas, 2008] Efing, A.C.; Freitas, C.O.A. *Assinatura Digital: Necessidade ou Obrigação?* Direito e Questões Tecnológicas: aplicadas no desenvolvimento social. Curitiba: Juruá, 2008. p.131-155.

[Bacher, 2008] Bacher, Shane; Krishnan, Padmanabhan. *Implementing Secure Document Circulation: A Prototype*. ACM 978-1-59593-753-7/08/0003, SAC'08 March 16-20, 2008, Fortaleza, Ceará, Brazil, p.1452-1456.

[Santin, 2004] Santin, Altair Olivo. *Teias de Federações: Uma Abordagem Baseada em Cadeias de Confiança para Autenticação, Autorização e Navegação em Sistemas de Larga Escala*. Tese de Doutorado, 2004, Florianápolis/SC, Brasil, p.8-9.

[Silva, 2007] Silva, Marcelino Pereira dos Santos. *Mineração de Dados - Conceitos, Aplicações e Experimentos com Weka.* Universidade do Estado do Rio Grande do Norte (UERN), Mossoró, RN, Brasil, 2007, p.32-38.

[Costa, 2008] Costa, Henrique Araújo. *Reexame de Prova em Recurso Especial: A Súmula 7 do STJ.* Brasília: Thesaurus, 2008, p.18.

[Denning, 1982] Denning, Dorothy. *Criptography and Data Security.* Addison-Wesley, 1982.

[Landwehr, 2001] Landwehr, C. E. *Computer Security.* IJIS (2001) Vol.1, p.3-13, 2001.

[Shirley, 2000] Shirley, R. *Internet Security Glossary*. IETF, RFC 2828. 2000.

[Mackenzie, 1997] Mackenzie, D. E Pottinger, G. *Mathematics, Technology, and Trust: Formal Verification, Computer Security, and the U.S. Military*, IEEE Annals of the History of Computing, Vol. 19, No 3.1997.

[Ayoub, 2009] Ayoub, Luiz Roberto; Muller, Caroline da Cunha; Maia, Isaque Brasil. *A Ata Notarial e seu Valor como Prova*. Revista da EMERJ – Escola da Magistratura do Estado do Rio de Janeiro, Rio de Janeiro, 2009, Vol.12, número 46, p.59-68.

[Preneel, 2008] Preneel, Bart. *CRYPTOGRAPHIC ALGORITHMS: Successes, Failures and Challenges*. ICETE - ICE-B -2008, Porto, Portugal, 2008, p.21-27.

[Watanabe, 2008] Watanabe, Katsuya; Ando, Masaya; Sonehara, Noboru. *WEBSITE CREDIBILITY: A Proposal on an Evaluation Method for e-Commerce*. ICETE - ICE-B -2008, Porto, Portugal, 2008, p.484-487.

[Baptista, 2008] Baptista, Frederico de Carvalho; Saraiva, João de Sousa; Silva, Alberto Rodrigues da. *eCT: THE B2C E-COMMERCE TOOLKIT FOR THE WEBCOMFORT PLATFORM*. ICETE - ICE-B -2008, Porto, Portugal, 2008, p.225-228.

[Marca, 2008] Marca, David A. *E-BUSINESS INNOVATION Surviving the Coming Decades*. ICETE - ICE-B -2008, Porto, Portugal, 2008, p.5-16.

Apêndice A

Instrumento Contratual

Abaixo segue um exemplo de um instrumento contratual gerado a partir de uma compra executada sobre o portal osCommerce do protótipo do mecanismo de autenticidade.

A.1 Compra de um Produto no Protótipo do Mecanismo de Autenticidade

Considerando o procedimento de cadastro do contratante já realizado no portal do protótipo, bem como a ativação, execução da compra, e recebimento do instrumento contratual pelo contratante, a Figura A.1 ilustra o produto selecionado durante a compra que é identificada como informação técnica no instrumento contratual enviado ao contratante.

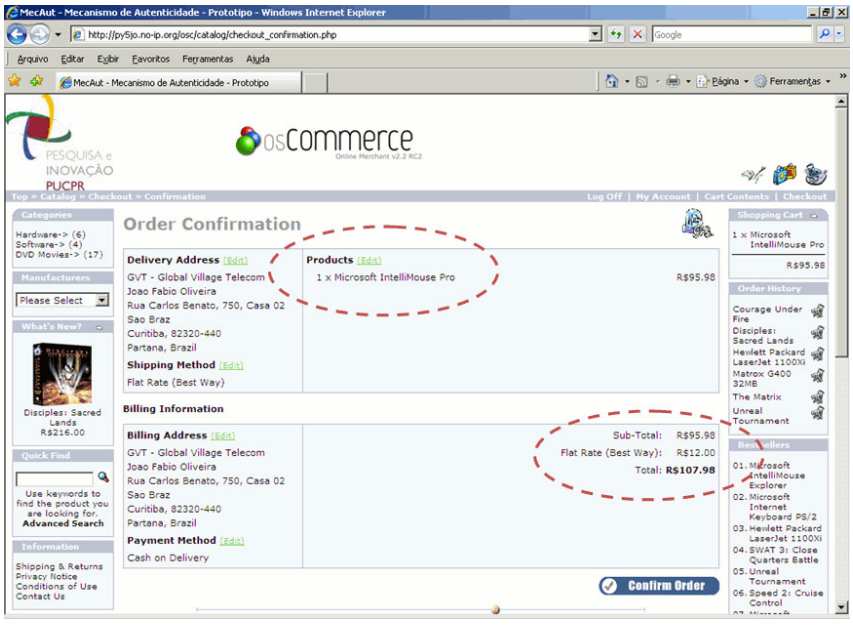

Figura A.1 – Compra de Produto no Portal

A.2. Identificação do Produto no Instrumento Contratual

A seguir, apresenta-se a identificação do produto adquirido pelo contratante no portal de comércio eletrônico do mecanismo de autenticidade. Os dados estão em formato técnico, considerando a estrutura hierarquia do protocolo TCP/IP conforme apresentado pelo mecanismo de autenticidade. Para efeito demonstrativo, alguns pacotes foram suprimidos do instrumento contratual mostrado na Tabela A.1 dado o volume de informações ali capturadas.

Tabela A.1 – Instrumento Contratual

INSTRUMENTO CONTRATUAL 268

Pelo presente instrumento contratual, é registrado o ajuste realizado entre:

Fornecedor:
Nome: Laboratorio de Direito e Tecnologia , CPF: 234.667.475-90
Endereço: Avenida Silva Jardim , 2345 , Conj. 330
Prado Velho , Curitiba , Parana , 80.730-090

Consumidor:
Nome: JOSE PEDRO DA SILVA , CPF: 12345654321
Endereço: RUA ABACAXI, 111
Email: joao.fabio@gvt.com.br

Por meio de acesso ao *website* **http://py5jo.no-ip.org/osc/catalog** através do Mecanismo de Autenticidade, aos **03/05/2009** , na cidade de **Curitiba - Parana** , às **19:54:44 hs**, em endereço eletrônico específico **http://py5jo.no-ip.org/osc/catalog** , e nele de comum acordo as partes celebraram contrato eletrônico de consumo, navegando em suas páginas e realizando a aquisição de sesus produtos e/ou serviços, conforme informações técnicas do Mecanismo de Autenticidade impressas e relatadas abaixo.

Desta forma, todos os dados relevantes relativos ao contrato ajustado, estão armazenados eletronicamente e codificados, podendo ser acessíveis às partes (com a ulitização da chave-senha registrada no momento do aceite do uso do Mecanismo de Autenticidade), bem como poderá compor ata notarial a ser lavrada por Tabelião Público em caso de necessidade de produção de prova para solução de litígio.

Portanto, as informações constantes neste instrumento contratual estão arquivadas tanto na máquina do fornecedor como na máquina do consumidor, sendo em princípio desnecessária a impressão física destes dados. As mesmas informações integram mensagem eletrônica enviada para o endereço: ***joao.fabio@gvt.com.br*** .

GLOSSÁRIO:
WEBSITE: Um grupo de documentos HTTP relacionados e arquivos associados, scripts e bancos de dados que residem em um servidor na World Wide Web.
INTERNET: Abreviatura de internetwork (ligação entre redes, interligação de redes), ou seja, é a rede que liga computadores no mundo inteiro.
HTTP (Acrônimo de Hyper Text Transfer Protocol):protocolo cliente/servidor usado para acessar informações na World Wide Web.

WWW (Acrônimo de World Wide Web): Conjunto totalmente interligado de documentos em hipertexto que residem em servidores HTTP no mundo inteiro.
HOME PAGE: Página inicial que permite o acesso a um conjunto de páginas da WWW e outros arquivos em um website.
++++++++++++: Separador de pacotes capturados pelo Mecanismo de Autenticidade. As informações técnicas capturadas estão descritas em cada pacote de rede capturado e mostrados abaixo entre cada identificador, em formato sequencial contemplando todos os pacotes relevantes capturados nesta sessão.

MECANISMO DE AUTENTICIDADE:
Numero de Serie do Instrumento Contratua l: 268 ---------- --------- Dados do Servidor (Contratado): Nome da Empresa: Globalcase Consultoria e Assessoria Ltda CNPJ da Empresa: 01.614.016/0001-57 Endereco da Empresa: Rua Carlos Benato, 750, Casa 02 - CEP: 82320-440 - Curitiba - Parana MAC Address do Servidor: 0:1d:7d:f6:b5:d d: Numero IP do Servidor: 192.168.15.52 Marcara do Servidor: 255.255.255.0 Broadcast do Servidor: 192.168.15.255 Nome do Servidor: core2duo ---------- --------- Dados do Cliente (Contratante): Numero IP do Cliente: 192.168.15.100 Nome do Cliente: JOSE PEDRO DA SILVA CPF do Cliente: 12345654321 Endereco do Cliente: RUA ABACAXI, 111 Telefone do Cliente: 23242323 ---------- --------- <++++++++++++>Sun May 03 19:54:22 GMT-0 3:00 2009 -> 192.168.15.52 -> 192.168.15 .100 -> 80 -> 3312 -> Dados do Pacote: . .q.....}.....E.....@.@..l...4...d.P....* .~..hP....3..HTTP/1.1 200 OK..Date: Sun, 03 May 2009 22:54:22 GMT..Server: Apach e/2.2.9 (Fedora)..X-Powered-By: PHP/5.2. 6..Content-Length: 1411..Connection: clo se..Content-Type: text/html; charset=iso -8859-1....<title>Mecanismo de Autentici dade - PUC-PR</title>.<body bgcolor=ffff ff text=3333aa>.<hr noshade>..<script la nguage="javascript">. function clos eWin() {. window.close();. }.</script>..<table width=100% border=0 bordercolor=000000 cellspacing=0 cellpad ding=3>.<td width=100% align=left valign =top>.<font size=3 face="tahoma,arial">. ..
.
..Mecanismo de Autenticidade
.
 .<font size=2 face="tahoma,arial">.A par tir deste ponto, todos os pacotes de red e relevantes para o Mecanismo de Autenti cidade estao sendo capturados e armazena dos para a geracao do INSTRUMENTO CONTRA TUAL que sera enviado a voce via email n o final da transacao comercial, e tambem estara disponivel no site para download . .
.Feche esta pagina e retorne ao < strong> Checkout , continuando o processo de compra e pagamento do seu produto e/ou servico. .
.Observe que na finalizacao de sua compra, havera uma chamada (click) para voce fazer o downl oad do INSTRUMENTO CONTRATUAL, bem como do software necessario para abri-lo em s eu computador, uma vez que ele estara en criptada para sua seguranca..
.O INST RUMENTO CONTRATUAL tambem sera enviado a o email cadastrado no ambiente do Mecani smo de Autenticidade..
.Para c <++++++++++++>Sun May 03 19:54:32 GMT-0 3:00 2009 -> 192.168.15.52 -> 192.168.15 .100 -> 80 -> 3313 -> Dados do Pacote: . .q.....}.....E...].@.@.;....4...d.P..(.. }...wP..P.a..HTTP/1.1 302 Found..Date: S un, 03 May 2009 22:54:32 GMT..Server: Ap ache/2.2.9 (Fedora)..X-Powered-By: PHP/5 .2.6..Expires: Thu, 19 Nov 1981 08:52:00 GMT..Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-chec k=0..Pragma: no-cache..Location: http:// py5jo.no-ip.org/osc/catalog/checkout_pay ment.php..Content-Length: 0..Connection: close..Content-Type: text/html; charset =iso-8859-1.... <++++++++++++>Sun May 03 19:54:32 GMT-0 3:00 2009 -> 192.168.15.100 -> 192.168.1 5.52 -> 3314 -> 80 -> Dados do Pacote: . .}.....q.....E....u@.....d...4...P... +).l.P.....GET /osc/catalog/checkout_p ayment.php HTTP/1.1..Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg , application/x-shockwave-flash, applica tion/vnd.ms-excel, application/vnd.ms-po werpoint, application/msword, applicatio n/xaml+xml, application/vnd.ms-xpsdocume nt, application/x-ms-xbap, application/x -ms-application, */*..Referer: http://py 5jo.no-ip.org/osc/catalog/checkout_shipp ing.php..Accept-Language: pt-br..UA-CPU: x86..Accept-Encoding: gzip, deflate..Us er-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; GTB5; .NET CLR 2.0. 50727; .NET CLR 3.0.04506.30; .NET CLR 3 .0.04506.648)..Host: py5jo.no-ip.org..Co nnection: Keep-Alive..Cache-Control: no- cache..Cookie: osCsid=700tlibrd13am1k0q1 jqr7ofk2.... <++++++++++++>Sun May 03 19:54:32 GMT-0 3:00 2009 -> 192.168.15.52 -> 192.168.15 .100 -> 80 -> 3314 -> Dados do Pacote: . .q.....}.....E...O)@.@.F....4...d.P..).l .....P...^u..HTTP/1.1 200 OK..Date: Sun, 03 May 2009 22:54:32 GMT..Server: Apach e/2.2.9 (Fedora)..X-Powered-By: PHP/5.2. 6..Expires: Thu, 19 Nov 1981 08:52:00 GM T..Cache-Control: no-store, no-cache, mu st-revalidate, post-check=0, pre-check=0 ..Pragma: no-cache..Connection: close..T ransfer-Encoding: chunked..Content-Type: text/html; charset=iso-8859-1....20bb.. <!doctype

html public "-//W3C//DTD HTML 4.01 Transitional//EN">.<html dir="LTR" lang="en">.<head>.<meta http-equiv="Cont ent-Type" content="text/html; charset=is o-8859-1">.<title>MecAut - Mecanismo de Autenticidade - Prototipo</title>.<base href="http://py5jo.no-ip.org/osc/catalog /">.<link rel="stylesheet" type="text/cs s" href="stylesheet.css">.<script langua ge="javascript"><!--.var selected;..func tion selectRowEffect(object, buttonSelec t) {. if (!selected) {. if (document .getElementById) {. selected = docu ment.getElementById('defaultSelected');. } else {. selected = document.a ll['defaultSelected'];. }. }.. if (selected) selected.className = 'moduleRo w';. object.className = 'moduleRowSelec ted';. selected = object;..// one butto n is not an array. if (document.checkou t_payment.payment[0]) {. document.che ckout_payment.payment[buttonSelect].chec ked=true;. } else {. document.checko ut_payment.payment.checked=true;. }.}.. function rowOverEffect(object) {. if (o bject.className == 'moduleRow') object.c lassName = 'moduleRowOver';.}..function rowOutEffect(object) {. if (obje <++++++++++++++>Sun May 03 19:54:32 GMT-0 3:00 2009 -> 192.168.15.52 -> 192.168.15 .100 -> 80 -> 3314 -> Dados do Pacote: . .q.....}.....E...O*@.@.F....4...d.P..).q .....P.......ct.className == 'moduleRowO ver') object.className = 'moduleRow';.}. //--></script>.<script language="javascr ipt"><!-- .function check_form() {. var error = 0;. var error_message = "Error s have occured during the process of you r form.\n\nPlease make the following cor rections:\n\n";. var payment_value = nu ll;. if (document.checkout_payment.paym ent.length) {. for (var i=0; i<docume nt.checkout_payment.payment.length; i++) {. if (document.checkout_payment.p ayment[i].checked) {. payment_val ue = document.checkout_payment.payment[i].value;. }. }. } else if (docu ment.checkout_payment.payment.checked) { . payment_value = document.checkout_p ayment.payment.value;. } else if (docum ent.checkout_payment.payment.value) {. payment_value = document.checkout_paym ent.payment.value;. }... if (payment_v alue == null) {. error_message = erro r_message + "* Please select a payment m ethod for your order.\n";. error = 1; . }.. if (error == 1) {. alert(erro r_message);. return false;. } else { . return true;. }.}.//--></script>.< /head>.<body marginwidth="0" marginheigh t="0" topmargin="0" bottommargin="0" lef tmargin="0" rightmargin="0">.<!-- header //-->.<table border="0" width="100%" ce llspacing="0" cellpadding="0">. <tr cla ss="header">. <td valign="middle"><a href="http://www.ppgia.pucpr.br/pesquisa /forense/"><img src="images/pesqpuc.jpg" border="0" alt="MecAut - Mecanismo de A utenticidade - Prototipo" title=" <++++++++++++++>
<++++++++++++++>
<++++++++++++++>

... muitos pacotes ...

<++++++++++++++>
<++++++++++++++>
<++++++++++++++>Sun May 03 19:54:32 GMT-0 3:00 2009 -> 192.168.15.52 -> 192.168.15 .100 -> 80 -> 3314 -> Dados do Pacote: . .q.....}.....E...O9@.@.E....4...d.P..).. 0....P....Q..order="0" alt="" width="11" height="14"></td>. </tr>.</table>.<tab le border="0" width="100%" cellspacing=" 0" cellpadding="1" class="infoBox">. <t r>. <td><table border="0" width="100% " cellspacing="0" cellpadding="3" class= "infoBoxContents">. <tr>. <td><img s rc="images/pixel_trans.gif" border="0" a lt="" width="100%" height="1"></td>. </ tr>. <tr>. <td class="boxText"><tabl e border="0" width="100%" cellspacing="0 " cellpadding="0"><tr><td align="right" valign="top" class="infoBoxContents"><sp an class="infoBoxContents">1 x ;</td><td valign="top" class="inf oBoxContents"> **Microsoft IntelliMouse Pro**</t d></tr></table></td>. </tr>. <tr>. <td class="boxText"><img src="images/pix el_black.gif" border="0" alt="" width="1 00%" height="1"></td>. </tr>. <tr>. <td align="right" class="boxText">**R$95. 98**</td>. </tr>. <tr>. <td><img src= "images/pixel_trans.gif" border="0" alt= "" width="100%" height="1"></td>. </tr> .</table>.</td>. </tr>.</table>. </td>. </tr>.<!-- shopping _cart_eof //-->.<!-- customer_orders //- ->. <tr>. <td>.<tabl e border="0" width="100%" cellspacing="0 " cellpadding="0">. <tr>. <td height ="14" class="infoBoxHeading"><img src="i mages/infobox/corner_right_left.gif" bor der="0" alt="" width="11" height="14"></ td>. <td width="100%" height=" <++++++++++++++>Sun May 03 19:54:32 GMT-0 3:00 2009 -> 192.168.15.52 -> 192.168.15 .100 -> 80 -> 3314 -> Dados do Pacote: . .q.....}.....E...O9@.@.E....4...d.P..).. 0....P....Q..order="0" alt="" width="11" height="14"></td>. </tr>.</table>.<tab le border="0" width="100%" cellspacing=" 0" cellpadding="1" class="infoBox">. <t r>. <td><table border="0" width="100% " cellspacing="0" cellpadding="3" class= "infoBoxContents">. <tr>. <td><img s rc="images/pixel_trans.gif" border="0" a

lt="" width="100%" height="1"></td>. </ tr>. <tr>. <td class="boxText"><tabl e border="0" width="100%" cellspacing="0 " cellpadding="0"><tr><td align="right" valign="top" class="infoBoxContents"><sp an class="infoBoxContents">1 x ;</td><td valign="top" class="inf oBoxContents"> **Microsoft IntelliMouse Pro**</t d></tr></table></td>. </tr>. <tr>. <td class="boxText"><img src="images/pix el_black.gif" border="0" alt="" width="1 00%" height="1"></td>. </tr>. <tr>. <td align="right" class="boxText">**R$95. 98**</td>. </tr>. <tr>. <td><img src= "images/pixel_trans.gif" border="0" alt= "" width="100%" height="1"></td>. </tr> .</table>.</td>. </tr>.</table>. </td>. </tr>.<!-- shopping _cart_eof //-->.<!-- customer_orders //- ->. <tr>. <td>.<tabl e border="0" width="100%" cellspacing="0 " cellpadding="0">. <tr>. <td height ="14" class="infoBoxHeading"><img src="i mages/infobox/corner_right_left.gif" bor der="0" alt="" width="11" height="14"></ td>. <td width="100%" height=" -> Dad os do Pacote: ..q.....}.....E...O9@.@.E. ...4...d.P..)..0....P....Q..order="0" al t="" width="11" height="14"></td>. </tr >.</table>.<table border="0" width="100% " cellspacing="0" cellpadding="1" class= "infoBox">. <tr>. <td><table border= "0" width="100%" cellspacing="0" cellpad ding="3" class="infoBoxContents">. <tr> . <td><img src="images/pixel_trans.gi f" border="0" alt="" width="100%" height ="1"></td>. </tr>. <tr>. <td class= "boxText"><table border="0" width="100%" cellspacing="0" cellpadding="0"><tr><td align="right" valign="top" class="infoB oxContents">1 x </td><td valign=" top" class="infoBoxContents">**Microsoft IntelliMouse Pro**</td></tr></table></td>. </ tr>. <tr>. <td class="boxText"><img src="images/pixel_black.gif" border="0" alt="" width="100%" height="1"></td>. < /tr>. <tr>. <td align="right" class= "boxText">**R$95.98**</td>. </tr>. <tr>. <td><img src="images/pixel_trans.gif" border="0" alt="" width="100%" height="1 "></td>. </tr>.</table>.</td>. </tr>.< /table>. </td>. </tr >.<!-- shopping_cart_eof //-->.<!-- cust omer_orders //-->. <tr>. <td>.<table border="0" width="100%" cellspacing="0" cellpadding="0">. <tr> . <td height="14" class="infoBoxHeadi ng"><img src="images/infobox/corner_righ t_left.gif" border="0" alt="" width="11" height="14"></td>. <td width="100%" height=" <++++++++++++++>Sun May 03 19:54:32 GMT-0 3:00 2009 -> 192.168.15.52 -> 192.168.15 .100 -> 80 -> 3314 -> Dados do Pacote: . .q.....}.....E...O:@.@.E....4...d.P..).. .....P....U..14" class="infoBoxHeading"> Order History</td>. <td height="14" c lass="infoBoxHeading" nowrap><img src="i mages/pixel_trans.gif" border="0" alt="" width="11" height="14"></td>. </tr>.</ table>.<table border="0" width="100%" ce llspacing="0" cellpadding="1" class="inf oBox">. <tr>. <td><table border="0" width="100%" cellspacing="0" cellpadding ="3" class="infoBoxContents">. <tr>. <td><img src="images/pixel_trans.gif" b order="0" alt="" width="100%" height="1" ></td>. </tr>. <tr>. <td class="box Text"><table border="0" width="100%" cel lspacing="0" cellpadding="1"> <tr> < td class="infoBoxContents">Courage Under Fi re</td> <td class="infoBoxContent s" align="right" valign="top"><img src="images/icons/cart.gif" border ="0" alt="In Cart" title=" In Cart " wid th="16" height="17"></td> </tr> <t r> <td class="infoBoxContents"><a hre f="http://py5jo.no-ip.org/osc/catalog/pr oduct_info.php?products_id=24">Disciples : Sacred Lands</td> <td class="in foBoxContents" align="right" valign="top "><img src="images/icons/cart .gif" border="0" alt="In Cart" title=" I n Cart " width="16" height="17"></td > </tr> <tr> <td class="infoBoxCont ents"><a href="http://py5jo.no-ip <++++++++++++++>
<++++++++++++++>
<++++++++++++++>

... muitos pacotes ...

<++++++++++++++>
<++++++++++++++>
<++++++++++++++>Sun May 03 19:54:36 GMT-0 3:00 2009 -> 192.168.15.52 -> 192.168.15 .100 -> 80 -> 3341 -> Dados do Pacote: . .q.....}.....E.....@.@.....4...d.P..,.. 32..YP..... <td><table border="0" w idth="100%" cellspacing="1" cellpadding= "2" class="infoBox">. <tr class ="infoBoxContents">. <td widt h="30%" valign="top"><table border="0" w idth="100%" cellspacing="0" cellpadding= "2">. <tr>. <td class="main">Billing Address (Edit)</td> . </tr>. <tr>.

<td class="main">GVT - G lobal Village Telecom
 Joao Fabio Oli veira
 Rua Carlos Benato, 750, Casa 0 2
 Sao Braz
 Curitiba, 82320-440<b r> Partana, Brazil</td>. </ tr>. <tr>. < td class="main">Payment Method (Edit)</td>. </tr>. <tr>. <td class="main">Cash on Delivery< /td>. </tr>. </t able></td>. <td width="70%" v align="top" align="right"><table border= "0" cellspacing="0" cellpadding="2">. <tr>. <td alig n="right" class="main">Sub-Total:</td>. <td align="right" class=" main">R$95.98</td>. </tr> <tr>. <td ali gn="right" class="main">Flat Rate (Best Way):</td>. <td align="ri ght" class="main">R$12.00</td>. </tr> <tr>. -> Dad os do Pacote: ..q.....}.....E.....@.@... ...4...d.P..,..32..YP..... <td><tab le border="0" width="100%" cellspacing=" 1" cellpadding="2" class="infoBox">. <tr class="infoBoxContents">. <td width="30%" valign="top"><tab le border="0" width="100%" cellspacing=" 0" cellpadding="2">. <tr>. <td class="main">Billi ng Address (Edit)< /span></td>. </tr>. <tr>. <td class ="main">GVT - Global Village Telecom
 Joao Fabio Oliveira
 Rua Carlos Bena to, 750, Casa 02
 Sao Braz
 Curiti ba, 82320-440
 Partana, Brazil</td>. </tr>. <tr>. <td class="main">Paymen t Method < span class="orderEdit">(Edit) </td>. </tr>. <tr>. <td class="main">Ca sh on Delivery</td>. </tr>. </table></td>. <t d width="70%" valign="top" align="right" ><table border="0" cellspacing="0" cellp adding="2">. <tr>. <td align="right" class="main">Su b-Total:</td>. <td align= "right" class="main">R$95.98</td>. </tr> <tr>. <td align="right" class="main">F lat Rate (Best Way):</td>. <td align="right" class="main">R$12.00 </td>. </tr> < tr>. -> Dados do Pacote: ..q.....}.. ...E.....@.@.....4...d.P..,..32..YP.... ... <td><table border="0" width="100% " cellspacing="1" cellpadding="2" class= "infoBox">. <tr class="infoBoxC ontents">. <td width="30%" va lign="top"><table border="0" width="100% " cellspacing="0" cellpadding="2">. <tr>. <td class= "main">Billing Address (Edit)</td>. </tr>. <tr>. <td class="main">GVT - Global Vill age Telecom
 Joao Fabio Oliveira
 Rua Carlos Benato, 750, Casa 02
 Sao Braz
 Curitiba, 82320-440
 Partana , Brazil</td>. </tr>. <tr>. <td class=" main">**Payment Method** (E dit)</td>. </tr> . <tr>. <td class="main">**Cash on Delivery**</td>. </tr>. </table></td> . <td width="70%" valign="top " align="right"><table border="0" cellsp acing="0" cellpadding="2">. <tr>. <td align="right" class="main">Sub-Total:</td>. <td align="right" class="main">R$95 .98</td>. </tr> <tr>. <td align="right" class="main">Flat Rate (Best Way):</td> . <td align="right" class ="main">R$12.00</td>. </tr> <tr>. -> Dados do Paco te: ..q.....}.....E.....@.@.....4...d.P ..,..32..YP..... <td><table border= "0" width="100%" cellspacing="1" cellpad ding="2" class="infoBox">. <tr class="infoBoxContents">. <td width="30%" valign="top"><table border= "0" width="100%" cellspacing="0" cellpad ding="2">. <tr>. <td class="main">Billing Address << span class="orderEdit">(Edit) </td>. </tr>. <tr>. <td class="main">GV T - Global Village Telecom
 Joao Fabi o Oliveira
 Rua Carlos Benato, 750, C asa 02
 Sao Braz
 Curitiba, 82320- 440
 Partana, Brazil</td>. </tr>. <tr>. <td class="main">Payment Method</ b> (Edit)</td>. </tr>. <tr>. <td class="main">Cash on Deli very</td>. </tr>. </table></td>. <td width="7 0%" valign="top" align="right"><table bo rder="0" cellspacing="0" cellpadding="2" >. <tr>. <td align="right" class="main">**Sub-Total**:</ td>. <td align="right" cl ass="main">**R$95.98**</td>. </ tr> <tr>. <t d align="right" class="main">Flat Rate (Best Way):</td>. <td alig n="right" class="main">R$12.00</td>. </tr> <tr>. - > Dados do Pacote: ..q.....}.....E.....@ .@.....4...d.P..,..32..YP..... <td ><table border="0" width="100%" cellspac ing="1" cellpadding="2" class="infoBox"> . <tr class="infoBoxContents">. <td width="30%" valign="top" ><table border="0" width="100%" cellspac ing="0" cellpadding="2">. < tr>. <td class="main"> **Billing Address** (E dit)</td>. </tr> . <tr>. <td class="main">**GVT - Global Village Teleco m**
 Joao Fabio Oliveira
 Rua Carlos Benato, 750, Casa 02
 Sao Braz
 C uritiba, 82320-440
 Partana, Brazil</ td>. </tr>. <t r>. <td class="main">P ayment Method (Edit)</td>. </tr>. <tr>. <td class="mai n">Cash on Delivery</td>. < /tr>. </table></td>. <td width="70%"

valign="top" align="r ight"><table border="0" cellspacing="0" cellpadding="2">. <tr>. <td align="right" class="mai n">Sub-Total:</td>. <td a lign="right" class="main">R$95.98</td>. </tr> <tr>. <td align="right" class="ma in">**Flat Rate** (Best Way):</td>. <td align="right" class="main">**R$ 12.00**</td>. </tr> <tr>. <+++++++++++++>Sun May 03 19:54:36 GMT-0 3:00 2009 -> 192.168.15.52 -> 192.168.15 .100 -> 80 -> 3341 -> Dados do Pacote: . .q.....}.....E.....@.@......4...d.P..,.# .2..YP....U.. <td align="righ t" class="main">**Total**:</td>. <td align="right" class="main">**R$ 107.98**</td>. </tr> </table></td>. </tr>. </table></td>. </tr>. <tr >. <td><img src="images/pixel_tra ns.gif" border="0" alt="" width="100%" h eight="10"></td>. </tr>. <tr>. <td><table border="0" width="100 %" cellspacing="0" cellpadding="0">. <tr>. <td align="right" class="main">.<input type="image" src=" includes/languages/english/images/button s/button_confirm_order.gif" border="0" a lt="Confirm Order" title=" Confirm Order ">. </td>. </tr>. </table></td>. </tr>. <t r>. <td><img src="images/pixel_tr ans.gif" border="0" alt="" width="100%" height="10"></td>. </tr>. <tr> . <td><table border="0" width="10 0%" cellspacing="0" cellpadding="0">. <tr>. <td width="25%"> <table border="0" width="100%" cellspaci ng="0" cellpadding="0">. <t r>. <td width="50%" align ="right"><img src="images/pixel_silver.g if" border="0" alt="" width="1" height=" 5"></td>. <td width="50%" ><img src="images/pixel_silver.gif" bord er="0" alt="" width="100%" height="1"></ td>. </tr>. </ta ble></td>. <td width="25%"><i mg src="images/pixel_silver.gif" border= "0" alt="" width="100%" height="1"></td> . <td width="25%"><tab <+++++++++++++>Sun May 03 19:54:36 GMT-0 3:00 2009 -> 192.168.15.52 -> 192.168.15 .100 -> 80 -> 3341 -> Dados do Pacote: . .q.....}.....E.....@.@......4...d.P..,.# .2..YP....U.. <td align="righ t" class="main">**Total**:</td>. <td align="right" class="main">**R$ 107.98**</td>. </tr> </table></td>. </tr>. </table></td>. </tr>. <tr >. <td><img src="images/pixel_tra ns.gif" border="0" alt="" width="100%" h eight="10"></td>. </tr>. <tr>. <td><table border="0" width="100 %" cellspacing="0" cellpadding="0">. <tr>. <td align="right" class="main">.<input type="image" src=" includes/languages/english/images/button s/button_confirm_order.gif" border="0" a lt="Confirm Order" title=" Confirm Order ">. </td>. </tr>. </table></td>. </tr>. <t r>. <td><img src="images/pixel_tr ans.gif" border="0" alt="" width="100%" height="10"></td>. </tr>. <tr> . <td><table border="0" width="10 0%" cellspacing="0" cellpadding="0">. <tr>. <td width="25%"> <table border="0" width="100%" cellspaci ng="0" cellpadding="0">. <t r>. <td width="50%" align ="right"><img src="images/pixel_silver.g if" border="0" alt="" width="1" height=" 5"></td>. <td width="50%" ><img src="images/pixel_silver.gif" bord er="0" alt="" width="100%" height="1"></ td>. </tr>. </ta ble></td>. <td width="25%"><i mg src="images/pixel_silver.gif" border= "0" alt="" width="100%" height="1"></td> . <td width="25%"><tab -> Dad os do Pacote: ..q.....}.....E.....@.@... ...4...d.P..,.#.2..YP....U.. <td align="right" class="main">Total:</t d>. <td align="right" cla ss="main">R$107.98</td>. </tr> </table></td>. </tr>. </table></td>. </tr>. <tr>. <td><img src="i mages/pixel_trans.gif" border="0" alt="" width="100%" height="10"></td>. </ tr>. <tr>. <td><table border ="0" width="100%" cellspacing="0" cellpa dding="0">. <tr>. <t d align="right" class="main">.<input typ e="image" src="includes/languages/englis h/images/buttons/button_confirm_order.gi f" border="0" alt="Confirm Order" title= " Confirm Order ">. </td>. </tr>. </table></td>. </tr>. <tr>. <td><img src=" images/pixel_trans.gif" border="0" alt=" " width="100%" height="10"></td>. < /tr>. <tr>. <td><table borde r="0" width="100%" cellspacing="0" cellp adding="0">. <tr>. < td width="25%"><table border="0" width=" 100%" cellspacing="0" cellpadding="0">. <tr>. <td wi dth="50%" align="right"><img src="images /pixel_silver.gif" border="0" alt="" wid th="1" height="5"></td>. <td width="50%"><img src="images/pixel_s ilver.gif" border="0" alt="" width="100% " height="1"></td>. </tr>. </table></td>. <td width="25%"><img src="images/pixel_silv er.gif" border="0" alt="" width="100%" h eight="1"></td>. <td width="2 5%"><tab <+++++++++++++>
<+++++++++++++>
<+++++++++++++>

... muitos pacotes ...

<+++++++++++++>
<+++++++++++++>
<+++++++++++++>Sun May 03 19:54:39 GMT-0 3:00 2009 -> 192.168.15.52 -> 192.168.15 .100 -> 80 -> 3346 -> Dados do Pacote: . .q.....}.....E....X@.@......4...d.P..... .P..3P..>....ht" valign="bottom"><img src="images/header_accoun t.gif" border="0" alt="My Account" title =" My Account " width="30" height="30">< /a> <a

href="http://py5jo.no- ip.org/osc/catalog/shopping_cart.php"><i mg src="images/header_cart.gif" border=" 0" alt="Cart Contents" title=" Cart Cont ents " width="30" height="30">   <img sr c="images/header_checkout.gif" border="0 " alt="Checkout" title=" Checkout " widt h="30" height="30"> </td> . </tr>.</table>.<table border="0" widt h="100%" cellspacing="0" cellpadding="1" >. <tr class="headerNavigation">. <t d class="headerNavigation"> < a href="http://py5jo.no-ip.org" class="h eaderNavigation">Top » Catalog » Checkout » Success</t d>. <td align="right" class="headerNa vigation">Log Off | M y Account | Cart Contents | Checkout   </td>. **INSTRUMENTO CONTRATUAL ENCERRADO**-------- ----------

Apêndice B

Interação Contratado e Contratante

A seguir, apresenta-se a ilustração da ativação, cadastro e aceite do procedimento inicial do mecanismo de autenticidade, e também a finalização do mesmo ao final da compra executada, onde é destacada a relação entre o site do contratado e as informações disponíveis ao contratante em sua relação com mecanismo no protótipo definido.

B.1 Fluxo de Interação Contratado e Contratante

De acordo com a definição do administrador do portal para a oferta inicial do mecanismo de autenticidade ao contratante, o mesmo terá a sua disposição a solicitação inicial de identificação definida pelo CPF (Código de Pessoa Física), que é a chave única de identificação do contratante nas bases de dados do servidor.

Com base nesta informação as Figuras B.1 e B.2 ilustram a solicitação do CPF e o cadastro do contratante junto ao mecanismo de autenticidade em seu acesso inicial ao portal (o cadastro é feito em única vez, não sendo necessário em próximas interações do contratante junto ao portal).

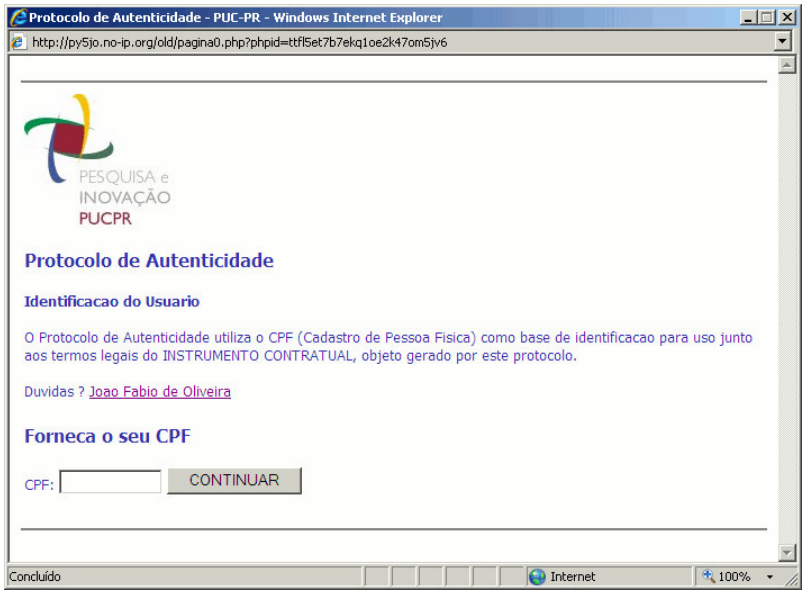

Figura B.1 – Solicitação do CPF no Mecanismo de Autenticidade

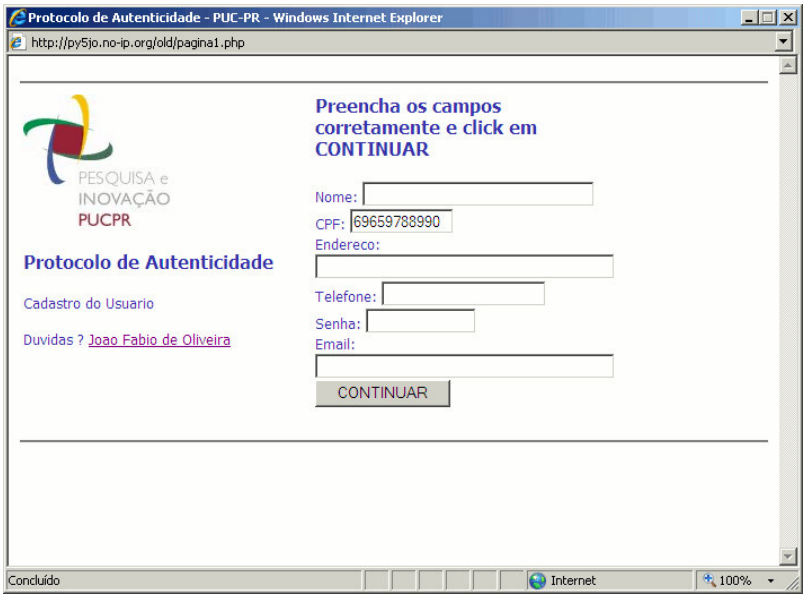

Figura B.2 – Cadastro do Contratante no Mecanismo de Autenticidade

Após a identificação do contratante, a próxima etapa é solicitar sua confirmação para uso do mecanismo de autenticidade, conforme manifestação de sua vontade explícita definida em Boiago Júnior (2005) explicada no Capítulo 3, de maneira a iniciar a captura dos pacotes e geração do *log* desta sessão, conforme mostrado na Figura B.3.

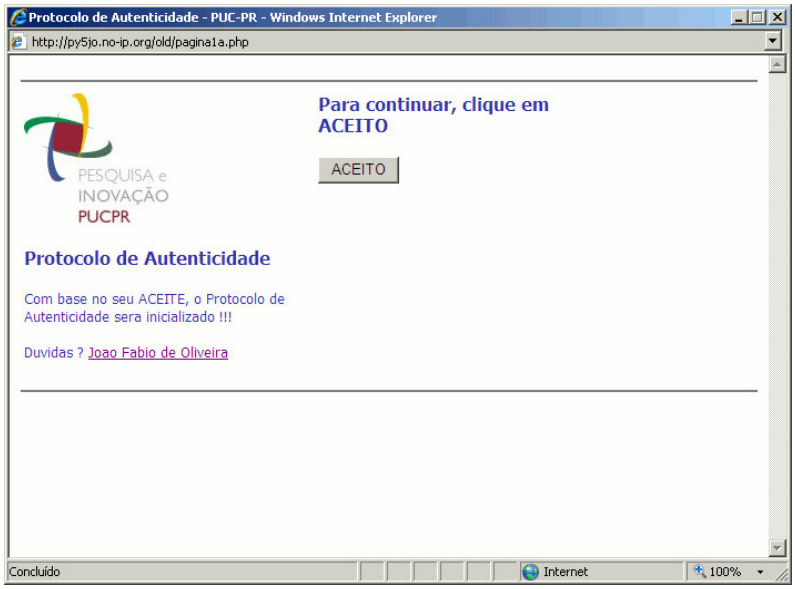

Figura B.3 – Aceite Explícito do Contratante

Na seqüência ao aceite do cliente, inicia-se a captura dos pacotes e a geração do *log*, sendo que as próximas páginas do portal eletrônico correspondem ao conteúdo do portal e segue-se pelas interações definidas no próprio portal de comércio eletrônico até o fomento final da compra em que o mecanismo de autenticidade é finalizado (definido pelo administrador do portal).

Na sessão final da transação comercial com o contratante no portal, a exemplo de um procedimento de compra de um bem onde se finaliza com a realização do pagamento e a confirmação do procedimento pelo fornecedor, o portal deve identificar esta finalização informando ao contratante e encerrando o procedimento de captura, ao mesmo tempo oferecendo-lhe o arquivo com o instrumento contratual gerado, conforme apresentado nos Capítulos 3 e 4. A Figura B.4 ilustra a finalização do uso do mecanismo de autenticidade.

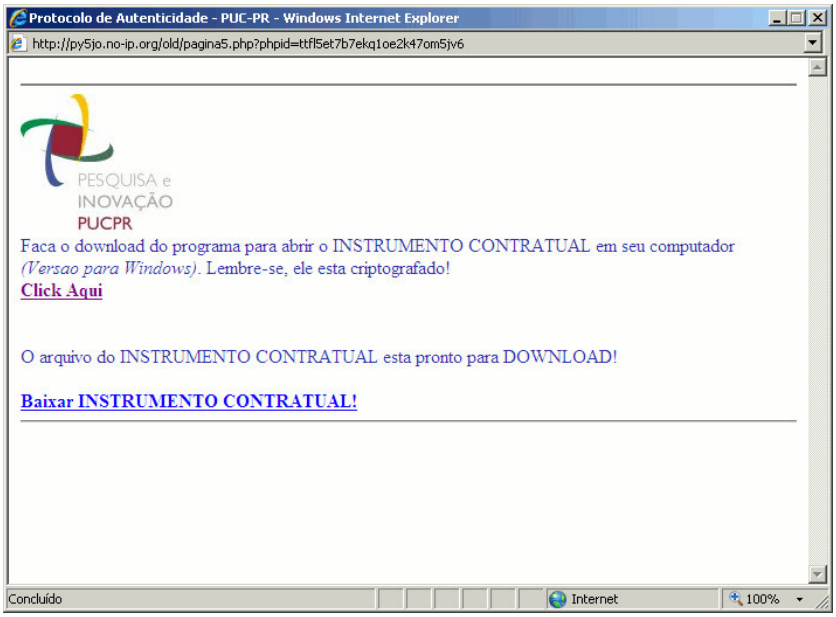

Figura B.4 – Finalização do Mecanismo de Autenticidade

Com posse do instrumento contratual, o contratante poderá abri-lo utilizando-se de um software cliente disponibilizado para tal finalidade. Este cliente faz parte das definições do mecanismo de autenticidade e deverá ser disponibilizado ao contratante no portal eletrônico do contratado, seja em páginas customizadas para tal finalidade ou mesmo no momento final da transação, como mostrado na Figura B.4.

A Figura B.5[66] ilustra o software cliente que é executado no ambiente do contratante, em que o arquivo encriptado recebido com e-mail, ou mesmo baixado diretamente no site do contratado (*IC_xxxx.JFL*) poderá ser aberto utilizando a respectiva senha simétrica do contratante.

[66] A versão o cliente para abertura do instrumento contratual na máquina do contratante é escrito em Java, possuindo o mesmo algoritmo usado para encriptação no ambiente do contratante, e está compilado para execução em ambiente Windows, testado em suas versões XP e Vista.

Figura B.5 - Software Cliente para Abertura do Instrumento Contratual Encriptado