KATIUCIA YUMI TADANO

GED: Assinatura Digital e Validade Jurídica de Documentos Eletrônicos

Cuiabá, MT - Brasil

Junho / 2002

GED: Assinatura Digital e Validade Jurídica de Documentos Eletrônicos

KATIUCIA YUMI TADANO

Trabalho monográfico para cumprimento de créditos da disciplina de Projeto Supervisionado, do curso de bacharelado em Ciência da Computação sob a orientação do Prof. Dr. G.A.R. Lima.

Cuiabá, MT - Brasil

Junho / 2002

TADANO, KATIUCIA TADANO

GED – Assinatura digital e validade jurídica de documentos eletrônicos

98p. 29,7 cm

Universidade Federal de Mato Grosso, UFMT

1. Documento Eletrônico, 2. Assinatura Digital, 3.Certificação Digital, 4.GED – Gerenciamento Eletrônico de Documentos

TADANO, KATIUCIA YUMI

GED: Assinatura Digital e Validade Jurídica de Documentos Eletrônicos.

Orientador: Prof. Dr. G. A. R. Lima

Cuiabá, MT - Brasil

Junho / 2002

IV

Resumo do trabalho monográfico apresentado para o Curso de Bacharelado em Ciência da Computação / UFMT como parte dos requisitos necessários para o cumprimento de créditos da disciplina de Projeto Supervisionado.

GED: Assinatura Digital e Validade Jurídica de Documentos Eletrônicos.

Cuiabá, MT - Brasil

Junho / 2002

Orientador: Prof. Dr. G. A. R. Lima

Departamento: Faculdade de Ciências e Tecnologia - FATEC

Universidade de Cuiabá – UNIC e Faculdades Integradas Cândido Rondon - UNIRONDON.

O principal objetivo deste trabalho é abordar o tema documento eletrônico, seus aspectos técnicos, práticos e jurídicos. A primeira parte do estudo é dedicada aos aspectos técnicos e funcionais de um documento eletrônico, bem como a especificação das técnicas de criptografia, assinatura digital e certificação digital que tornam um documento eletrônico seguro e confiável. A segunda parte é dedicada aos aspectos legais dos documentos eletrônicos de senso amplo com relação à eficácia probatória, as normas atuais pertinentes à prova documental com enfoque na importância da informação e desmaterialização do documento e por fim , a conclusão .

EPÍGRAFE

"A forma deve sempre se
adequar a função..."

Louis Sullivan

DEDICATÓRIA

Dedico este trabalho à minha amada mãe, que dedicou toda sua vida a mim e ao meu pai (*in memorian*) que me ensinou a ser forte igual a ele.

AGRADECIMENTOS

A Deus, força maior do Universo;

Ao professor Dr. G.A.R. Lima, pela atenção, paciência, dedicação e por me ajudar nos momentos em que as soluções pareciam não existir;

À minha mãe e irmãs, que me apoiaram e me encorajaram até o fim da jornada;

Ao meu noivo, pela compreensão e carinho dedicados nos momentos difíceis

FIGURAS

SUMÁRIO

Introdução

Cada vez mais o mundo dos negócios e empreendimentos está gerando documentos apostos em papel. A rapidez na localização da informação contida no documento é hoje a prioridade das empresas e organizações, 95% das informações relevantes para o processo de negócio encontra-se aposto em papel, segundo a A.I.I.M.[ε].

Organizar os documentos em pastas e arquivos físicos dificulta a agilidade de recuperação, trazendo conseqüências para o gerenciamento dos processos que os documentos representam. Além de tudo, a informação contida em documentos impressos tem uma menor flexibilidade e tende a gerar gastos de manutenção maiores do que quando o armazenamento é feito eletronicamente. Até pouco tempo atrás, a tecnologia usada para processar documentos era restringida a melhorar os recursos para gerar, imprimir e transportar os documentos criados eletronicamente. Porém, recentemente tem sido muito usado um conjunto de novas tecnologias voltadas exclusivamente para o gerenciamento eletrônico de documentos, conhecido pela sigla de GED – Gerenciamento Eletrônico de Documentos, cuja proposta é permitir que as empresas alcancem grande produtividade – e conseqüente competitividade de mercado – convertendo toda espécie de documento aposto em papel para meios digitais. Pode-se citar o GED como exemplo de uma abordagem operacional, eminentemente centrada na conversão e manuseio de documentos eletrônicos. Hoje os sistemas de GED são

[ε] A.I.I.M. – Association for Information and Image Management International.

utilizados para capturar, indexar, armazenar, consultar e gerenciar versões digitalizadas (sob a forma de imagens), de documentos eletrônicos.

A idéia de converter documentos impressos em formas alternativas de armazenamento, a princípio com o objetivo de conservação temporal, só se tornou possível graças aos avanços da tecnologia de processamento de imagem. A conversão para microfilme foi o primeiro recurso disponível, e que agora cede espaço para o armazenamento eletrônico de documentos. Com o conceito de GED um documento desempenha um papel importantíssimo nos novos paradigmas da administração empresarial. O uso desta tecnologia de GED traz consigo algumas mudanças importantes no que diz respeito a maneiras de como criar, armazenar e distribuir um documento, assim como, gerenciar fluxo de trabalho baseado em documentos eletrônicos. De uma perspectiva mais ampla, GED é uma expansão no domínio do gerenciamento de informações, pois no processo administrativo, a tomada de decisão é um elemento básico e fundamental.

Com a chegada da Internet, a transação a longa distância popularizou-se e hoje estamos vivendo a época do comércio eletrônico. Entretanto, este novo tipo de comércio criou um paradigma quanto ao aspecto de impessoalidade nas transações, ou seja, como confiar em algo escrito por alguém a milhares de quilômetros de distância? Novamente a tecnologia apresentou alternativas para esclarecer dúvidas neste sentido. Uma dessas alternativas é a chamada assinatura digital, a qual pode ser vista como um dado que acompanha o significado de um documento e que pode ser utilizado para comprovar tanto o emissor do documento como o fato de que o documento não foi alterado.

A possibilidade da assinatura digital deixa evidente a necessidade de uma abordagem sobre o conceito de documento eletrônico e sua validade jurídica.

O presente trabalho encontra-se organizado da seguinte maneira: no Capítulo I - Documento Eletrônico, é abordado o conceito de documento eletrônico, o gerenciamento de documento eletrônico e as técnicas envolvidas no GED. No capítulo II – Criptografia e Assinatura Digital, introduz o conceito de criptografia, seus métodos e a concretização da assinatura digital. No capítulo III – Certificação Digital, apresenta-se o ato de certificar um documento eletrônico e a autoridade certificadora. No capítulo IV – Validade Jurídica do documento eletrônico, aborda o

amparo legal existente no Brasil no que se diz respeito à documento eletrônico. Finalizando este trabalho estão a Conclusão, algumas considerações finais, referências bibliográficas utilizadas neste trabalho e por fim os apêndices e anexos.

I – Documentos Eletrônicos

Transações comerciais eletrônicas são, fundamentalmente, muito semelhantes às transações tradicionais (transações feitas no Marketing Place). A diferença entre o comércio feito no marketing Place e no Marketing Space (comércio eletrônico) está justamente no contrato firmado entre as partes. Faz-se necessário uma certa confiança entre as partes envolvidas já que a transação feita entre ambas as partes é realizada entre diferentes localizações geográficas e efetuadas em um mundo virtual. Como então garantir a fidelidade da manifestação de vontade entre as partes? A melhor solução para este problema é um sistema de controle (chamado de Autoridade Certificadora – AC), baseado na definição de assinatura digital. Em outras palavras, uma certificação, é uma coleção de informações com as quais uma assinatura digital é anexada ao documento eletrônico por alguma AC, para que haja validade jurídica, devendo esta, ser reconhecida pelo Poder Legislativo.

O entendimento da expressão assinatura digital, tem como princípio a identificação, e para ilustrar a problemática que envolve a questão, este estudo começa tratando do entendimento do termo “documento eletrônico”.

1.1 – O Termo "Documento Eletrônico"

Inúmeras vezes o termo documento eletrônico é citado neste trabalho. O termo “eletrônico" é um adjetivo que qualifica algo *"relativo à eletrônica". "Eletrônica",* por sua vez, diz respeito à *"parte da física dedicada ao estudo do comportamento de circuitos elétricos que contenham válvulas, semicondutores, transdutores, etc., ou à*

*fabricação de tais circuito*s".(FERREIRA, 1988:504). Os "documentos eletrônicos" são produzidos, manuseados e transmitidos com o auxílio de máquinas eletrônicas, porém, em si mesmos, tais documentos não são "eletrônicos", pois não são circuitos elétricos e nem possuem válvulas, semicondutores ou qualquer outro dispositivo eletrônico. Neste contexto a comunidade científica entende que: *"o documento eletrônico necessita de um instrumento de criação, conservação, cancelamento e transmissão, constituído por aparelhos eletrônicos"*. Eletrônico, então, é o computador que cria e manipula tal espécie de documento.

Os "documentos eletrônicos" nada mais são do que informações manipuladas e armazenadas com o uso do computador sendo, portanto, compostos unicamente por *bit*s. O fato do *bit* vir a ser sinônimo de dígito binário (MONTEIRO, 1996:390), permite afirmar que o documento eletrônico encontra-se sob uma forma digitalizada. O termo "digitalização" se refere ao processo de conversão que é feito para se representar alguma coisa em uma versão digital, por exemplo, utilizando-se unicamente de *bits* podemos representar um documento ou uma imagem (forma digital). Consequentemente, seria mais apropriado e específico denominar o "documento eletrônico" de "documento digital", porém, a fim de seguir o uso mais aceito, neste estudo será usado o termo "documento eletrônico".

Partindo-se do entendimento de que o documento eletrônico ou documento digital – é todo documento produzido através do uso do computador, pode-se distingui-lo em duas espécies distintas: documento eletrônico *stricto sensu* (ou de senso estrito*)* e *lato sensu* (ou de senso amplo).

Os documentos eletrônicos de senso estrito são somente aqueles que se encontram memorizados em forma digital, não perceptíveis para os seres humanos senão mediante intermediação (no caso, feita através de um computador e de um *software* adequado).

Os documentos eletrônicos de senso amplo, por sua vez, são todos aqueles criados no computador mediante seus próprios dispositivos eletrônicos, ou periféricos de entrada e saída. Observe-se que nessa segunda espécie, os documentos não existem em forma exclusivamente digital, como é o caso, de um documento impresso. Cabe aqui ressaltar que, através do uso de dispositivo de saída do computador, a impressora, o documento pode ser aposto em papel,

tornando-se, em sua forma final, um documento tradicional. Ou ainda pode existir aposto em papel e ser convertido para a forma digital através do uso de um dispositivo de entrada chamado scanner [φ].

Em substância, os documentos eletrônicos em senso estrito são destinados a serem lidos ou interpretados pelo computador, e os documentos eletrônicos em senso amplo são criados através do uso do computador e têm como característica o fato de poderem ser percebidos pelo homem sem a intervenção de máquinas tradutoras.

1.2 – Gerenciamento de Documentos Eletrônicos

No mundo dos negócios de hoje, as empresas que usam computadores estão mudando tanto operacionalmente como culturalmente, a tecnologia tem sido a chave do sucesso para conquistar clientes e reduzir custos operacionais. No cotidiano das empresas, mesmo com toda a tecnologia disponível, ainda se lida com grandes volumes de informações apostas em papel.(MURSHED,1997). Como, então, ser competitivo no ambiente em que há alta tecnologia, mas ainda muito papel?

A solução para este desafio é o GED – Gerenciamento Eletrônico de Documentos, cuja proposta é permitir que as empresas alcancem grande produtividade – e conseqüente competitividade de mercado – convertendo toda espécie de documento aposto em papel para meios digitais. Pode-se citar o GED como exemplo de uma abordagem operacional, eminentemente centrada no manuseio. A tecnologia é utilizada para captar, indexar, armazenar, consultar e gerenciar versões digitalizadas (sob a forma de imagens) de documentos em papel. O GED também pode ser denominado como "processamento de imagens", tendo por objetivo possibilitar que documentos, inicialmente existentes sob a forma de papel, sejam capturados por sistemas de computação, com a capacidade de armazenar, manipular, recuperar e imprimir os mesmos, além de poder enviá-los a

[φ] Dispositivo que captura uma imagem e converte-a para um formato digital.

diferentes destinatários localizados em regiões geográficas diversas com a rapidez de comunicação hoje oferecida pela tecnologia de rede de computadores.

Um sistema voltado para o gerenciamento eletrônico de documentos visa permitir que grandes massas documentais, que ocupam volumosos e caros espaços físicos, sejam armazenadas em diversos tipos de suportes informáticos (atualmente, usam-se discos ópticos).

A simples imagem de documento, conforme as utilizadas no âmbito do GED, em princípio, não apresenta eficácia probatória, já que nos sistemas de GED não há preocupação, por exemplo, de implementar um mecanismo que garanta a integridade do documento gerado. No caso de documentos apostos em papel, pode-se estabelecer uma perfeita correspondência com o documento original. Poder-se-ia comparar tal imagem de documento, em termos de prova, com uma foto sem negativo, sendo que a foto poderia levar alguma vantagem por permitir procedimentos de perícia que tentassem estabelecer se houve montagem, enquanto que a imagem digital alterada não deixaria traço nenhum. Neste caso, os sistemas de GED somente teriam a função de facilitar a organização, pesquisa e recuperação dos documentos, não se livrando, contudo, de ter que produzir um documento tradicional, impresso sobre papel e assinado, para dar a eficácia jurídica pretendida para cada ato.

Porém, existe hoje a possibilidade de qualquer uma dessas simples imagens utilizadas no GED vir a ser dotada de força probatória, desde que submetida a procedimentos especiais (conforme o capítulo III), visando o atendimento dos requisitos necessários para tanto. Uma vez feito isso, as duas visões dos documentos, uma operacional e outra jurídica, se complementariam, o que permitiria que se pudesse extrair, em grau máximo, todas as vantagens que os sistemas de GED pode oferecer à sociedade moderna (ampla facilidade de manipulação e transmissão, conjugada com eficácia probatória).

1.3 – Técnicas envolvidas pelo GED

Controlar documentos de forma segura e rápida tornou-se uma necessidade para a maioria das empresas. A distribuição simultânea dos

documentos a todas as estações de trabalho, inclusive o acesso pela Internet, por meios de usuários definidos por tipo de ação que cada colaborador pode fazer, garante o acesso com segurança aos documentos.

O GED é a somatória de todas as técnicas e produtos que visam gerenciar informações de forma eletrônica, eliminando o acúmulo de documentos apostos em papel e permitindo acesso, gerenciamento, localização e uma distribuição mais rápido das informações.

Um sistema de GED usa a tecnologia da informação para capturar, armazenar, localizar e gerenciar versões digitais dos documentos com objetivo de gerenciar o ciclo de vida das informações desde sua criação até a sua distribuição e arquivamento. As informações podem, originalmente, estarem registradas em mídias analógicas ou digitais em todas as fases de seu ciclo de vida. Podem ser criadas, revisadas, processadas e arquivadas em papel ou em mídias eletrônicas. Existem situações em que podem haver combinações de mídias analógicas e digitais. Por exemplo, informações criadas e revisadas em sistemas eletrônicos são impressas para o seu processamento e arquivamento em papel, ou criadas e revisadas em mídia de papel para então serem digitalizadas por meio de um *scanner* e processadas e arquivadas eletronicamente.

Para iniciar a caracterização do GED, podemos definir que o ciclo de vida das informações é gerenciado por dois macrogrupos de soluções: os de gerenciamento de documentos (document management) e gerenciamento de imagens de documentos (document imaging).

As tecnologias e técnicas que impulsionam o gerenciamento eletrônico de documentos, foram sendo agregadas ao GED na medida em que, com o passar do tempo, surgiam nas empresas a necessidade do gerenciamento de documentos, devido ao acúmulo de informação.

O *Document Imaging* ou Gerenciamento de Imagens de Documentos é uma das técnicas que o GED utiliza. Esta técnica permite que uma imagem seja processada por um processador de textos ou por um sistema de processamento de dados. A imagem deve passar pelo reconhecimento de caracteres, que transforma a

imagem de um texto num arquivo de dados realmente textual (ASCII[θ]), que posteriormente pode ser editado por um processador de textos. O reconhecimento, quando processado sobre caracteres padronizados, como os dos documentos impressos, utiliza-se a técnica de OCR (*Optical Character Recognition*), quando é necessário reconhecer textos manuscritos, a técnica utilizada é o ICR (*Intelligent Character Recognition*).

O amadurecimento dessas técnicas de reconhecimento viabilizaram as aplicações de processamento de formulários ou *Forms Processing*, que fazem uso de sistemas digitais para extrair dados de documentos eletrônicos, evitando o serviço de digitação manual.

Com a possibilidade de conversão de documentos apostos em papel em documentos eletrônicos, foi necessário desenvolver uma técnica que automatizasse o processo de trâmite de documentos eletrônicos. Surgiu então, a técnica de *Workflow* ou fluxo de trabalho, possibilitando os processos automatizados, reduzindo assim o fluxo de papel e dos custos operacionais e aumentando a agilidade dos processos e produtividade organizacional.(DALLEYRAND, 1955:31).

O próprio avanço da tecnologia e a disseminação dos microcomputadores na última década, fizeram com que boa parte da geração dos documentos fossem feitas pelos sistemas digitais. Num ambiente de escritório, isso significa documentos criados a partir de processadores de texto, planilhas eletrônicas e todas as demais ferramentas dessa natureza. Em meados de 90 surgiram as ferramentas para *Document Management*[&] ou Gerenciamento de Documentos. Esta técnica esteve inicialmente mais envolvida no gerenciamento de documentos de engenharia e normas técnicas, sendo uma das exigências da ISO 9000[ϑ]. Essa técnica permite a rastreabilidade das alterações dos documentos. Hoje, a quantidade de arquivos nos diretórios, a necessidade do compartilhamento de documentos, tanto nas redes

---

[θ] ASCII é um acrônimo para *American Standard Code for Information Interchange* (ou Código Padrão Americano para Intercâmbio de Informações);

[&] DM (Document Management): Gerencimento do Documentos.

[ϑ] ISO: International Standardization Organization (Organização para Padronização Internacional)

internas como na Internet, e o controle das atualizações em ambiente distribuído, justifica a implantação de sistemas de *Document Management* para todas as aplicações de gerenciamento de documentos. O DM implementa, no mundo digital, muitas das funcionalidades já existentes nas aplicações de *Records Management* (Gerenciamento de Arquivos) em se tratando de documento aposto em papel.

Outra técnica envolvida no GED é o COLD (*Computer Output to Laser Disk* ou Saída do Computador para o Disco Laser). Esta técnica foi inicialmente introduzida no mercado para substituir a tecnologia COM (*Computer Output to Microfilm* ou Saída do Computador para Microfilme), apresentado pelo armazenamento óptico em relação ao microfilme. A técnica permite o armazenamento e gerenciamento de relatórios de forma digital. Devido a abrangência dessa técnica, ela passou a ser chamada de ERM (*Enterprise Report Management* ou Gerenciamento dos Relatórios da Empresa).

Outra ténica que o GED impulsiona é o KM (*Knowledge Managment*), que gerencia o conhecimento existente na empresa, requerendo que os documentos e as informações sejam registradas e distribuídas de forma adequada dentro da empresa.

A seguir, será detalhado a funcionalidade de cada técnica em relação ao manuseio de documentos eletrônicos:

a) DI - Document Imaging

A técnica *Imaging* ou *Document Imaging* utiliza o conjunto de ferramentas para converter os documentos impressos (papel, microfilmes e microfichas) para o formato digital.

A técnica de DI consiste em gerar uma imagem do documento capturada através de *scanners*. Esses equipamentos simplesmente convertem os documentos apostos em papel ou microfilme para uma mídia digital. A imagem gerada é um mapa de bits, não existindo uma codificação por caracteres, diferente da digitação, em que há codificação de cada letra do texto por um teclado.(DUYSHART, 1998).

b) DM - Document Management

Todos os documentos eletrônicos precisam ser gerenciados, principalmente aqueles com grande quantidade de revisão. A técnica de DM controla o acesso físico aos documentos, ensejando maior segurança e atribuindo localizadores lógicos, como a indexação. Seu foco é o controle das versões dos documentos, mecanismo de busca, data das alterações feitas pelos respectivos usuários e o histórico da vida do documento.

c) Workflow

É uma técnica que permite gerenciar de forma pró-ativa qualquer processo de negócio das empresas. Garante o acompanhamento constante de todas as atividades e um aumento de produtividade com objetividade, eficácia e segurança.(CRUZ, 2000:72).

O W*orkflow* é um conceito definido pelos analistas de sistema como movimento e processamento organizado da informação para o desempenho de funções específicas e está diretamente ligado ao melhor desempenho de processos.(FRUSCIONE, 1994).

A técnica do W*orkflow* permite analisar, modelar, implementar e revisar os processos de trabalho de uma forma simples e interativa, reduzindo tempos de execução e custos totais. Ela se refere ao fluxo/processamento de um documento dentro da empresa. Os documentos são analisados, integrados e distribuídos automaticamente. Na realidade, no W*orkflow*, quando integrados no sistema de GED, os documentos e arquivos não são simplesmente armazenados e localizados, mas usados para conduzir as etapas dos negócios.

d) COLD/ERM

A técnica COLD ou Saída do Computador para o Disco Laser permite inserir em um sistema de GED relatórios oriundos de sistemas de Processamento de Dados. Inicialmente a aplicação gera um relatório, que é mandado a um *spool* (fila) de impressão localizado numa estação que funcionará como uma impressora, e que transformará o arquivo que lhe foi enviado em uma imagem, e esta será inserida na base de dados do sistema de GED. Pode-se citar como exemplo da aplicação COLD

os sistemas bancários para arquivar extratos de conta corrente, os relatórios contábeis de uma empresa e a segunda via de notas fiscais.

e) Forms Processing (OCR/ICR)

É o termo em inglês que significa *Processamento de Formulários*. É uma técnica de processamento eletrônico de formulários que permite reconhecer as informações e/ou dados contidos nos formulários e relacioná-los com campos e bancos de dados.

Essa técnica que automatiza o processo de digitação, é utilizado, por exemplo, pelos bancos para agilizar o processamento dos formulários de abertura de contas e concessão de créditos. Para o reconhecimento automático de caracteres são utilizado técnicas de *OCR* e *ICR*, dependendo da informação e/ou dado estar em caracteres padronizados ou manuscritos.

f) RM - Records Management

Gerenciamento de Arquivos, é o gerenciamento do ciclo de vida do documento, independentemente da mídia em que ele se encontra. O gerenciamento da criação, armazenamento, processamento, manutenção, disponibilização e até descarte dos documentos são controlados pela categorização de documentos e tabelas de temporalidade.

g) CM - Content Management

Gerenciamento de Conteúdo, é o conjunto das técnicas para criação, captação, ajustes, distribuição e gerenciamento de todos os conteúdos que apoiam o processo de negócios da empresa. Os conteúdos podem estar em qualquer formato digital.

h) KM - Knowledge Managment

Gerenciamento do conhecimento é o processo de gerenciar e compartilhar as experiências e conhecimentos dos funcionários, tendo como objetivo, o acesso a melhor informação existente em uma empresa em um tempo

limitado. Estas informações podem estar registradas em diversas formas, devendo ser pesquisável, partilhada e permitir sua fácil reutilização.

1.4 – Armazenamento do documento

Os documentos eletrônicos podem ser armazenados em diversas mídias que existem no mercado. As mídias podem ser divididas em magnéticas, óticas e magneto-ópticas (ou ópticas regraváveis). As magnéticas são os discos fixos (*hard disks*) e as fitas magnéticas. Estes meios de arquivamento não são usados com muita freqüência, pois as mídias magnéticas são as que possuem a menor vida útil dentre todas. Quando se utiliza mídia magnética, a necessidade de regravação periódica é fato. Entre outras implicações, os discos fixos são um tipo de mídia muito cara e que de acordo com as necessidades da organização, aumentarão muito os orçamentos. Já as fitas magnéticas, apesar de alguns avanços tecnológicos, têm o problema de possuir os dados armazenados de maneira contínua, que pode proporcionar um atraso considerável na busca de dados não contínuos.

Os meios de armazenamento mais comuns dentre os sistemas de GED são os meios óticos, e dentre os meios óticos, o mais usado é o disco WORM (*Write Once, Read Many*). Os discos WORM são bastante parecidos com os CD-ROMs na sua forma de gravação e leitura, mas diferem em tamanho e capacidade.

O grande problema dos discos WORM é que os fabricantes não possuem uma norma de compatibilidade, sendo a maioria dos equipamentos de leitura/gravação e os discos de tecnologia proprietária. Os discos WORM são bastante utilizados, pois como não são regraváveis, podem ser utilizados como mídia confiável de documentos que podem ir a juízo.

Os discos magneto-óticos são discos também utilizados em GED, e possuem um funcionamento interessante. Eles são discos refletores, como os CD's, mas sua superfície possui propriedades magnéticas.

Já existem sistemas de GED que fazem uso dos DVDs (*Digital Versatile Disk* – Disco Versátil Digital) para armazenar seus acervos, mas esta é uma tecnologia ainda em desenvolvimento, e seu uso ainda é restrito a poucas corporações.

As mídias óticas e magneto-óticas podem ser lidas em dispositivos de leitura simples, ou disponibilizadas em conjunto em *jukeboxes*[θ]. As *jukeboxes* automatizam o processo de procura de informações, e fazem as trocas de discos automaticamente. Esse processo de troca de discos influencia no tempo final de uma consulta.

1.5 – Vantagens de um sistema de GED

Os sistemas de GED, como visto acima, preservam as características visuais e espaciais e a aparência do documento original aposto em papel. O documento pode ser exibido ou impresso em papel onde e quando necessário em apenas alguns segundos. Uma das grandes vantagens do GED é a capacidade de capturar, recuperar e transmitir documentos contendo todos os tipos de informação, tais como: manuscritas, criadas por computador, diagramas, fotografias, desenhos de engenharia, impressões digitais, assinaturas, etc.

Nesse contexto, o GED tem sido a base de criação de um bom suporte documental, para o gerenciamento do conhecimento e principalmente do gerenciamento das relações com os clientes.

Vejamos as principais vantagens e benefícios do GED:

Principais benefícios:

a) Redução de custos.

b) Gerenciamento automatizado de processos, minimizando recursos humanos e aumentando produtividade.

c) Melhoria no atendimento ao cliente (qualidade).

d) Documentos compartilhados em rede de computadores.

f) Acesso a documentos via Internet/Intranet em qualquer lugar do mundo.

Principais vantagens:

[θ] Caixas que podem abrigar vários discos, e possuem o mesmo nome e idéia de funcionamento igual ao das mais antigas, que eram usadas com discos de música de vinil.

a) Integração da solução GED com sistema corporativo (ERP/CRM - *Enterprise Resource Planning*/*Customer Relationship Management*) e base de dados da empresa.
b) Com o documento digitalizado em meio óptico, o acesso é rápido (informações on-line).
c) Disponibilização dos documentos digitalizados na Rede Local, *Internet*, *Intranet*, *Extranet* ou via linhas discadas.
d) Segurança das informações. Apenas as pessoas autorizadas têm acesso aos respectivos documentos.
e) Preservação e administração dos documentos originais, que são mantidos em local seguro e com sistema de rastreabilidade.
f) Conversão dos documentos em texto (através de OCR/ICR), possibilitando a busca por palavras-chave.

Em resumo, o GED, através de técnicas como *Document Imaging*, permite que todos os tradicionais arquivos de documentos apostos em papel sejam convertidos para o meio digital. Os documentos passam a ser disponibilizados localmente ou via *Internet*, sendo rapidamente localizados e melhor gerenciados. Como conseqüência, obtêm-se a agilidade no suporte à tomada de decisões, fundamental na velocidade exigida nos negócios de hoje e, sobretudo, uma drástica redução nos espaços utilizados no arquivamento de documentos numa empresa.

Com o desenvolvimento das tecnologias citadas acima, dentre outras, essenciais a sobrevivência das empresas, um esforço vem sendo realizado com o intuito de reduzir as incompatibilidades do documento aposto em papel e os documentos eletrônicos, o que se desdobra em duas partes: no âmbito da informática, que desenvolvem técnicas que preencham as exigências legais dos documentos eletrônicos; e sob o ângulo legislativo, que busca positivar esta utilização, estabelecendo-se um amplo reconhecimento legal dos documentos eletrônicos.

Um dos critérios para a equiparação dos documentos apostos em papel e os documentos eletrônicos é a assinatura, assim como um documento pode ser assinado, um documento eletrônico, juntamente com outras gamas de tecnologias

que estão surgindo e evoluindo, também pode ser assinado. No próximo capítulo, serão abordadas as tecnologias utilizadas para determinar que um documento eletrônico seja íntegro e confiável.

II – Tecnologias usadas para assinatura digital

Este capítulo tem como objetivo descrever os aspectos relevantes das tecnologias usada na assinatura digital. Aborda-se primeiramente os fundamentos da criptografia, ou seja, a base conceitual necessária para compreender os métodos de cifragem e decifragem de uma informação e posteriormente sua relação com o conceito de chave pública ou privada.

2.1 – Aspectos gerais da criptografia

Criptografia* é a arte ou ciência de escrever em cifra ou em códigos, utilizando um conjunto de técnicas que torna uma mensagem ilegível, chamado de texto cifrado, de forma a permitir que apenas o destinatário desejado consiga decodificar e ler a mensagem com clareza, ou seja, a criptografia transforma textos legíveis, ou texto claro em um texto cifrado ou codificado, que usualmente tem a aparência de um texto randômico ilegível.

A técnica de criptografia é tão antiga quanto a própria escrita, já estava presente no sistema de escrita hieroglífica dos egípcios. Os romanos utilizavam códigos secretos para comunicar planos de batalha. O mais interessante é que esta técnica não mudou muito até meados deste século, somente depois da Segunda Guerra Mundial, com a invenção do computador, a área de pesquisa em criptografia realmente floresceu incorporando complexos algoritmos matemáticos que hoje são usados em aplicações comerciais. No âmbito da computação, a criptografia é importante para que se possa garantir a segurança quanto a alteração intencional ou

* (kriptós = escondido, oculto; grápho = grafia)

acidental em todo o ambiente computacional que necessite de sigilo, como por exemplo, documentos eletrônicos e transferência de fundos via Internet.

Há duas maneiras básicas de criptografar informações: através de códigos ou através de cifras. A primeira procura esconder através de códigos predefinidos entre as partes envolvidas na troca de informações, a segunda, a informação é cifras através da mistura e/ou substituição das letras que compõem a informação original.

Cifrar é o ato de transformar informações legíveis em alguma forma ilegível. Seu propósito é o de garantir a privacidade, mantendo a informação escondida de usuários não autorizados, mesmo que estas consigam visualizar os dados criptografados. Decifrar é o processo inverso, ou seja, transformar os dados criptografados na sua forma original, inteligível. Para cifrar ou decifrar uma informação, há necessidade de um elemento geralmente denominado chave ou senha. Dependendo do método de criptografia, emprega-se a mesma chave para criptografar e para descriptografar mensagens ou utilizam-se de senhas diferentes.

2.1.1 – Tipos de cifras

Os principais tipos de cifras são: (VOLPI, 2001:8).

a) Cifras de transposição*:* Método pelo qual o conteúdo da mensagem é o mesmo, porém as letras postas em ordem diferente. Por exemplo, pode-se cifrar o nome “KATIUCIA” e escrevê-lo “TAIACUKI”.

b) Cifras por substituição*:* Troca-se cada letra ou grupo de letras da informação original de acordo com uma tabela de substituição. As cifras de substituição podem ser divididas em:

a) Cifra de substituição simples ou Cifra de César: É o tipo de cifra na qual cada letra da mensagem é substituída por outra, de acordo com uma tabela baseada geralmente num deslocamento da letra original dentro do alfabeto. É um método que visa proteger textos com pequeno grau de sigilo. Por exemplo, trocar cada letra por outra que está 4 letras adiante na ordem alfabética, no caso de “KATIUCIA”, teremos “OEYMWGME”.

b) Cifra de substituição poli-alfabética: Consiste em usar várias cifras de substituição simples, em que as letras são substituídas segundo um processo de rotação em sequência. Por exemplo, pode-se utilizar duas tabelas usadas em alternância a cada 3 caracteres. Na tabela 1 é estabelecida a seguinte relação: K = *, A = &, T = %, I = D , U = 6, C = R, I = 1 , A= @; e na tabela 2 a relação: K = @, A = 1, T = R, I = 6 , U = D, C = %, I = & , A = *, a palavra "KATIUCIA" seria cifrada em "*&%6D%1@".

c) Cifra de substituição por deslocamento: Não utiliza um valor fixo para a substituição de todas as letras. Cada letra tem um valor associado para a rotação através de um critério. Por exemplo, cifrar a palavra 'KATIUCIA' utilizando o critério de rotação '216', seria substituir 'K' pela letra que está 2 (duas) posições a frente no alfabeto, o 'A' pela letra que está 1 (uma) posição a frente e assim sucessivamente, repetindo-se o critério. Então teríamos "MBZKVIKB".

d) Cifra de substituição de polígramos: Utiliza um grupo de caracteres ao invés de um único caractere individual para a substituição da informação, este método consiste em uma escrita que se baseia em um conjunto de símbolos cujo significado é conhecido por poucos, permitindo com isto que se criem textos que serão incompreensíveis aos que não saibam o padrão de conversão necessário para a sua leitura.

Vejamos um exemplo, a partir de um texto qualquer, a palavra "KATIUCIA". Se criarmos um código próprio, estabelecendo uma relação arbitrária entre letras e sinais, como:

KA = + TI = & UC = # IA = @

Apenas os que conhecerem a codificação entenderão que os sinais +&#@, unidos, significam a palavra "KATIUCIA", ou que +@ = "KAIA".

Pode-se então aplicar este método em dado arquivo digital e, a partir de um critério de conversão eleito, criar um segundo arquivo, criptografado. O seu conteúdo representará um *criptosistema* e assim, um texto redigido em linguagem cifrada.

A criptografia possibilita que se altere o arquivo digital original legível, estabelecendo uma relação arbitrária entre seu conteúdo e um novo arquivo criado a

partir deste, de modo que somente através de um procedimento específico para decifrá-lo, pode-se alcançar novamente a compreensão direta das informações que nele contiver.

Programas de computador foram criados para realizar esta tarefa, e adequados para que infinitos padrões de conversão possam ser oferecidos. Chegou-se ao ponto em que é possível criar um padrão específico para cada arquivo, de modo que o seja inaplicável aos demais. Com isso o sinal “+” pode significar a sílaba “KA” em um arquivo, o número “7” em outro, o caractere “%” em um terceiro, e assim por diante.

É esta relação de significância entre o arquivo original legível e seu criptograma que é aqui designado de padrão de conversão. Se o padrão de conversão deixa de ser geral, e passa a ser específico para cada vez que se quiser encriptar um arquivo, é necessário guardar os critérios usados para fixar o modo único de correlação de sinais ali aplicado, informação essencial para que o programa de computador posteriormente decodifique o criptograma e recupere o conteúdo original.

2.2 – Conceito de Chaves

As chaves são elementos fundamentais que interagem com um conjunto de algoritmos para a cifragem/decifragem de informação. São parâmetros atribuídos a um algoritmo criptográfico para que produza um criptograma específico. A chave decorre de equações matemáticas aplicadas a partir do conteúdo do arquivo, podendo também derivar de sua associação a outros dados digitalizados.

Do ponto de vista do usuário, as chaves de criptografia são similares às senhas de acesso. Usando a senha correta, o usuário tem acesso ao conteúdo da informação, caso contrário, o acesso é negado. No caso da criptografia, as chaves estão relacionadas com o acesso ou não à informação cifrada. Assim como as senhas, as chaves na criptografia também possuem diferentes tamanhos, sendo seu grau de segurança relacionado ao tamanho da chave.

Na criptografia moderna, as chaves são longas sequências de *bits*. Visto que um bit pode ter apenas dois valores, 0 ou 1, uma chave de três dígitos oferecerá

2^3 = 8 possíveis valores para a chave. Sendo assim, quanto maior for o tamanho das chaves, maior será o grau de confidenciabilidade[α] da informação.

É claro que aquele que conheça a chave terá o elemento central para manipular o arquivo, e assim possuir o total acesso ao seu conteúdo. À medida que um número maior de pessoas conheça a chave, a possibilidade de alguém revertê-lo ao estado original, alterá-lo e novamente criptografá-lo, aumenta, causando a diluição da certeza de sua integridade.

2.3 – Tipos de criptografia em relação ao uso de chaves

Há basicamente dois tipos de criptografia em relação ao uso de chaves. Diz-se estar usando um sistema de criptografia simétrico ou por chave secreta quando a encriptação e a decriptação são feitas com uma única chave, ou seja, tanto o emissor quanto o receptor usam a mesma chave. Caso estas chaves sejam diferentes, diz-se usar um sistema de criptografia assimétrica ou chave pública.

2.3.1 – Criptografia por chave simétrica

Tanto o emissor quanto o receptor da mensagem cifrada devem compartilhar a mesma chave, que deve ser mantida em segredo por ambos, conforme figura 1. Se uma das partes, por descuido ou não, divulgar a chave, o sigilo estará comprometido.

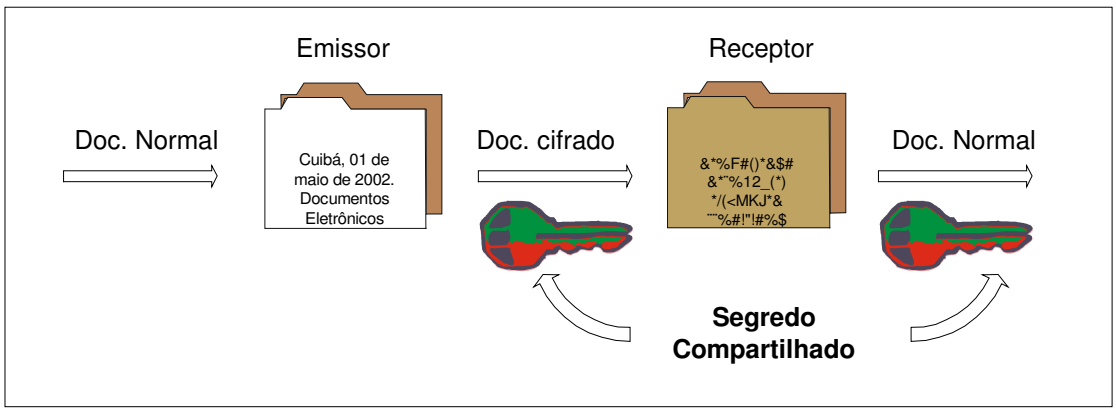

Figura 1 - Criptografia por chave simétrica.

[α] garantir que apenas quem autorizado possa acessar as informações.

Como o objetivo deste estudo é abordar a eficácia probatória do documento eletrônico, trataremos então somente de criptografia por chave assimétrica. Outro motivo para abordar somente este tópico, deve-se a Infra-estrutura que está sendo adotada no Brasil no que diz respeito a certificação digital.

2.3.2 – Criptografia por chave assimétrica

A criptografia por chave pública ou criptografia assimétrica, é baseada no uso de pares de chaves de caráter complementar para cifrar/decifrar mensagens. Estas chaves são matematicamente relacionadas, usando funções unidirecionais para a codificação da informação. Uma chave, chamada pública, é usada para cifrar, enquanto a outra, chamada chave privada ou secreta, é usada para decifrar.

A chave privada é necessariamente sigilosa, permanecendo com seu criador, e a outra (chave pública) é de livre conhecimento por terceiros, devendo ser alvo de ampla divulgação. Através delas, dois modos de operação ganham especial feição.

O primeiro modo permite que qualquer pessoa possa utilizar a chave pública para encriptar um arquivo. O criptograma que lhe é derivado, entretanto, só poderá ser revertido ao seu estado original se for utilizado uma chave privada. Com isso, só o detentor da chave privada poderá acessar o conteúdo do arquivo. É um processo que se volta mais para a função primeira da criptografia, que é a manutenção da confidenciabilidade das informações contidas no documento.

O segundo modo, de maior interesse para nossa análise, é o que permite ao titular utilizar a sua chave privada para criar o criptograma, o qual só poderá ser revertido ao seu estado original através da chave pública. Neste método, se a chave privada permanecer em sigilo e houver confiança nas máquinas e programas de computador utilizados para criar o criptograma, pode-se imputar, com razoável grau de segurança, a autoria da criação do arquivo ao detentor da chave privada, a qual compõe, com a chave pública, o par necessário às duas operações. Se a chave privada vier a ser descoberta por um intruso, o segredo das informações criptografadas com a chave privada e a chave pública correspondentes está comprometido.

2.4 – Criptografia simétrica X Criptografia assimétrica

Comprovando as bases fundamentais dos métodos de criptografia simétrica e assimétrica, observa-se que a criptografia assimétrica ou por chave pública tem vantagem sobre a chave secreta no sentido de viabilizar a comunicação segura entre partes envolvidas em uma dada relação. Outra vantagem é o fim do problema da distribuição de chaves existentes na criptografia simétrica, pois não há necessidade de compartilhamento de uma mesma chave, nem de um pré-acordo com as partes interessadas. Obtendo com isso, uma maior segurança.

2.5 – Principais algoritmos que utilizam chave assimétrica

Diversos são os algoritmos que utilizam em criptografia de chave assimétrica.

a) Diffie-Hellman: O algoritmo de Diffie-Hellman adota a técnica de troca de uma chave de cifragem de tal forma que uma terceira parte não autorizada, não tenha como deduzi-la. Cada participante inicia com sua chave secreta e através da troca de informações é derivada uma outra chave chamada chave de sessão, que será usada para futuras comunicações. O algoritmo baseia-se na exponenciação discreta, pois sua função inversa, os logaritmos discretos, é de alta complexidade.

b) RSA: Desenvolvido por a *Ron Rivest*, *Adi Shamir* e *Len Adleman*, o algoritmo tomou por base o estudo feito por *Diffie-Hellman*, porém usando outro fundamento matemático para a criação das chaves públicas. Utilizam o fato de que é fácil de se obter o resultado da multiplicação de dois números primos[&] extensos, porém, é muito complicado (moroso) se obter os fatores primos de um número muito extenso (COUTINHO, 2000:18).

Pelo fato do algoritmo RSA ser o mais utilizado e conhecido método da criptografia de chave pública em certificação digital, no Apêndice A é descrito detalhadamente seu funcionamento.

[&] Diz-se o número que é divisível apenas por ele mesmo e pela unidade.

2.6 – Autenticidade e sigilo

Com a criptografia assimétrica, pode-se garantir a autenticidade e o sigilo de um documento eletrônico. É fácil entender usando o envio de um documento eletrônico como exemplo: quando o emissor envia um documento cifrado usando sua chave privada, o receptor somente poderá decifrá-lo usando a chave pública do emissor, tendo assim, a garantia da autenticidade do documento, conforme a figura 2.

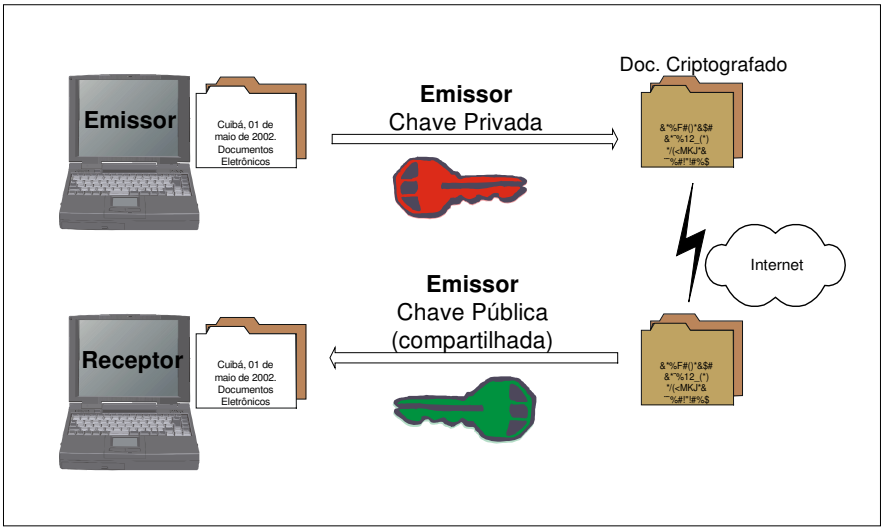

Figura 2 – Criptografia assimétrica – Autenticidade.

Uma vez que o receptor conhece a chave pública do emissor, ele possui meios de verificar a identidade do emissor, pela certificação digital. Neste caso, o sigilo não está garantido, pois qualquer pessoa que conheça a chave pública do emissor, poderá decifrar o documento.

Quando o emissor envia um documento cifrado usando a chave pública do receptor, somente o receptor poderá decifrá-lo usando sua chave privada, tendo assim a garantia do sigilo do documento.

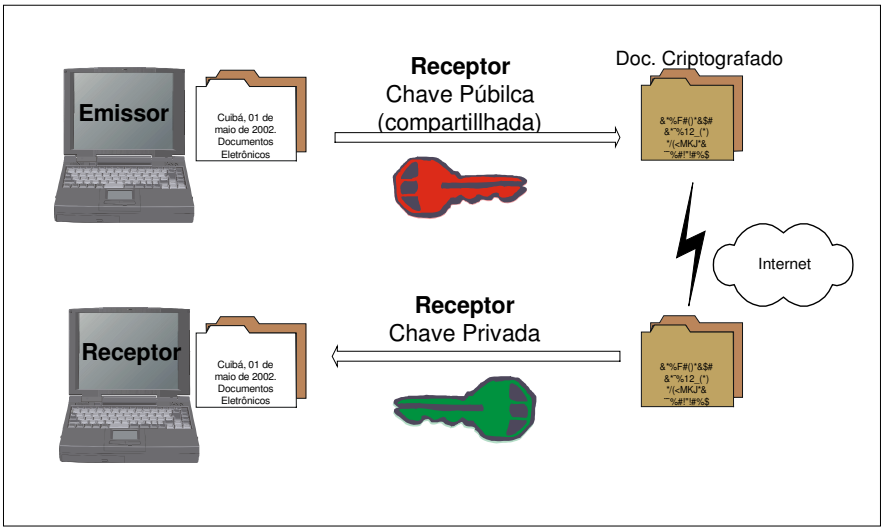

Figura 3 – Criptografia Assimétrica – Sigilo.

Neste caso, a autenticidade não está garantida, pois qualquer pessoa que tenha a chave pública do receptor pode usá-lo em nome de outra pessoa e enviar o documento.

Para garantir as duas coisas em um único processo, pode-se combinar os dois processos anteriores e utilizar uma função *Hashing* para facilitar a cifragem/decifragem das mensagens e garantir a integridade[α] do documento.

2.7 – Função *Hashing* e integridade

A função *hashing* aplicada ao conteúdo de um documento, gera um resumo. Este resumo é chamado de código *hash,* que para ser eficiente no seu propósito deve atender a dois critérios: - deve ser único para cada documento com conteúdo diferente e – deve ser tal que não se possa recompor o documento a partir do código *hash*.

Esta função tem por objetivo garantir a integridade do documento recebido e agilizar a decifração de um documento, pois a criptografia assimétrica embora muito eficiente na cifragem do documento, é muito lenta na decifração.

[α] garantir que os dados têm a origem correta e que não foram alterados entre origem e destino.

Se o documento for enviado com o resumo, basta o receptor aplicar a função *hashing* ao documento, calcular um novo código *hash* e comparar o novo código com o código *hash* descriptografado, proveniente do remetente criptografado. Tendo assim, a garantia de integridade, ou seja, comprova-se que o documento não foi violado. Basta que apenas um *bit* seja alterado no documento para que o novo código *hash* seja totalmente diferente do código *hash* recebido.

A função *hashing* utilizada de forma isolada em uma transmissão não garante totalmente a integridade, pois um intruso pode violar o documento, calcular e distribuir o código *hash*. Para resolver este problema, a criptografia assimétrica deve-se juntar à função *hash*, originando em um único processo denominado assinatura digital.

No exemplo a seguir, será mostrado uma situação prática exemplificando os conceitos de autenticidade, sigilo e integridade:

Se o usuário A e o usuário B quiserem se comunicar usando criptografia assimétrica, primeiramente, terão que obter respectivamente seus pares de chaves. Após tornarem-se responsáveis pela chave privada e chave pública gerada, o usuário A torna disponível sua chave pública para o usuário B, que por sua vez também fará o mesmo com a própria chave pública. Quando o usuário B quiser enviar uma mensagem secreta para o usuário A, ele deverá cifrar a mensagem, usando a chave pública de o usuário A, garantindo assim, que somente o usuário A, detentor e único conhecedor de sua chave privada possa decifrar a mensagem. Observa-se que se o usuário B utilizar somente a chave pública do usuário A para enviar a mensagem, o usuário A não terá como confiar na origem do mensagem, isto é, que o usuário B lhe enviou a mensagem. Verificando-se também que, se o usuário B cifrar a mensagem com sua chave privada e enviar, todos que conhecerem a chave pública poderão decifrá-la. Sendo assim, para que o usuário A tenha certeza da origem da mensagem, o usuário B terá que assiná-la digitalmente, combinando dois processos. Primeiramente, ele terá que cifrar a mensagem com sua chave privada, e em seguida, usar a chave pública do usuário A para cifrá-la novamente antes de enviar. Ao receber a mensagem, o usuário A deverá primeiramente usar a sua chave privada e após a chave pública do usuário B para obter a mensagem e notificar que realmente a mensagem é originada do usuário B, pois caso a

originalidade e sigilo da mensagem estiver comprometida, o usuário A não conseguirá decifrá-la, isto é, uma mensagem cifrada com uma chave somente será decifrada com a outra correspondente ao par.

2.8 – Assinatura digital

Cabe aqui ressaltar a diferença entre a assinatura eletrônica da assinatura digitalizada. A assinatura digital é um tipo de assinatura eletrônica e a assinatura digitalizada trabalha basicamente com captura e análise de dados biométricos como: impressão digital, íris e assinatura manuscrita. Assim, um documento do tipo fax, assinado, ao ser recebido, possuirá uma assinatura digitalizada.

A assinatura digital é um processo que utiliza basicamente a criptografia assimétrica e a função *hashing*, e tem como principal propósito garantir o sigilo, integridade e autenticidade dos documentos envolvidos em transações eletrônicas.

As propriedades da assinatura digital são:

a) assinatura autêntica: quando o receptor utiliza a chave pública do emissor para decifrar um documento, ele confirma que o documento provem do emissor e somente do emissor;

b) assinatura não pode ser forjada: somente o receptor conhece sua chave secreta;

c) documento assinado não pode ser alterado: se houver alteração no texto criptografado, o mesmo não poderá ser restaurado com o uso da chave pública do receptor;

d) assinatura não reutilizável: assinatura é particular de cada documento e não poder ser transferida para outro documento;

e) assinatura não poder ser repudiada: a assinatura pode ser reconhecida por quem as recebe, verificando sua validade e caso seja válida, ela não pode ser negada pelo seu proprietário.

As assinaturas digitais, aliadas à imputação das chaves a um sujeito determinado, compõem uma técnica que permite a estabilização do conteúdo do arquivo e a identificação do seu criador, atribuindo, com permanência, certo grau de

infungibilidade aos elementos imateriais ali expressos. É um mecanismo análogo ao modo pelo qual o elemento criativo individualiza as obras autorais, ou este, somado ao registro, fixa a extensão do objeto envolvido por um patente.

2.8.1 – Sigilo, integridade e autenticidade

É possível, através da criptografia assimétrica obter a garantia da autenticidade de forma isolada e o sigilo também de forma isolada. Obtêm-se também, com o uso da função *Hash* a garantia de integridade isolada. Pra obter-se a garantia de autenticidade, sigilo e integridade de forma íntegra é necessário juntar todos os processos vistos acima em apenas um. A seguir, estabelece-se primeiramente um processo para obter a integridade e a autenticidade, após a integridade e o sigilo e finalmente a integridade, autenticidade e sigilo em um único processo.

Para a garantia da integridade e autenticidade do documento, o emissor deve gerar o código *Hash* a partir do documento original e cifrá-lo usando sua chave privada, obtendo assim, uma assinatura criptografada. O receptor por sua vez, deve decifrar a assinatura criptografada com a chave púbica do emissor, em seguida, gerar o novo código *Hash* do documento recebido e comparar o resultado obtido com a assinatura (código *Hash*) decifrada. Se forem iguais, a integridade está garantida, e o fato de apenas o emissor do documento pode ser identificado pela sua chave pública, pois somente o mesmo detêm posse de sua chave privada, a autenticidade também está garantida, conforme é mostrada na figura 4.

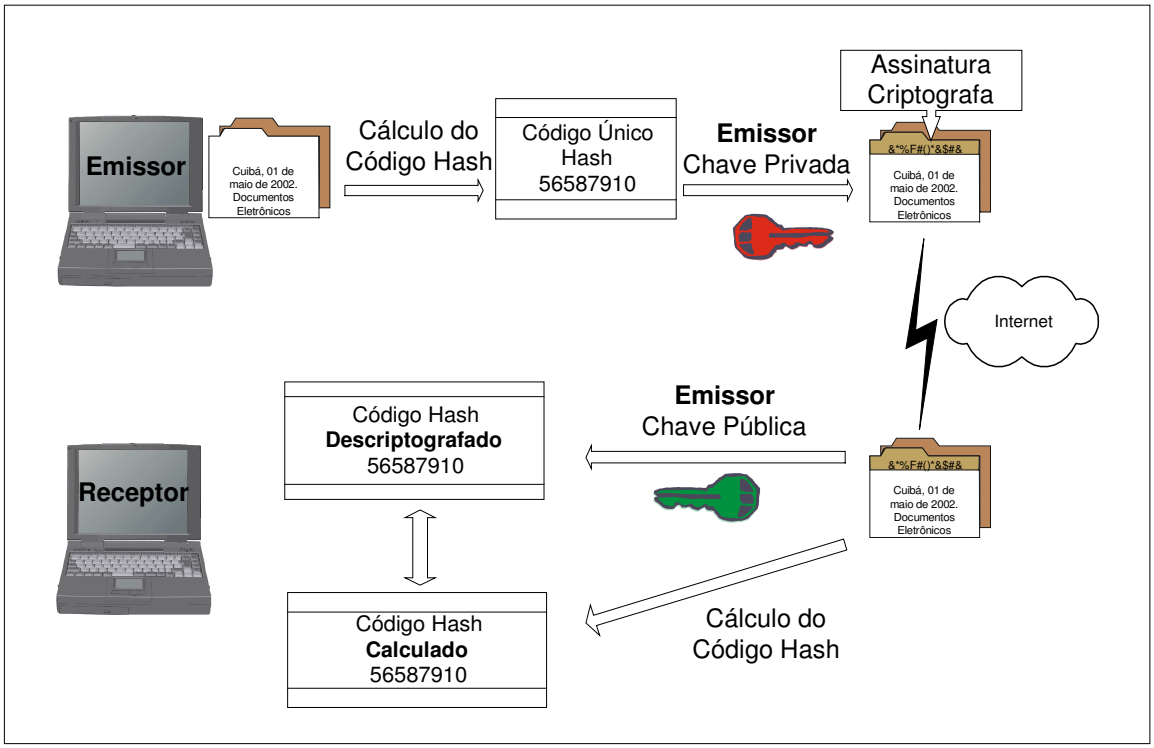

Figura 4 – Garantia de integridade e autenticidade - Criptografia assimétrica + *Hash*.

Para a garantia da integridade e sigilo do documento, o emissor deve gerar o código *Hash* a partir do documento original e cifrá-lo usando a chave pública do receptor, obtendo assim, uma assinatura criptografada. O receptor por sua vez, deve decifrar a assinatura criptografada com sua chave privada, em seguida, gerar o novo código *Hash* do documento recebido e comparar o resultado obtido com a assinatura (código *Hash*) decifrada. Se forem iguais, a integridade está garantida, e o fato de apenas o receptor do documento poder decifrá-lo com sua chave privada, , pois somente o mesmo detêm posse desta, o sigilo também está garantido, conforme ilustra a figura 5.

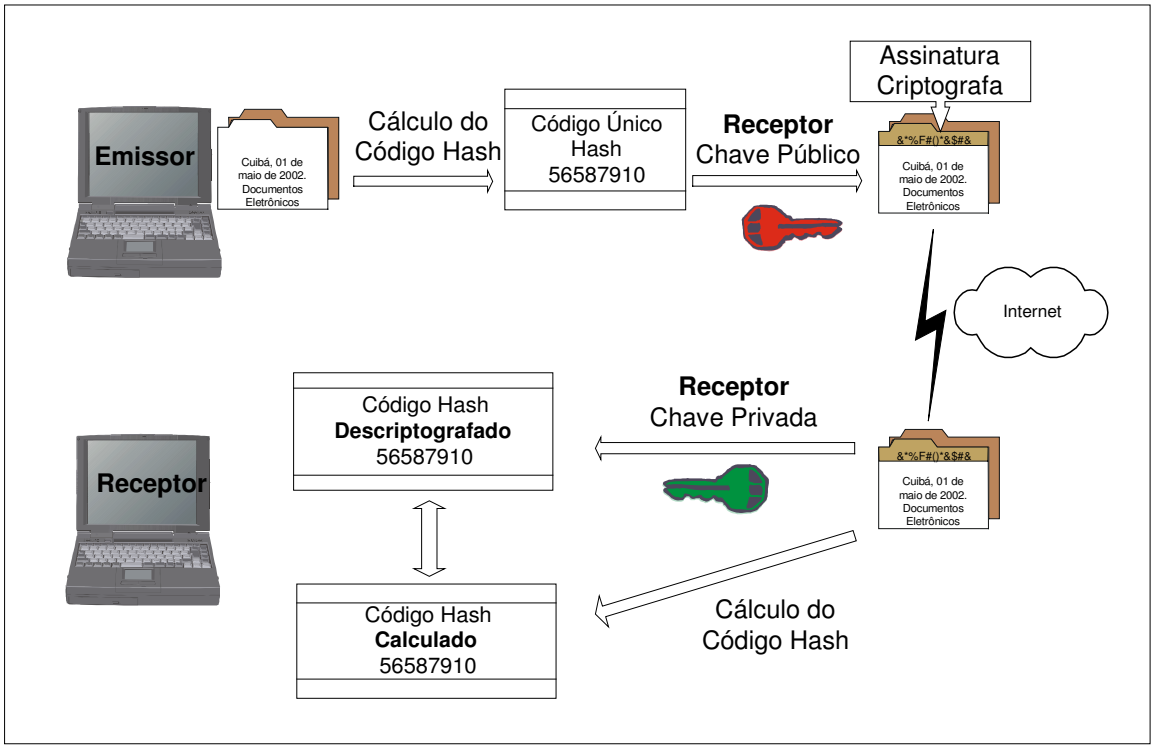

Figura 5 – Garantia de integridade e sigilo - Criptografia assimétrica + *Hash*.

Finalmente, para a garantia da integridade, autenticidade e sigilo do documento, deve-se combinar os dois processo acima onde o emissor deve, após gerar o código *Hash* a partir do documento original, cifrá-lo duas vezes: primeiro com sua chave privada, e após, cifrar o resultado obtido com a chave pública do receptor. O receptor por sua vez, deve decifrar a assinatura criptografada com sua chave privada, e após, descriptografar o resultado obtido com a chave pública do emissor e, só então, gerar o novo código *Hash* do documento recebido e comparar o resultado obtido com a assinatura (código *Hash*) decifrada.

A aceitação da assinatura digital como hábil para solucionar as questões de integridade e autoria dos arquivos depende não apenas da confiança em sua idoneidade, mas também de operacionalizar a solução de importantes problemas que ela introduz.

Dentre os mais relevantes, podemos citar a necessidade de procedimentos que determinem a pertinência do par de chaves e seu prazo de validade, com o correlato direito a repudiá-las, caso estejam vencidas ou seja

detectada fraude. Uma proposta de solução é a de atribuir a um terceiro, por lei ou por acordo entre os interessados, poderes para certificar que as chaves são válidas e pertinentes ao presumido autor do arquivo. É a mais adotada pelos países que, em reconhecendo atributos dos documentos nos arquivos digitais, emanaram leis diretamente voltadas para viabilizar os modos desta equiparação.

Atendendo a última propriedade da assinatura digital, isto é, para validar, se realmente a assinatura digital ou chave pública refere-se à determinada pessoa deve-se recorrer a tecnologia de certificados digitais. No próximo capítulo será abordada a tecnologia de certificados digitais e a Infra-estrutura de chaves privadas, cujo objetivo principal é vincular uma assinatura digital a um indivíduo, organização ou qualquer entidade.

III – Certificação digital e Infra-estrutura de chaves públicas

A técnica de criptografia assimétrica é a base dos sistemas de segurança de documento eletrônico. A assinatura digital, que é resultado da aplicação da criptografia assimétrica, utiliza a chave pública e privada para garantir a autenticidade, sigilo e integridade dos documentos eletrônicos. Devido a crescente utilização destas chaves, surgem dúvidas referente à distribuição das chaves públicas e da garantia de que a chave pública se refere na íntegra à pessoa de posse da mesma. Sem um controle das chaves, qualquer pessoa poderia utilizar uma chave pública aleatória, dizendo ser de sua posse. Sobre essa visão, uma das soluções para este impasse seria a troca das chaves pessoalmente entre duas pessoas, porém o transtorno e a obrigação do encontro corpóreo e o elevado custo envolvido na troca, tornam esta solução inviável.

Desenvolveu-se então, como solução para o problema acima citado, a tecnologia dos certificados digitais.

3.1 – Certificação digital

O certificado digital associa a identidade de um titular a um par de chaves assimétricas (uma pública e outra privada), que, usadas em conjunto, fornecem a comprovação da identidade. É uma versão digital de algo parecido com uma cédula de identidade e serve como prova de identidade, reconhecida diante de qualquer situação onde seja necessária comprovação de identidade.

O objetivo fim da Certificação digital é dar validade jurídica aos documentos eletrônicos, isto é, torná-los passíveis de serem autenticados e com firma reconhecida como é no mundo real.

Assim como a Carteira de Identidade é assinada por um Órgão de Segurança que lhe dá credibilidade, o certificado digital é emitido e assinado (chancelado) por uma Autoridade Certificadora (AC) digital que emite o certificado.

Um certificado digital contém três elementos:

a) informação de atributo: são as informações sobre o projeto que é certificado. No caso de uma empresa, pode-se incluir a razão social, CNPJ, responsável, etc;

b) chave de informação pública: é a chave pública da entidade certificada. O certificado associa a chave pública à informação do atributo.

c) assinatura da autoridade em certificação: a AC assina dois primeiros elementos e, então adiciona credibilidade ao certificado. Quem receber o certificado, se verificará e se convencerá na informação do atributo e da chave pública se acreditar na autoridade certificadora.

Com a informação do atributo, a chave de informação pública e a assinatura da autoridade em certificação, forma-se a certificação digital. Segue abaixo as fases de um certificado digital.

3.1.1 – Fases de um certificado digital

Todo certificado passa por várias fases, desde seu requerimento até o fim de sua validade. Fica a autoridade certificadora, responsável pelo acompanhamento de todo o ciclo de vida dos certificados por ela emitidos.

O certificado digital é constituído das seguintes etapas:

a) requerimento: é o pedido da certificação digital , feito por uma pessoa interessada à Autoridade Certificadora;

b) validação do requerimento: é função da AC garantir que o requerimento seja válido e que os dados do requerentes sejam corretos;

c) emissão do certificado: é o ato de reconhecimento do título do certificado digital pelo requerente e sua emissão;

d) aceitação do certificado pelo requerente: após emitido, o requerente deve retirá-lo da AC e confirmar a validade do certificado emitido;

e) uso do certificado: é de total responsabilidade do requerente o uso do certificado;

f) suspensão do certificado digital: é o ato pelo qual o certificado se torna temporariamente inválido para operações por algum motivo especificado pela AC, como, o comprometimento da chave pública;

g) revogação do certificado: é o processo pelo qual o certificado se torna definitivamente inválido pelo comprometimento da chave privada do titular ou quando ocorrer algum fato que torne o certificado digital pouco seguro para uso. Um certificado suspenso ou revogado deve ser publicado na lista de certificados revogados (LCR) e estar sempre disponível para consulta;

h) término da validade e renovação do certificado: o certificado digital tem um período preestabelecido de validade atribuído pela AC. Em geral, este período é de um a três anos, dependendo da importância e finalidade da chave.

Abaixo, a figura 6 mostra uma representação pictórica do ciclo de vida do Certificado Digital.

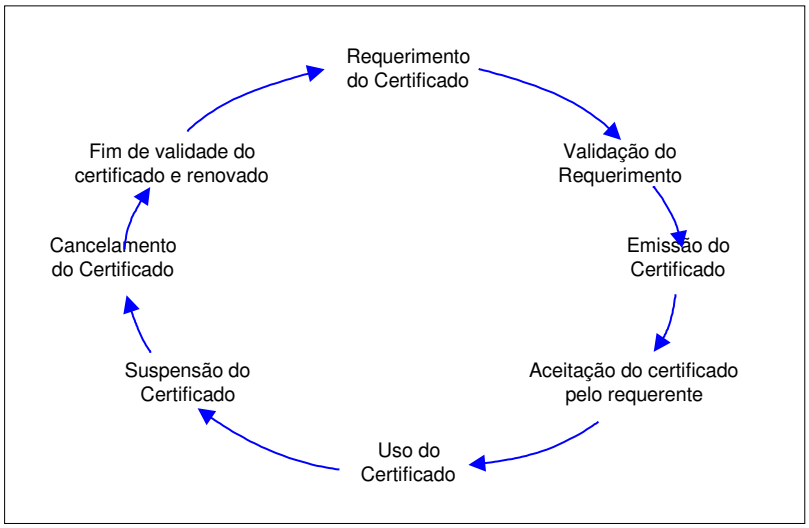

Figura 6 – Ciclo de vida do Certificado Digital.

Durante a fase de uso, os certificados digitais podem ser utilizados principalmente para envio de documentos eletrônicos assinados e/ou codificados e

para o estabelecimento de conexões seguras em seções Web entre cliente e servidor e, entre servidores.

Atualmente, os browsers possuem suporte para mensagens certificadas, o que torna muito simples a instalação da chave e seu uso para criptografar e assinar digitalmente as mensagens enviadas e decifrar as mensagens recebidas.

A certificadora digital é apenas um dos componentes que viabiliza a funcionalidade dos cartórios no mundo virtual, permitindo transações muito mais sofisticadas. Uma estrutura maior e organizada é necessária para estabelecer os requisitos mínimos para a seguridade e legalidade das autoridades certificadoras, essa estrutura é a PKI (*Public Key Infrastructure*) ou ICP (Infra-estrutura de chaves públicas).

3.2 – Infra-estrutura de chaves públicas

Chama-se Infra-estrutura de Chaves Públicas a toda infra-estrutura do uso e obtenção de certificados digitais, pode-se dizer simplificadamente, que ela tem como função básica certificar, isto é, vincular uma chave pública a um indivíduo, organização ou qualquer entidade, e verificar a validade de um certificado emitido. Os elementos que fazem parte da infra-estrutura de chaves públicas são: i) titular do certificado: aquele que faz uso do certificado digital; ii) autoridade certificadora raiz (AC-Raiz): realiza o licenciamento das AC, emite , mantêm e cancela os certificados das AC; iii) autoridade certificadora (AC): responsável pela emissão do certificado digital, pela identificação do titular do certificado e pelo gerenciamento da lista de certificados revogados; iv) autoridade de registro (AR): responsável pela identificação do usuário final, por receber solicitações de emissão ou de revogação dos certificados, disponibilizar os certificados emitidos pela AC aos seus respectivos solicitantes e serve como intermediária entre o usuário e a AC; v) repositório de certificados e LCR: é um repositório que pode ser acessado por todos os membros da ICP e onde ficam armazenados os certificados emitidos, bem como os revogados.

Na figura 7 é ilustrada o Sistema Hierárquico da ICP-Brasil.

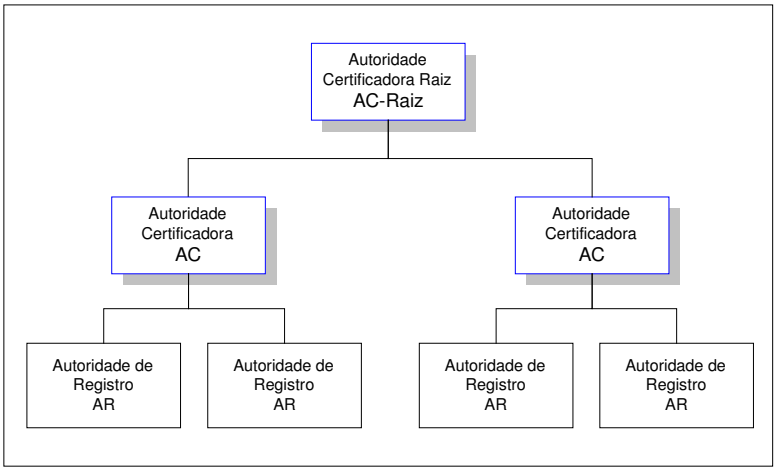

Figura 7 – Hierarquia da Infra-Estrutura de Chave Púbica

Por meio da Medida Provisória 2200, de 28 de junho de 2001, foi instituída no Brasil a Infra-estrutura de chaves públicas. O órgão formulará a política e definirá normas e procedimentos para garantir a autenticidade, integridade e validade jurídica dos documentos eletrônicos em todo os níveis de cadeia de certificação. Fica responsável também por homologar, auditar e fiscalizar os prestadores de serviço de certificação digital.

Depois de muito decidir, a SERPRO[&] foi nomeada Unidade Certificadora Raiz por ser o órgão mais capacitado tecnologicamente para assumir este papel e é a responsável pela chave raiz da ICP-Brasil. Perante esta decisão, fica claro sob o prejuízo das empresas privadas, pois, sendo a SERPRO governamental, fica ela obrigada a prestar serviços aos órgão públicos.

O Comitê Gestor da ICP-Brasil, que exerce a função de autoridade gestora de políticas, vinculada à Casa Civil da Presidência da República terá entre os seus membros representantes da sociedade civil que sejam integrantes dos setores interessados, os quais serão designados pelo Presidente da República, com mandato de dois anos (permitida a recondução), e sem remuneração por se tratar de função de relevante interesse público. Além disto, o Comitê Gestor ICP – Brasil é

[&] Serviço Federal de Processamento de Dados, prestadora de serviços do Instituto Nacional de Tecnologia da Informação(ITI), neste contexto.

composto pelos representantes dos seguintes Ministérios: Justiça; Fazenda; Desenvolvimento, Indústria e Comércio Exterior; Planejamento, Orçamento e Gestão; Ciência e Tecnologia; Casa Civil da Presidência da República e Gabinete Institucional da Presidência da República. Seus membros aprovaram os requisitos mínimos para políticas de certificado na ICP-Brasil pela Resolução Nº 7, de 11 de Dezembro de 2001. Abaixo, segue alguns dos principais requisitos.

Os certificados digitais usa a criptografia assimétrica e para usuários finais da ICP são divididos em oito tipos, sendo quatro relacionados com assinatura digital e quatro com sigilo. Os quatro tipos dentro da assinatura e do sigilo se dividem segundo os requisitos de segurança, podendo ser: tamanho da chave criptográfica, mídia armazenadora da chave, processo de geração do par de chaves, procedimentos de identificação do titular de certificado, frequência de emissão da correspondente LCR e extensão do período de validade do certificado.

Devido aos inúmeros motivos para se revogar um certificado antes da sua data de expiração, como por exemplo, quando constatada emissão imprópria ou defeituosa do mesmo ou quando for necessário a alteração de qualquer informação constante no mesmo, a ICP deve ter incorporado um sistema de revogação de certificados. Todos os certificados, quando revogados, devem ser adicionados à LCR dentro de um tempo limite para revogação. Esta lista deve ser consultada para se assegurar da validade da certificação digital, pois o fato do certificado não ter sigilo violado, não implica necessariamente que este não tenha sido cancelado.

A ICP deve prover meios de cópia de segurança e recuperação de chaves para atender à casos como esquecimento de senha, ou perda da chave por danificação ou panes dos próprios equipamentos. As cópias de segurança somente poderão ser feitas mediante solicitação do respectivo titular, e quando se tratar de certificado de sigilo por ela emitido.

Os pares de chaves não possuem vida útil indeterminada, devem ser atualizados periodicamente, dependendo do nível de segurança previsto para o tipo de certificado. Além disso, é necessário que o histórico das chaves de criptografia de sigilo usados anteriormente sejam preservados para garantir que informações antigas criptografadas possam ser decodificadas.

Apesar da certificação digital ser de interesse de todos que se mantém atualizados tecnologicamente, como intensificador que garanta a segurança na atividade de negócios eletrônicos, está nítido que o desfio para desenvolver a infra-estrutura de chaves públicas subjacentes que contemple todos os diversos aspectos satisfatoriamente é grande.

Resumindo, assim como um documento aposto em papel, um documento eletrônico pode determinar seu autor e a veracidade de seu conteúdo no mundo virtual, ou seja, um documento eletrônico pode ser autenticado e ter firma reconhecida como no mundo real, conforme figuras 8 e 9.

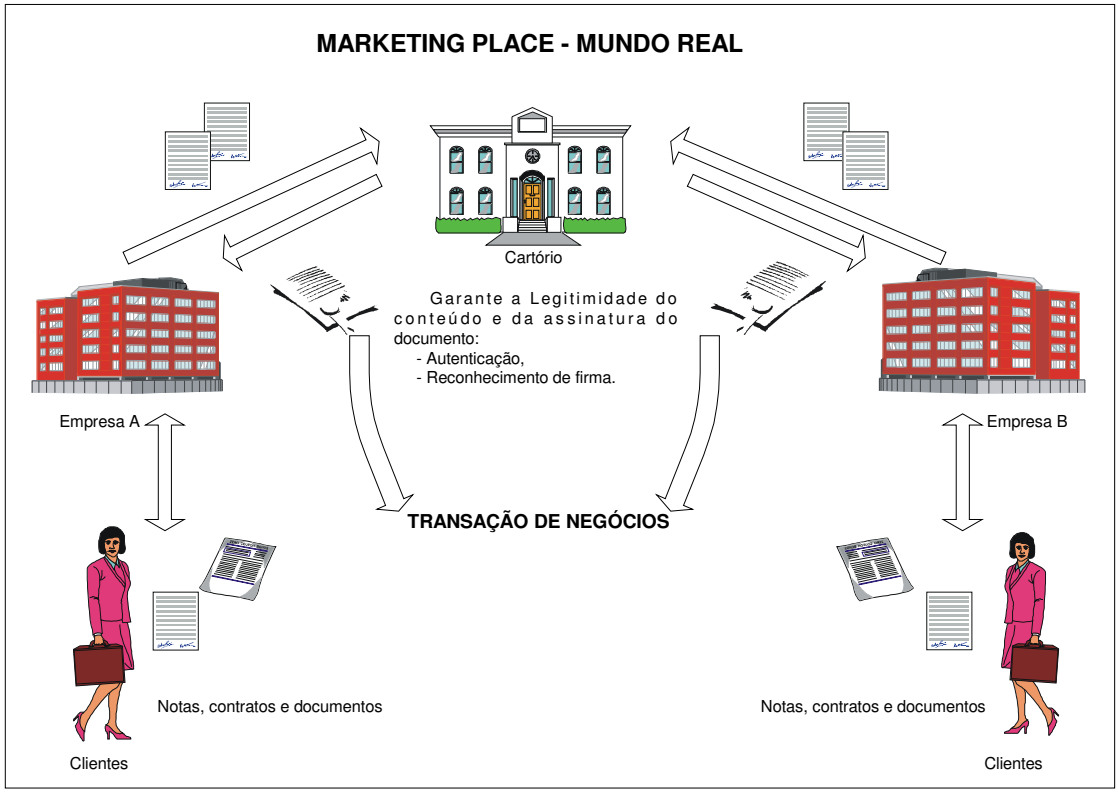

Figura 8 – Marketing Place – Mundo Real

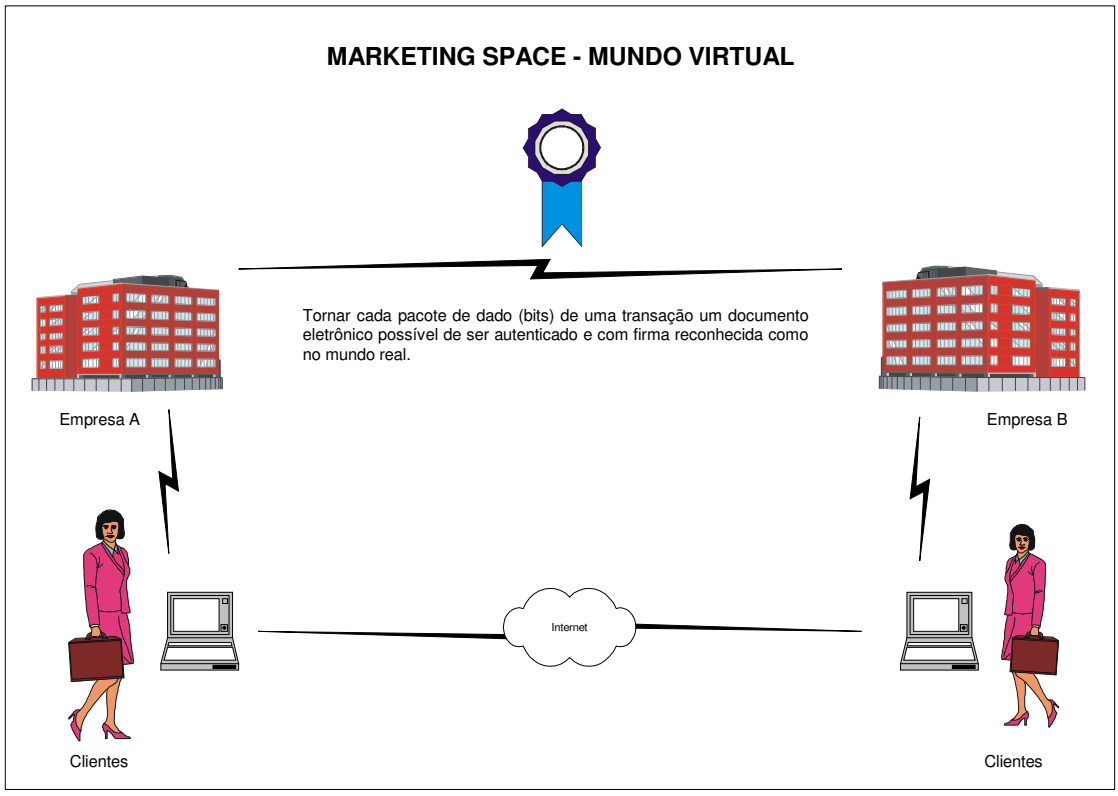

Figura 9 – Marketing Place – Mundo Virtual.

No próximo capítulo serão abordados os aspectos jurídicos relevantes dos documentos eletrônicos e a integração do GED aos sistemas jurídicos vigentes.

IV – Validade Jurídica do Documento Eletrônico

A inadequação do papel, ou de outros materiais similares, como suporte material para documentos, se evidencia quando se analisa as complicações que surgem no momento de sua conservação ou transmissão. Além disso, tanto a assinatura como os próprios suportes materiais são objeto de falsificações sempre mais perfeitas e de mais difícil verificação.

O reconhecimento do uso cotidiano, cada vez maior, de documentos eletrônicos estimulado pelas inúmeras aplicações do comércio eletrônico que surgem. As relações jurídicas prevêem, quase sempre, uma troca de documentos em relação aos quais se conheça com razoável certeza a paternidade e originalidade: em outras palavras, é muito importante saber que aquele documento foi redigido realmente por aquela pessoa e não possa ter sido posteriormente modificado.

4.1 – A Necessidade de uma Abordagem Jurídica dos Documentos Eletrônicos

No intuito de fornecer uma definição de documento eletrônico e na busca de estabelecer qual seja o valor jurídico de tal documento, devemos ter presentes dois interesses algumas vezes contrapostos:

a) a necessidade de permitir a mais eficaz e a mais vasta utilização dos novos meios oferecidos pela tecnologia (no caso do GED);

b) a necessidade de tutelar adequadamente a confiança dos operadores econômicos e, mais geralmente, de todos os cidadãos, nos novos documentos e na sua segurança.

Estudiosos sobre documentação eletrônica como o advogado Marcos da Costa[β], abordam a necessidade do estudo e normatização dos documentos eletrônicos com base em suas evidentes vantagens, quando comparados com os documentos tradicionais sobre o papel: o aporte de recursos eletrônicos tem o condão de expandir essas circunstanciais limitações, tornando o documento mais seguro, confiável, melhor administrável no sentido de que seu armazenamento e recuperação, sendo sua transmissão muito mais eficiente e rápida, além de segura.

Cabe aqui ressaltar que há necessidade de bem identificar, e eliminar, os eventuais obstáculos que possam opor-se à ampla adoção dos documentos eletrônicos se, então, não existem obstáculos lógicos para que o documento assuma forma sobre materiais, torna-se oportuno identificar os obstáculos que se interpõem à sua adoção (documentos eletrônicos) e difusão com valor legal.

A passagem do documento em papel para aquele digital é uma passagem obrigatória em direção à sociedade da informação, seja para a administração pública, seja nas relações privadas, porque permite desmaterializar a informação, desvinculando-a do suporte. Desta maneira se obtém um tipo de 'informação pura', somente 'conteúdo', que pode de tempos em tempos ser colocada sobre o papel ou sobre um suporte informático, ou transmitida para qualquer lugar em tempo real.

4.2. – Documento genericamente considerado e Documento eletrônico

A palavra documento, pode ser conceituada como: "Qualquer base de conhecimento, fixada materialmente e disposta de maneira que se possa utilizar para consulta, estudo, prova, etc"; "Escritura destinada a comprovar um fato;

[β] Ver em http://www.marcosdacosta.adv.br

declaração escrita, revestida de forma padronizada, sobre fato(s) ou acontecimento(s) de natureza jurídica" (FERREIRA, 1988:488)

Os autores, ao conceituar documento, dividem-se em duas correntes. A primeira se apega à matéria e ao meio de fixação física do mesmo, enquanto que a segunda procura destacar o seu conteúdo. Nesta segunda posição, pode-se destacar a presença dos juristas, visto que estes visualizam o documento como sendo o instrumento cuja finalidade é a prova de algum fato.

A idéia acentuada que existe é que o documento se consubstancia numa coisa fixada materialmente; por esta razão, muitos entendem que o elemento-conteúdo é inseparável de seu suporte físico.

Partindo dos dados levantados, pode-se verificar que a preocupação em conceituar documento de forma a evidenciar sua materialidade não é desprovida de fundamento, pois a maior parte dos conceitos atribui uma especial consideração ao seu suporte físico. Muitos autores asseveram que é justamente o elemento continente, ou seja, o suporte utilizado para materialização do documento, que garantirá o grau de fidelidade em relação ao que seu autor quis representar

Não se pode associar o documento com uma representação de um fato por meio da linguagem escrita e aposta em papel, pois desde os tempos mais remotos não é fundamental que seu suporte seja o papel.

A função básica dos documentos genericamente considerados sempre foi e continua sendo, idealmente, o registro fiel de um fato ou informação. É crucial que o documento cumpra sua finalidade, independentemente da forma de documentação utilizada

Diante da evolução da sociedade deve-se tender cada vez mais para a flexibilização dos conceitos. Por isso, um documento é qualquer meio capaz de representar um significado compreensível, não sendo necessário que seja escrito a mão ou por quaisquer outros meios mecânicos. Seu suporte não é o mais relevante, que o que interessa, realmente, é seu conteúdo.

O documento tradicional, aposto em papel, não mais se adequa à necessidade atual de dar agilidade à circulação de informações. São evidentes as suas limitações, tanto em relação à conservação, como à transmissibilidade e segurança.

Marcacini contribui para um conceito mais evoluído de documento:

> "A característica de um documento é a possibilidade de ser futuramente observado; o documento narra, para o futuro, um fato ou pensamento presente. Daí ser também definido como prova histórica. Diversamente, representações cênicas ou narrativas orais, feitas ao vivo, representam um fato no momento em que são realizadas, mas não se perpetuam, não registram o fato para o futuro. Se esta é a característica marcante do documento, é lícito dizer que, na medida em que a técnica evolui permitindo registro permanente dos fatos sem fixá-los de modo inseparável de alguma coisa corpórea, tal registro também pode ser considerado documento. A tradicional definição de documento enquanto coisa é justificada pela impossibilidade, até então, de registrar fatos de outro modo, que não apegado de modo inseparável a algo tangível".

Diante desse entendimento, sendo o documento íntegro e confiável para a representação de um fato, não importa sua forma de apresentação, não persistindo a idéia de vinculação de seu conteúdo com seu elemento continente.

Conceituar documentos eletrônicos, bem como os demais elementos de seu entorno, não se apresenta como tarefa das mais fáceis. Isso não decorre só da normal dificuldade em se definir algo com precisão mas, também, decorre do fato do tema apresentar um complicador adicional, oriundo da estreita dependência de técnicas e tecnologias extremamente novas e mutáveis. Sendo os documentos eletrônicos produtos altamente vinculados a tais fatores, é difícil formular-se um conceito com a necessária neutralidade. O documento eletrônico, concretamente, na realidade de hoje, explica-se a partir de um determinado modelo técnico e de uma determinada realidade tecnológica, pode-se conceituar como sendo uma dada seqüência de *bits* que, captada pelos nossos sentidos com o uso de um computador e um *software* específico, nos transmite uma informação.

O PROJETO DE LEI n.º 2.644/96 (veja Anexo IV)– de autoria do deputado Jovair Arantes, que visa dispor sobre a elaboração, o arquivamento e o uso de documentos eletrônicos –, em seu art. 1.º afirma que *"considera-se documento eletrônico, para os efeitos desta Lei, todo documento, público ou particular, originado por processamento eletrônico de dados e armazenado em meio magnético, optomagnético, eletrônico ou similar*."

Na elaboração de um conceito de documento eletrônico e, por extensão, de normas que o regulem, é fundamental a observação de alguns critérios. O primeiro deles é a sua não vinculação direta a uma técnica específica ou a um suporte determinado, mesmo que dominante ou único no momento, considerando a

constante evolução tecnológica não convém que se faça uma opção por esta ou aquela tecnologia, que poderá estar ultrapassada em curto prazo de tempo.(CASTRO, s/a). O segundo ponto importante está em ressaltar-se as características de garantia de integridade e plena possibilidade de verificação da autenticidade (autoria, proveniência, paternidade). Finalmente, em terceiro lugar, deve-se manter a tendência de privilegiar o entendimento do termo "documento" como referindo-se muito mais ao fato registrado do que ao meio de feitura deste registro. Nesse sentido, assim se resumem as exigências a serem por ele atendidas pelos documentos eletrônicos: a) ser capaz de registrar um fato; b) poder visualizar-se numa forma humanamente compreensível; c) ser relativamente permanente e idôneo (não modificável sem deixar vestígios); d) propiciar a capacidade de transmissão dos fatos registrados; e) ser capaz de garantir a imputabilidade subjetiva e o não repúdio; f) utilizar-se de uma tecnologia eletrônica ou digital qualquer (tanto para suporte do documento, quanto para sua manipulação).

4.3. – Requisitos Essenciais Básicos para a Obtenção da Validade Jurídica dos Documentos Eletrônicos

Um documento eletrônico não pode ser assinado no modo tradicional, através do qual o autor escreve o seu nome e sobrenome. Em razão disso, é impossível que ele, por si só considerado, assuma o mesmo valor de um documento assinado sobre um suporte de papel, visto que a assinatura carrega as três funções fundamentais já mencionadas (identificativa, declarativa e probatória). Não havendo assinatura, não se cumprem essas três citadas funções e, com isso, não se tem como aferir a autenticidade do documento eletrônico. Além disso, um documento eletrônico normal, comum, por sua própria natureza e em virtude de seus próprios fins, é algo extremamente volátil, alterável, que não guarda nenhum vestígio das modificações que sobre ele sejam efetuadas. Assim delimita o problema da validade jurídica destes novos documentos, "escritos" através do uso de *bit*s: Os *bits* são uns iguais aos outros, sua cópia é sempre idêntica ao original, as alterações não deixam rastros, a falsificação é facílima. Necessita-se de um sistema para 'certificar' os *bit*s, para fazer com que se possa ter certeza que uma 'escritura digital' é dada por

constituída em um determinado momento, por um determinado sujeito e que a partir dali o seu conteúdo não possa ter sido modificado.

Os documentos eletrônicos, para que possuam validade jurídica plena vale dizer, o atributo da eficácia probatória, devem preencher determinados requisitos essenciais. Tais requisitos, em termos de finalidades, apresentam-se similares àqueles exigidos dos documentos tradicionais e, ao mesmo tempo, apresentam-se completamente diferentes destes em relação à forma prática de seu suprimento e verificação. Logo, tem-se, que, em primeiro lugar, é necessário assegurar-se que um documento eletrônico possua integridade, ou seja, que permita um controle sobre a manutenção e conservação da inteireza de seu conteúdo, impossibilitando adulterações não detectáveis. Em segundo lugar, um documento eletrônico deve ser autêntico, ou seja, devem ter sua autoria, sua paternidade, sua proveniência, seguramente determinável, de maneira a assegurar o não repúdio. Em terceiro lugar, acrescente-se, é necessário que o documento eletrônico possua uma forma confiável de datá-lo, a fim de que a sua tempestividade possa ser aferida e comprovada com ampla segurança. Em relação à tempestividade, registre-se que, conforme já explicado anteriormente, ainda que seja ela entendida como aspecto inerente à integridade, não é exagero citá-la em separado. Isso, para fins de destaque, em função do cuidado especial que merecem as datas, em geral, no âmbito do Direito e, com mais razão, no âmbito específico dos documentos eletrônicos, devido à fácil alterabilidade apresentada pelos dados digitais.

4.4 – A Busca Inicial de Formas de Garantir a Validade Jurídica dos Documentos Eletrônicos

Conhecidos os requisitos essenciais a serem atendidos para a obtenção de documentos eletrônicos com validade jurídica (autenticidade, integridade e tempestividade), torna-se importante o conhecimento de algumas idéias iniciais que procuraram atingir tal objetivo, ainda que não tenham logrado pleno êxito (nesse caso, dentro do possível, procurar-se-á apontar as eventuais causas determinantes do insucesso).

4.4.1 – Uso de Suportes Informáticos Indeléveis (Visando Integridade)

Inicialmente, com o advento dos suportes informáticos não regraváveis (como os discos ópticos WORM e CD-ROM, por exemplo), pensou-se que neles se encontraria uma forma de criação de documentos eletrônicos com validade jurídica. Uma vez que tais suportes informáticos não permitem alteração de conteúdo após a execução da primeira e única gravação, observou-se que tal indelebilidade dotaria, o documento eletrônico assim formado de uma garantia de integridade. Ocorre, porém, que tais suportes informáticos não possibilitam, por si só, nenhuma forma viável de comprovação de autenticidade. Cogitou-se a possibilidade do próprio disco óptico sofrer a aposição de uma assinatura manual tradicional, porém, um disco óptico pode conter milhares de documentos distintos, e não seria possível lançar todas as assinaturas sobre sua superfície. Além disso, mesmo que o procedimento de assinatura fosse factível desse modo, não se conseguiria vincular cada assinatura ao respectivo e específico documento ao qual ela devesse referir. Mesmo na hipótese de que os problemas citados fossem superáveis, constata que, ainda assim, o uso de suportes informáticos as características WORM não constituir-se-ia em grande avanço, apesar disso, criando-se um liame físico entre continente e conteúdo, a memória WORM apresenta os mesmos limites próprios dos tradicionais documentos em papel: o conteúdo não pode, de fato, separar-se do continente, sob pena da perda do seu eventual valor jurídico, a menos que o procedimento de duplicação seja acompanhado de idônea garantia (por exemplo, intervenção de um oficial público) de modo análogo à duplicação de um tradicional documento em papel.

A partir dessa necessidade de não só conferir integridade ao conteúdo, mas também conferir-lhe autenticidade, é que partiu-se para a busca de meios capazes de suprir os efeitos de uma assinatura tradicional. Dentro de tal entendimento, a seguir serão abordadas algumas questões relativas à busca de um meio qualquer que, aplicável sobre um documento eletrônico, fosse capaz de suprir as mesmas finalidades exigidas de uma assinatura manuscrita tradicional.

4.4.2 – A Idéia da Assinatura Digitalizada (Visando Autenticidade)

A assinatura digitalizada se refere a uma imagem que reproduz a assinatura escrita de próprio punho de uma pessoa, tal qual ocorre quando se envia um fax de um documento assinado a mão. Assim, um documento do tipo fax, assinado, ao ser recebido por alguém, possuirá uma assinatura digitalizada sobre ele e, não, uma assinatura ou firma digital juridicamente relevante. A assinatura constante de uma imagem de documento, como a utilizada pelo Gerenciamento Eletrônico de Documentos, por si só, não possui valor jurídico. A existência de uma assinatura digitalizada aposta em um determinado documento não possui valor jurídico pelo fato de, por ser uma imagem, ser passível de ser reutilizada infinitas vezes, o que lhe concerne caráter probatório. A reutilização é similar àquela que se poderia obter, manualmente, na hipótese de que uma pessoa efetuasse uma fotocópia de um documento original assinado, recortasse a assinatura presente na cópia e, posteriormente, colasse essa assinatura recortada em um outro documento qualquer. Obviamente, tal colagem seria perceptível de imediato ante a visão de um documento assim fraudado, porém, através de seu envio via fax ou, mesmo, da visão de uma fotocópia sua, tornar-se-iam imperceptíveis os traços da colagem efetuada. A reutilização de uma assinatura digitalizada, através de sua aposição sobre diferentes imagens de documentos eletrônicos, mediante uso do computador para efetuar-se os recortes e colagens necessários, é procedimento extremamente simples de ser realizado. O resultado desse tipo de abordagem manifesta-se sob forma de uma subutilização do enorme potencial de melhoria da eficiência que a informática poderia proporcionar. Porém, a questão principal está em saber separar os fins visados dos meios necessários para conseguí-los. Os meios manuais e os meios computacionais podem e devem ser bem diferentes, sempre que as circunstâncias assim o exigirem, cuidando-se, apenas, que as finalidades visadas, em qualquer caso, sejam integralmente atingidas. Ressalte-se que, normalmente, comparando-se o meio manual com o computacional, na imensa maioria das vezes, o segundo alcança todas as finalidades do primeiro, de forma muito mais eficiente e

rápida e, além disso, acaba abrindo proporcionando novas possibilidades, até então desconsideradas.

A assinatura digitalizada, portanto, não se presta à substituição de uma assinatura tradicional manual e nem supre seus efeitos, como fazem as assinaturas ou firmas eletrônicas. É oportuna a sua abordagem no presente trabalho, com a finalidade de esclarecer as duas formas de “assinatura", as digitalizadas e as eletrônicas, de nome parecido, mas de resultados e possibilidades diferentes. Em seguida, ainda dentro dessa descrição de meios inicialmente pensados para dotar os documentos eletrônicos de validade jurídica, será introduzida a idéia do uso de firmas biométricas.

4.4.3 – Uso de Firmas Biométricas (Visando Autenticidade)

As firmas biométricas identificam seres humanos pelas partes de seu corpo, tais como a impressão digital e a íris dos olhos (GANDINI).

Há muito, sabe-se que tais conformações são exclusivas para cada pessoa, tanto que um indivíduo pode ter um fato criminoso qualquer imputado contra si e, dentre o conjunto de elementos probatórios, ser validamente utilizada sua impressão digital colhida no próprio local do crime. Portanto, a firma biométrica é exclusiva e reconhecível (imputável a uma e somente uma determinada pessoa). Mas, para haver uso de tais firmas biométricas na obtenção de documentos eletrônicos juridicamente válidos, haveria necessidade do preenchimento dos já citados requisitos essenciais de uma assinatura. O que se verifica, na prática, é que tais firmas biométricas não são capazes de satisfazê-los, pois, apesar de serem capazes de identificar perfeitamente o indivíduo que a originou e de, presumivelmente somente poder ser utilizada por ele, não apresenta nenhuma vinculação com o conteúdo do documento eletrônico no qual esteja presente. Isso significa que, uma vez aposto uma firma biométrica sobre um determinado documento eletrônico, poderão, posteriormente, ser efetuadas quaisquer alterações em seu conteúdo sem que isso implique em alteração da firma biométrica. A firma biométrica supri o requisito da autenticidade, por estar relacionada exclusivamente relacionada a determinada pessoa e o suporte informático WORM o da integridade.,

porém, mesmo com a integração desses dois métodos não se teria um documento eletrônico com eficácia probatória. O critério não atendido é a reutilizabilidade, a duplicidade da firma biométrica não pode ser detectada, pois não apresenta vínculo direto com o conteúdo do documento. Pode-se comparar a firma biométrica, num certo sentido, com a chave secreta utilizada pela criptografia simétrica (criptografia tradicional, de chave única). Quem tiver conhecimento de qualquer uma das duas, terá meios para produzir um documento "assinado". Ocorre que, posteriormente, tal assinatura não poderá ser imputada de forma exclusiva a ninguém (isto é, não se pode saber, com certeza, quem foi que produziu a "assinatura" sobre o documento, dentre os muitos que, eventualmente, soubessem como fazê-lo). Assim, vê-se que a firma biométrica é uma firma eletrônica que, a princípio, não se mostra capaz de resultar numa obtenção de validade jurídica para os documentos eletrônicos

4.4.4 – Uso de Espécies de Senhas *(PIN*s, *Passwords* e *Passphrase*s)

Cabe um breve comentário a respeito de algumas formas análogas entre si e, muitas vezes, também identificadas como sendo "firmas (ou assinaturas) eletrônicas": i) PIN *(Personal Identification Number* ou número de identificação pessoal); ii) *password* (palavra de passagem ou de aprovação, num sentido literal) e iii) *passphrase* (frase de passagem ou de aprovação, num sentido literal).

A forma de *passphrase* está sendo introduzida atualmente em algumas atividades como o acesso à conta bancária via Internet, as formas de PIN e *password* são as mais utilizadas nos dias atuais, podemos citar como exemplo: os terminais de caixas bancários automáticos, fechaduras eletrônicas, acionamento de alarmes, acesso à Internet através do provedor, acesso a determinados computadores, acesso à caixa postal do correio eletrônico, etc.. O uso de PINs, *passwords* ou *passphrases* não produzem resultados muito diferentes das firmas biométricas. Inicialmente, cabe dizer que todas são senhas, no sentido genérico de que possuem função de reconhecimento de seu portador. A diferença básica reside no fato de que um PIN, como o próprio nome já diz, trata-se de um simples número (normalmente, com 4 dígitos ou mais), enquanto que uma *passwor*d, trata-

se de um conjuntos de caracteres alfanuméricos ou apenas numéricos, confundindo-se, nesse último caso, com os PINs. Existe, ainda, a chamada *passphras*e, que é formada por um conjunto de palavras separadas, como uma frase ou como várias *passwords* separadas por espaços em branco. A função básica do uso destas senhas é a de averiguar a legitimidade da pessoa que a usa, para efetuar determinadas atividades restritas somente às pessoas autorizadas.

A diferença entre verificar a identidade de uma pessoa (para fins de legitimidade) e a imputabilidade requerida para os documentos eletrônicos é, antes de tudo, fundamental distinguir entre: verificação da identidade pessoal, que é a correspondência biunívoca entre um sujeito e seus dados identificativos consistentes, na realidade, em uma presunção – que é efetuada pelos mais variados meios (por exemplo, exibição de um documento de reconhecimento, garantia de conhecimento pessoal, etc.) e imputabilidade do documento, que é a verificação do autor de um documento pré-confeccionado, que vem envolto por meio da tradicional verificação da assinatura e da integridade do suporte material. Enquanto no primeiro caso não está sendo efetuado nenhum ato (se vai apenas verificar uma legitimação); no segundo caso se trata de identificar o autor de um ato já efetuado, normalmente a pessoa primeiramente é legitimada e em seguida há verificação da identidade. Tratam-se, evidentemente, de planos de todo diversos. O simples uso e exibição de uma senha não permite certeza de atribuir ao documento eletrônico que dela derive a eficácia probatória de um documento assinado. Isso ainda que, na presença de um acordo contratual específico, possa reconhecer valor jurídico ao resultado da memória de certos computadores eletrônicos, modificáveis por uma pessoa autorizada, mediante a inserção de uma senha (ou PIN) pessoal, como acontece nos serviços de bancos eletrônicos.

4.5 – A "Assinatura" dos Documentos Eletrônicos

No caso de um documento eletrônico, o termo "assinatura" pode ser entendido como um "lacramento" personalizado de seu conteúdo, que visa garantir a integridade e a autenticidade. O ato de "assinar" neste contexto, assume um sentido e um modo de concretização bem diferentes do que sugere o verbo, que remete a

um modo de concretização similar à tradicional forma de subscrição (que é a aposição de uma marca, um sinal, isolado, em determinado local de um documento). A "assinatura" de um documento eletrônico não é posta em um local do documento mas, sim, envolve todo o seu conteúdo e, em função dele, é produzida.

4.5.1 – Autenticação dos Documentos Eletrônicos – A Propriedade da Auto-Certificação

Em termos de documentos tradicionais, viu-se que os requisitos essenciais que fundam sua eficácia probatória possuem a garantia de seu suprimento, eminentemente, a cargo do suporte material. No caso dos documentos eletrônicos, por outro lado, a verificação do cumprimento dos requisitos essenciais não se prenderá ao suporte (continente), e sim ao seu próprio conteúdo, que deve ser uma das bases da criação de uma firma eletrônica. Essa independência entre suporte e conteúdo, só é possível mediante o uso de algumas técnicas e tecnologias atualmente existentes, as quais, se aplicadas a um documento eletrônico comum, serão capazes de lhe conferir características extras, aptas a lhe dotarem de capacidade para satisfação dos requisitos exigíveis de uma prova documental plena de eficácia. Daí a necessidade de se instituir formas juridicamente tuteladas de "autenticação" dos documentos eletrônicos. Entenda-se o ato de "autenticar" (ou "certificar") um documento eletrônico como sendo um procedimento tendente a permitir que a proveniência subjetiva, a integridade de seu conteúdo e a sua tempestividade (data de elaboração contemporâneo com o fato registrado) sejam confirmados como seguros e confiáveis. Em relação aos documentos tradicionais, as formas de autenticação baseiam-se em características materializadas no suporte (não no próprio conteúdo, como é o caso dos documentos eletrônicos), tais como a aposição de assinaturas e marcas, o uso de produtos de segurança (papéis e tintas especiais, por exemplo), a feitura de perícias grafológicas e técnicas, etc. No caso dos documentos eletrônicos, a autenticação será efetuada somente com base no conteúdo (desprezando-se o suporte), através de meios adequados a esse tipo específico de documento e, portanto, de filosofia bem diversa dos meios citados, usados para autenticar documentos tradicionais. Apesar dessa diferença de meios, a

autenticação, em ambos os casos, busca atingir os mesmos resultados, ou seja, aferir o cumprimento de requisitos essenciais para a obtenção da eficácia probatória.

Cabe ressaltar que, um documento com firma digital tem um conteúdo completamente desvinculado de seu suporte e garante a integridade e autenticidade do documento eletrônico baseado somente em *software*[α], sem requerer auxílio de *hardware*[β]. Sobre a questão da autenticação dos documentos eletrônicos ser feita, somente, mediante verificação de conteúdo, o que retira do suporte toda a sua anterior importância.

Chega-se ao aspecto mais importante da 'revolução digital', de um ponto de vista mais cultural do que eminentemente jurídico: o novo conceito de 'documento', que prescinde da natureza e, até mais do que isso, da própria existência do suporte. A bem da verdade, no documento tradicional o que vem certificado não é a informação, mas sim o suporte que a contém, Firmas, timbres, filigranas, selos, mesmo a fita metálica inserida no papel-moeda não autenticam a informação, mas sim o suporte. A autenticidade do conteúdo é dada através de sua inseparabilidade do continente. Ora, o conteúdo digital é perfeitamente separável do seu continente e a autenticação refere-se ao conteúdo em si, podendo sem qualquer problema haver a separação sem qualquer perda de eficácia. A existência de uma forma de autenticação efetuada, somente, com base no conteúdo de um documento, confere a este uma inédita independência em relação ao suporte que o contém. Essa propriedade que o documento eletrônico apresenta – de possuir um conteúdo verdadeiramente auto-certificável –, faz com que, entre outras coisas, havendo sua duplicação (no sentido de clonagem e não de cópia, conforme já explicado), tudo o que seja necessário verificar-se, para obtenção de uma autenticação positiva, seja igualmente duplicado. Daí afirmar que, em termos de documentos eletrônicos, não existe diferenciação entre "cópia" e "original", pois todas as duplicações resultam em

---

[α] Refere-se a todos os elementos de programação de um sistema de computação, isto é, sejam de aplicação ou básico do sistema.

[β] Conjunto de equipamentos eletrônicos que compõe um computador, incluindo seus periféricos, como o vídeo, o teclado, a impressora, etc..

novos originais, sempre portadores de idêntica propriedade de auto-certificação (capacidade de serem autenticados).

4.5.2 – Exclusividade de Uso do Meio Técnico

Em qualquer caso descrito até aqui, seja no uso de senhas ou de firmas biométricas, seja no uso da criptografia simétrica (de chave secreta), observa-se um detalhe importante: o conhecimento do segredo envolvido não é de uma só pessoa. No caso das senhas e firmas biométricas, o sistema de verificação tem que ter conhecimento do código secreto de cada pessoa (em qualquer caso, seja da firma biométrica, do PIN, do *password* ou da *passphras*e), com a finalidade de comparação, a ser feita sempre que esta pessoa faça uso prático de seu código de acesso. No caso da chave secreta da criptografia simétrica, todas as partes envolvidas deverão conhecer o segredo, o qual, portanto, não é exclusivo de cada pessoa, passando a ser um segredo coletivo. Isso torna todos inseguros para o desempenho das tarefas esperadas de uma firma eletrônica, pois não existe a "exclusividade de uso do meio técnico", no sentido de que mais de uma pessoa tem o conhecimento do código necessário à produção do que seria a "firma". Em outras palavras, do mesmo modo que uma assinatura manuscrita verdadeira somente pode ser aquela aposta pelo seu titular (pelas suas características próprias de ser autógrafa), uma firma eletrônica também somente deve poder ser produzida, sobre um documento eletrônico, por seu titular. Esse efeito é conseguido através da atribuição, a cada titular, de um severo dever legal de guarda do segredo de produção da firma, sob pena de responsabilidade.

Fazendo uma reflexão pertinente, ao abordar o uso da firma digital (ou seja, enfocando, especificamente, o uso das chaves pública e privada da criptografia assimétrica): neste sistema (criptografia assimétrica), o próprio usuário cria o par de chaves e somente a ele compete manter em sigilo a chave privada. Criador e operador, então, se confundem na mesma pessoa do próprio titular da chave. E terceiros, para conferir a assinatura, só se utilizam chave pública, sem jamais terem acesso à chave privada. Isto encerra uma vantagem e uma desvantagem. A vantagem é que ninguém mais tem acesso à sua chave privada. Só este fato permite

perceber que a criptografia de chave pública chega a ser mais segura do que o mais desenvolvido dos sistemas, em que, em algum lugar, por mais protegida que esteja, a senha do usuário está cadastrada. A desvantagem é que não teremos a quem culpar, pela eventual negligência em manter a chave privada segura, já que a apropriação indevida desta chave pode ser considerado o maior risco que afeta a segurança do sistema. Diria, então, como importante recomendação, que toda a cautela possível deve ser tomada na proteção da chave privada pelo seu titular.

4.6 – Abordagem Interpretativa

A finalidade do presente sub-tópico é a de registrar sucintamente as argumentações utilizadas por alguns autores, na defesa da tese de que os documentos eletrônicos, no Brasil de hoje, mesmo sem a edição de quaisquer normas específicas reguladoras da matéria, seriam perfeitamente utilizáveis como prova documental. Observe-se, contudo, que, mesmo tais autores, entendem não ser possível o uso desses "hermenêuticos"[δ] documentos eletrônicos para determinados fins, justamente, por falta de normas legais específicas que assim os prevejam. Registre-se, ainda, que não se pretende, neste momento, adotar esta ou aquela posição, pois as conclusões do presente estudo serão expostas no momento oportuno (nas considerações finais).

Com o intuito de legitimar o documento eletrônico como espécie de prova, isto é, meio probatório, segundo Lima Neto, do disposto no art. 332 do Digesto Processual Civil[∝] – "*Todos os meios legais, bem como moralmente legítimos, ainda que não especificados neste código, são hábeis para provar a verdade dos fatos, em que se funda a ação ou defesa*.", pode-se interpretar que ao dar tamanha amplitude, o legislador fê-lo deixando claro que o elenco probatório que a lei processual especifica é, apenas, exemplificativo e não exaustivo. Não é essencial portanto, que o meio de prova que a parte deseja produzir esteja catalogado no Código. O que é necessário é que ele não esteja maculado por qualquer eiva de ilicitude.

[δ] Interpretação dos sentidos das palavras. Interpretação dos textos sagrados. Arte de interpretar leis.

[∝] Código de Processo Civil (Anexo VI).

Completa-se a interpretação do artigo acima citado, pode-se dizer que a finalidade processual da prova é convencer o Juiz. Além das qualidades humanas, que tem ele, ou de inteligência, de reflexão, de raciocínio, o Estado, que o fez seu órgão, lhe impõe certas regras de convicção a que tem de obedecer, regras que vão de máximo (sistema da livre convicção do Juiz) até o mínimo de liberdade (sistema da taxação da prova). Sempre que o legislador enfrenta o problema dos meios de prova, o que desafia é o balanceamento do que deve fixar e do que há de deixar ao elemento lógico e científico.(MIRANDA *apud* NETO, s/a)

Cabe aqui citar, devido a liberdade probatória (art. 332 CPC), o princípio do livre convencimento motivado, insculpido na redação do artigo 131 do Código de Processo Civil onde: "*O juiz apreciará a prova livremente, atendendo aos fatos e circunstâncias constantes dos autos, ainda que não alegados pelas partes; mas deverá indicar na sentença os motivos que lhe formaram o convencimento*.", isto demonstra que o raciocínio do julgador haverá de julgar e formar a consciência a respeito da verdade pesquisada.

Assim, não existem empecilhos para magistrado apreciar, desde que lícita, a prova produzida em meio eletrônico.

Saber que o documento eletrônico serve como prova em um processo é, apenas, uma parte menor da questão jurídica. O fundamental é saber qual é a eficácia probatória desse meio, qual seria a força de convencimento do mesmo. Seguindo a mesma linha de raciocínio até aqui exposta, referindo-se ao problema da eficácia dessa prova, pode-se dizer que nada há a impedir a utilização de documentos eletrônicos, seja como forma para se documentar atos jurídicos, seja como meio de prova a ser produzido em juízo. Evidentemente, além de moralmente legítimo, o meio de prova deve mostrar-se idôneo a permitir o convencimento. Daí, documentos eletrônicos sujeitos a alteração ou a serem 'fabricados' unilateralmente pela parte a quem aproveitam não podem ser dotados de força probante. Este não é o caso, como se viu acima, dos documentos eletrônicos 'assinados' mediante uso da criptografia assimétrica. Sua utilização como meio de prova é, então, perfeitamente possível, em face do sistema jurídico já existente.

O centro da questão está na eficácia probatória e, não, na admissão do documento eletrônico como meio de prova. Entendemos, também, que a validade do

documento eletrônico em si não deve ser questionada. Ora, se um contrato verbal é admitido como válido desde 1916, o contrato realizado em meio eletrônico por maior razão deverá ser considerado como válido. O grande problema com que nos deparamos se relaciona à eficácia do 'documento eletrônico', mas especificamente à eficácia probatória.

Fundamentada a admissão do documento eletrônico como meio de prova, trata-se de cuidar de seu uso, na prática, e da eficácia probatória concreta que ele poderia possuir, do que dispõem as normas atuais pertinentes à prova documental. Importante observar que, no cotidiano processual, é na questão da forma de uma prova documental que se centram a maioria das contestações feitas. Nesse sentido, pode-se dizer que, embora a lei seja flexível quanto ao reconhecimento de documentos, qualquer parte em um processo que possa vir a sofrer alguma penalidade em conseqüência de um registro obtido por meios tecnológicos tende a questionar as formas técnicas de produção do documento.

Fica claro, afastando o critério de interpretação literal e restritivo, fundado sobretudo nos dispostos nos arts. 368 e 369 do Código de Processo Civil onde: "*As declarações constantes do documento particular, escrito e assinado, ou somente assinado, presumem-se verdadeiras em relação ao signatário*", "*Cessa a fé do documento particular quando: I - omissis; II - assinado em branco* ", que a existência e validade do documento eletrônico em si não pode ser recusada. Não há qualquer razão que imponha tal raciocínio, e, pelo contrário, usando-se a interpretação sistemática do art. 383 onde: "*qualquer reprodução mecânica, como a fotográfica, cinematográfica, fonográfica, faz prova dos fatos representados, se aquele contra quem foi produzida lhe admitir a conformidade*", chega-se a reafirmação de que o produto de uma relação informatizada, tido como *documen*to pode ser aceito como prova legal, ainda que, para tanto deva preencher certos requisitos.

Pode-se aplicar ao documento eletrônico, mediante a hermenêutica, as disposições do Código de Processo Civil a respeito da prova documental e é perfeitamente possível enquadrar o documento eletrônico na teoria e disposições legais relativas à prova documental. Assim, um documento eletrônico pode ser usado como prova de atos e fatos jurídicos, todavia, algumas cautelas ou formalidades a mais haverão de ser tomadas, enquanto não houver disposição legal

acerca do uso e validade das assinaturas digitais. E, por outro lado, é forçoso admitir que o documento eletrônico não poderá ser *sempre* utilizado em substituição ao documento cartáceo, na falta de alguma regulamentação estatal.

Há que se dizer que na hipótese de uso somente na vigência das normas atuais sobre a prova documental, por ser a forma o documento eletrônico algo recente, certamente muitas questões seriam levantadas com base nesses fatores. Aqui, a falta de normas específicas apresenta, talvez, a sua principal deficiência: a inexistência de um modelo aceito, de um padrão a ser seguido e, consequentemente, a falta da afirmação legal de que se trata de um documento reconhecido e seguro. Sem esses fatores norteadores fornecido pelo legislador e fundado em amplos estudos prévios supostamente efetuados, ficaria a cargo da própria pessoa, que iria formar o documento eletrônico, a determinação de quais seriam os cuidados necessários a se tomar. Não sendo o assunto um tema muito simples, dependendo de tecnologias e técnicas específicas, pode-se dizer que, na maioria das vezes, o documento produzido conteria defeitos, os quais acabariam por afetá-lo em sua inteireza probatória. Com isso, certamente repetir-se-iam os insucessos desse meio de prova em juízo, o que acabaria por trazer desconfiança acerca do próprio meio de documentação em si, fazendo com que os documentos eletrônicos acabassem tendo uso muito mais restrito do que o devido. Finalmente, pode-se dizer que para determinados fins, na falta de normas legais permissivas, seria impossível o uso dos documentos eletrônicos de forma juridicamente válida. Um bom exemplo encontra-se em seu uso oficial, no âmbito da Administração Pública, em virtude, principalmente, do princípio da legalidade que rege seus atos. Observe-se, contudo, que não se está tratando só dos meros atos administrativos internos do Poder Público, quando se fala em "uso oficial no âmbito da Administração Pública". O que se quer significar, isso sim, é o uso dos documentos eletrônicos na produção de documentos externos, fornecidos aos particulares, de modo geral (como, por exemplo, a substituição de uma certidão assinada qualquer, por uma certidão eletrônica com idêntico poder probatório).

As dificuldades que se encontram na plena equiparação do documento eletrônico ao documento tradicional residem na falta de alguma regulamentação, seja legislativa, seja meramente administrativa, de seu uso e aceitação por parte de

entes públicos. Assim, atos notariais como a elaboração de instrumentos públicos em forma eletrônica, a autenticação de cópias físicas de documentos eletrônicos – ou vice-versa –, o *'reconhecimento*' das chaves públicas, a certificação da data dos documentos eletrônicos, ou outras participações possíveis que o tabelião possa ter na formação ou comprovação de documentos digitais dependerão de algum tipo de regulamentação, senão legislativa, ao menos administrativa.

Alguns aspectos e orientações para serem tomadas como referência sobre a regulamentação da assinatura digital e comércio eletrônico, se encontram na lei modelo da UNCITRAL[ε], que busca regulamentar a Internet, equiparando a assinatura digital àquela convencionalmente aposta em um suporte físico. Em respeito a todas as funções que o documento aposto em papel proporciona, a Lei modelo da UNCITRAL estabelece que os registros eletrônicos, para que recebam o mesmo nível de reconhecimento legal, devem satisfazer, no mínimo, o mesmo grau de segurança que os documentos em papel oferecem, o que deve ser alcançado por uma série de recursos técnicos.

[ε] *United Nations Commission on International Trade Law* - Lei Modelo sobre Comércio Eletrônico aprovada pela Comissão das Nações Unidas para o Direito Comercial Internacional.

CONCLUSÃO

Decorrente do aumento da quantidade de documentos apostos em papel gerado no mundo do negócio da sociedade da informação, tem-se como consequência a necessidade do gerenciamento eficiente das informações contidas nestes documentos. Para agilizar este processo, atualmente existe a tecnologia do GED – Gerenciamento Eletrônico de Documentos, cujo elemento principal é o documento eletrônico.

Hoje, se vivencia uma ampla discussão sobre a equiparação do documento eletrônico com o documento aposto em papel, com o intuito de poder usufruir e utilizar-se de todo seu benefício, uma vez que, suas diferenças básicas estão somente em suas formas de materialização e não na informação armazenada, informação esta que representa o interesse das partes envolvidas.

Pode-se citar a assinatura digital como um avanço tecnológico que visa aumentar a segurança dos documentos eletrônicos, garantindo sua integridade, autenticidade e tempestividade. Para os estudiosos e conhecedores da tecnologia, o método de criptografia assimétrica e certificação digital é um modelo de técnica de excelência que garante os requisitos básicos da validade jurídica dos documentos eletrônicos. Porém, pelo fato da sociedade se basear em parâmetros para nortear suas relações com outrem, como por exemplo o amparo legal, as mudanças sociais, novas tecnologias e consequentemente novas relações ou fatos jurídicos, devem ser seguidas por regulamentação das leis.

No Brasil, foi instituída a Medida Provisória 2200, sobre a Infra-Estrutura de Chaves Públicas Brasileira, a ICP-Brasil, para garantir a autenticidade e integridade de documentos eletrônicos utilizando a criptografia, porém, nem todos seus requisitos estão concluídos.

Embora por enquanto não exista um Diploma Legal específico para a validação e eficácia probatória do documento eletrônico, ficando a mercê dos juristas avaliar a apreciação da prova, é incontestável que um documento eletrônico sirva como meio legal de prova.

Compete ao meio legislativo regular as relações entre indivíduos dando-lhes segurança e estabilidade nas relações jurídicas que os mesmos estabelecem, não deixando subutilizar novas evoluções em virtude de entendimentos inflexíveis de antigos dogmas jurídicos.

Crenças e paradigmas de que o documento eletrônico nada mais é que uma imagem digitalizada sem valor jurídico devem ser substituídos pela idéia concreta de sinônimo de progressão social e inovações benéficas que visam à comodidade e facilidade da sociedade.

Finalizando este trabalho, é preciso enfatizar a necessidade de maiores estudos e debates acerca do tema da presente pesquisa, que se apresenta vasta e possuidora de muitas lacunas. A troca de idéias é fundamental para a conformação de uma base para sistematização, somente assim é que se poderá formar um conhecimento adequado, capaz de produzir normas e procedimentos que popularizarão o uso dos documentos eletrônicos com validade jurídica.

É evidente que o documento aposto em papel já não condiz com a agilidade exigida pela sociedade atual, portanto, não há dúvida que em virtude das inúmeras vantagens que o documento eletrônico pode apresentar em relação ao documento aposto em papel haverá uma mudança, mais que uma mera concessão ao conforto ou a uma efêmera modernidade, será uma mudança de imperativa necessidade.

Até que as leis sobre a validade jurídica dos documentos eletrônicos não se concretizem, as empresas continuam a consumir papel, a morosidade aumenta, o fluxo de trabalho é prejudicado, e todo o potencial da tecnologia do Gerenciamento Eletrônico de Documentos continua sem atingir seu máximo.

REFERÊNCIAS BIBLIOGRÁFICAS

1) AVEDON, Don M.. *Controle e Certificação da Qualidade no Processamento Eletrônico e imagens de documentos.* CENADEM, São Paulo, 1995.

2) AVEDON, Don M.. *Telecomunicações no Gerenciamento Eletrônico de Documentos.* CENADEM, São Paulo, 1997.

3) CAHALI, Yussef Said (**organizador**). *Código civil - Código de Processo Civil - Constituição Federal.* Editora Revistas dos Tribunais, 4ª Edição, São Paulo, 2002.

4) CASTRO, Aldemario Araujo Castro. *O documento eletrônico e a assinatura digital.* S/A. Disponível em http://www1.jus.com.br/doutrina/texto.asp?id=2632

5) COUTINHO, S.C. *Números Inteiros e Criptografia RSA.* 2ª Edição. IMPA/SBM, Rio de Janeiro, 2000

6) CRUZ, Tadeu. *Workflow: A tecnologia que vai revolucionar processos.* 2ª Edição. Atlas, São Paulo, 2000.

7) DUYSHART, Bruce. *The digital document: A reference for Architects, Engineers and Design Professionals.* Butterworh-Heinemann, New York, 1998.

8) D'ALLEYRAND, Marc. *Workflow em Sistemas de Gerenciamento Eletrônico de Imagens.* CENADEM, São Paulo, 1995.

9) DINIZ, Davi Monteiro. *Documentos Eletrônicos, Assinatura Digital.* Ltr Editora LTDA. São Paulo, 1999.

10) FERREIRA, Aurélio Buarque de Holanda. *Novo dicionário da Língua Portuguesa.* Nova Fronteira. Rio de Janeiro, 1988.

11) FRUSCIONE, James J.. *Automated Workflow Developing General Designs and Support Plans.* Management International, New York, 1994.

12) KOCH, Walter. *Gerenciamento eletrônico de documentos – GED – Conceitos, tecnologias e considerações finais.* São Paulo, 1998.

13) KUBIÇA, Stefano. *Documentos com segurança na Internet.* S/A. Disponível em http://www.pr.gov.br/celepar/celepar/batebyte/edicoes/2001/bb107/documentos.htm

14) MARCACINI, Augusto Tavares Rosa. *O documento eletrônico como meio de prova.* S/A. Disponível em http://advogado.com/internet/zip/tavares.htm

15) MONTEIRO, Mário Antonio. *Introdução à Organização de computadores.* 3ª Edição, Editora Afiliada, Rio de Janeiro, 1996.

16) MURSHED, N. A. (**Editor**) . *Advences in Document Image Analysis: Proceeding, 1st Brazilian Symposium.* Springer-Verlag, New York, 1997.

17) PISTELLI, Daniela. *Criptografia.* S/A. Disponível em http://www.nucc.pucsp.br/novo/cripto/cripto.html.

18) SPRAGUE JR., Ralph H. *Electronic Document Management: Challenges and Opportunities for Information Systems Managers.* Disponível em

http://www.cba.hawaii.edu/sprague/MISQ/MISQfinal.htm. Hawaii, 1995.

19) STARBIRD, Robert W. e VILHAUER, Gerald C. *Como tomar a decisão de implantar a tecnologia de do Gerenciamento Eletrônico de Documentos.* CENADEM, São Paulo, 1997.

20) STRINGHER, Ademar. *Aspectos Legais da Documentação em Meios Micrográficos, Magnéticos e Ópticos*. 2ª Edição. CENADEM, São Paulo, 1996.

21) VOLPI, Marlon Marcelo. *Assinatura Digital – Aspectos técnicos, práticos e legais.* Axcel Books do Brasil Editora, Rio de Janeiro, 2001.

22) WEY,José Daniel Ramos*. Criptografia ao alcance de todos.* S/A. Disponível em http://www.geocities.com/SiliconValley/Campus/6230/cripto.html.

APÊNDICES

Algoritmo RSA

Este algoritmo foi inventado em 1978 por *Ron **R**ivest, Adi **S**hamir* e *Len **A**dleman,* que na época trabalhavam no *Massachussets Institute of Technology (M.I.T.).* As letras RSA correspondem às iniciais dos inventores do código (COUTINHO, 2000:3).

Este algoritmo baseia-se no lema: ”é simples arranjar dois números primos grandes, mas é muito complicado (moroso) fatorizar o seu produto”. O RSA tem sustentado todas as investidas dos cripto-analistas, contudo, por se tratar de problema matemático, existe sempre o risco de descoberta de uma técnica para resolver o problema de forma eficiente.

A geração das chaves é feita seguindo os procedimentos abaixo:

i) escolhem-se dois número primos grandes e aleatórios a e b, com aproximadamente o mesmo tamanho;

ii) calcula-se n = a x b;

iii) calcula-se ø(n) = (a-1) x (b-1);

iv) seleciona-se um número inteiro aleatório p que seja primo relativo de ø(n) e < ø(n), isto é, mdc[δ](p, ø(n)) = 1;

v) calcula-se s tal que (p x s) mod[α] ø(n) = 1 .

[δ] Maior divisor inteiro comum

O par (n, p) constitui a chave pública sendo d a chave secreta.

A cifragem da mensagem original é calculada pela fórmula $C = M^p \bmod n$ e a decifragem da mensagem cifrada é calculada pela fórmula $M = C^s \bmod n$, onde M e C são respectivamente a mensagem original e mensagem cifrada, ambas com valores possíveis de zero a n-1.

Uma propriedade interessante do RSA é a possibilidade de inversão das chaves, pode-se cifrar uma mensagem com a chave s, para decifrar será necessária a chave pública: utilizável para autenticação e assinatura digital.

Por exemplo, os números primos a = 7 e b = 17:

i) n = a x b = 119

ii) ø(n) = (a-1) x (b-1) = 96

iii) como primo relativo de ø(n) pode-se escolher p=5, então para obter p x s mod 96 = 1, podemos usar s = 77 pois 5 x 77 = 385, 385 mod 96 = 1

A chave pública é (5;119) e a chave secreta é 77.

As operações a realizar na decifragem não são simples, especialmente se atendermos a que os números **a** e **b** devem ser grandes.

Para os valores 0 e 1 a medida e o resultado da cifragem coincidem, contudo, isto não é muito grave, os valores usados para n são muito elevados (na ordem de 10^{200}), o tamanho mais comum para as mensagens a cifrar (M) é de 512 bits (que representa números até mais de 10^{154}), para este número de bits não são vulgares os valores 0 e 1, de qualquer modo isto pode ser resolvido pela adição de duas unidades a M antes de entrar no algoritmo de cifragem e subtração de duas unidades depois de sair do algoritmo de decifragem.

Gerar chaves RSA não é uma operação simples, o primeiro problema é arranjar dois números primos **a** e **b** com uma ordem de grandeza de 10^{100}, usar os algoritmos tradicionais de geração de números primos é impossível, a solução é usar testes eliminatórios, estes testes permitem saber se um número não é primo, ou qual a probabilidade de ser primo, se um dado número depois de testado intensivamente não é eliminado será adotado. A segunda questão prende-se com a determinação

---

$^{\alpha}$ operador resto da divisão inteira.

de um primo relativo de ø(n), p ou s e de seguida é necessário determinar outro número para verificar a relação (p x s) mod ø(n) = 1.

Sob o ponto de vista de cripto-análise e devido ao número de bits das chaves a aplicação de força bruta (tentar todas as chaves secretas possíveis) está excluída. A abordagem é tentar obter os dois fatores primos de n. Contudo tal é extremamente complexo para a ordem de grandeza usada para n, o tempo necessário cresce exponencialmente com o valor de n.

Para evitar perdas de dados torna-se necessário aplicar a seguinte propriedade da aritmética modular:(a x b) mod n = ((a mod n) x (b mod n)) mod n.

Visando melhor esclarecimento, um exemplo completo da cifragem e decifragem usando a chave pública (5;119) e a chave secreta 77 calculada acima, será listado a seguir.

Para cifrar o número 2 com a chave pública temos:

$C = 2^5 \bmod 119 = 32 \bmod 119 =$ **32**

Para decifrar utiliza-se $M = \mathbf{32}^{77} \bmod 119$, para usar uma calculadora, sem perder dados podemos usar 11 parcelas:

$((32^7 \bmod 119) \times ... \times (32^7 \bmod 119)) \bmod 119$, obtemos então $25^{11} \bmod 119$, pode-se aplicar $((5^{11} \bmod 119) \times (5^{11} \bmod 119)) \bmod 119$, obtem-se $45^2 \bmod 119 =$ **2**

Também se pode cifrar o número **2** com a chave secreta temos

$C = 2^{77} \bmod 119$, para usar uma calculadora, sem perder dados podemos usar 11 parcelas:

$((2^7 \bmod 119) \times ... \times (2^7 \bmod 119)) \bmod 119 = 9^{11} \bmod 119 =$ **32** Para decifrar utiliza-se $M = \mathbf{32}^5 \bmod 119 =$ **2**

ANEXOS

Resolução 11 – ICP-Brasil

Presidência da República

COMITÊ GESTOR DA ICP-BRASIL

RESOLUÇÃO Nº 11, DE 14 DE FEVEREIRO DE 2002.

Altera os requisitos mínimos para as políticas de certificado na ICP-Brasil, a declaração de práticas de certificação da AC Raiz da ICP-Brasil, delega atribuições para a AC Raiz e dá outras providências.

O SECRETÁRIO-EXECUTIVO DO COMITÊ GESTOR DA INFRA-ESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA - ICP-BRASIL faz saber que aquele Comitê, no uso das atribuições previstas nos incisos I e II e no parágrafo único do art. 4º da Medida Provisória nº 2.200-2, de 24 de agosto de 2001,

R E S O L V E :

Art. 1º Os REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL, aprovados pela Resolução nº 7, de 12 de dezembro de 2001, passam a vigorar com as seguintes alterações:

"1.3.4. Aplicabilidade

Neste item devem ser relacionadas as aplicações para as quais são adequados os certificados definidos pela PC e, quando cabíveis, as aplicações para as quais existam restrições ou proibições para o uso desses certificados.

Aplicações voltadas para atendimento ao público em geral, assim considerados, dentre outros, os consumidores, os contribuintes, os cidadãos, os beneficiários do sistema de saúde, do FGTS, da seguridade social, que aceitarem certificados de um determinado tipo previsto pela ICP-

Brasil, devem aceitar todo e qualquer certificado de mesmo tipo, ou com requisitos de segurança mais rigorosos, emitidos por qualquer AC integrante da ICP-Brasil.

Na definição das aplicações para o certificado definido pela PC, a AC responsável deve levar em conta o nível de segurança previsto para o tipo do certificado. Esse nível de segurança é caracterizado pelos requisitos mínimos definidos para aspectos como: tamanho da chave criptográfica, mídia armazenadora da chave, processo de geração do par de chaves, procedimentos de identificação do titular de certificado, freqüência de emissão da correspondente Lista de Certificados Revogados (LCR) e extensão do período de validade do certificado, apresentados na tabela constante do Anexo I.

Certificados de tipos A1, A2, A3 e A4 serão utilizados em aplicações como confirmação de identidade na Web, correio eletrônico, transações on-line, redes privadas virtuais, transações eletrônicas, informações eletrônicas, cifração de chaves de sessão e assinatura de documentos eletrônicos com verificação da integridade de suas informações.

Certificados de tipos S1, S2, S3 e S4 serão utilizados em aplicações como cifração de documentos, bases de dados, mensagens e outras informações eletrônicas, com a finalidade de garantir o seu sigilo."

"7.1.2. Extensões de certificado

Neste item, a PC deve descrever todas as extensões de certificado utilizadas e sua criticalidade.

A ICP-Brasil define como obrigatórias as seguintes extensões:

- "Authority Key Identifier", não crítica: o campo keyIdentifier deve conter o hash SHA-1 da chave pública da AC;

- "Key Usage", crítica: em certificados de assinatura digital, somente os bits digitalSignature , nonRepudiation e keyEncipherment podem estar ativados; em certificados de sigilo, somente os bits keyEncipherment e dataEncipherment podem estar ativados;

- "Certificate Policies", não crítica: deve conter o OID da PC correspondente e o endereço Web da DPC da AC que emite o certificado;

- "CRL Distribution Points", não crítica: deve conter o endereço na Web onde se obtém a LCR correspondente;

A ICP-Brasil também define como obrigatória a extensão "Subject Alternative Name", não crítica e com os seguintes formatos:

Para certificado de pessoa física, um único campo otherName, contendo:

- OID = 2.16.76.1.3.1 e conteúdo = nas primeiras 8 (oito) posições, a data de nascimento do titular, no formato ddmmaaaa; nas 11 (onze) posições subseqüentes, o Cadastro de Pessoa Física (CPF) do titular; nas 11 (onze) posições subseqüentes, o número de inscrição do titular no PIS/PASEP; nas 11 (onze) posições subseqüentes, o número do Registro Geral (RG) do titular; nas 6 (seis) posições subseqüentes, as siglas do órgão expedidor do RG e respectiva unidade da federação.

Para certificado de pessoa jurídica, 3 (três) campos otherName, contendo, nesta ordem:

- OID = 2.16.76.1.3.4 e conteúdo = nas primeiras 8 (oito) posições, a data de nascimento do responsável pelo certificado, no formato ddmmaaaa; nas 11 (onze) posições subseqüentes, o Cadastro de Pessoa Física (CPF) do responsável; nas 11 (onze) posições subseqüentes, o número de inscrição do responsável no PIS/PASEP; nas 11 (onze) posições subseqüentes, o número do Registro Geral (RG) do responsável; nas 6 (seis) posições subseqüentes, as siglas do órgão expedidor do RG e respectiva unidade da federação;

- OID = 2.16.76.1.3.2 e conteúdo = nome do responsável pelo certificado;

- OID = 2.16.76.1.3.3 e conteúdo = Cadastro Nacional de Pessoa Jurídica (CNPJ) da pessoa jurídica titular do certificado.

Quando o número de CPF, PIS/PASEP, RG ou CNPJ não estiver disponível, o campo correspondente deve ser integralmente preenchido com caracteres "zero".

Campos otherName adicionais, contendo informações específicas definidas pela AC, poderão ser utilizados com OID atribuídos pelo CG da ICP-Brasil.

Os outros campos que compõem a extensão "Subject Alternative Name" poderão ser utilizados, na forma e com os propósitos definidos na RFC 2459."

Art. 2º O item 1.4. da DECLARAÇÃO DE PRÁTICAS DE CERTIFICAÇÃO DA AC RAIZ DA ICP-BRASIL, aprovada pela Resolução nº 1, de 25 de setembro de 2001, passa a vigorar com a seguinte redação:

"1.4. Dados de Contato

Nome: Instituto Nacional de Tecnologia da Informação - ITI

Endereço: Palácio do Planalto, Anexo II - S, Sala 220

Telefone: (550xx61) 4112082

Fax: 2265636

Página Web: http://www.iti.gov.br

E-mail: acraiz@iti.gov.br"

Art. 3º No âmbito da Reestruturação do Sistema de Pagamentos Brasileiro, para os fins do art. 2º da Circular nº 3.060, do Banco Central do Brasil, de 20 de setembro de 2001, o bit dataEncipherment poderá estar ativado também em certificados de assinatura digital, na extensão "Key Usage", definida no item 7.1.2. dos REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL, aprovados pela Resolução nº 7, de 11 de dezembro de 2001, desde que os dados a serem cifrados correspondam, necessariamente, a valores iniciais ou a vetores de inicialização, utilizados nos modos de implementação CBC (cipher block chaining) ou CFB (cipher-feedback mode).

Parágrafo único. Os certificados a que se refere o caput expirarão, no máximo, em 15 de novembro de 2002.

Art. 4º Ficam delegadas à Autoridade Certificadora Raiz - AC Raiz as seguintes atribuições:

I - aprovar políticas de certificados, práticas de certificação e regras operacionais das AC;

II - credenciar e autorizar o funcionamento das AC, das AR, e de seus prestadores de serviços de suporte, bem como autorizar a emissão do correspondente certificado; e

III - as tarefas atribuídas ao Comitê Gestor da ICP-Brasil e à sua Secretaria-Executiva nos CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL, aprovados pela Resolução nº 6, de 22 de novembro de 2001.

Parágrafo único. Fica, a título de recomendação, a cargo da AC Raiz dar início às atividades de identificação e avaliação das políticas de ICP externas, bem como de negociação de acordos de certificação bilateral, de certificação cruzada, regras de interoperabilidade e outras formas de cooperação internacional, observado o disposto em tratados, acordos ou atos internacionais.

Art. 4º Esta Resolução entra em vigor na data de sua publicação.

MURILO MARQUES BARBOZA

Resolução 12 – ICP-Brasil

Presidência da República

COMITÊ GESTOR DA ICP-BRASIL

RESOLUÇÃO Nº 12, DE 14 DE FEVEREIRO DE 2002.

Estabelece regras processuais para credenciamento na ICP-Brasil.

O SECRETÁRIO-EXECUTIVO DO COMITÊ GESTOR DA INFRA-ESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA - ICP-BRASIL faz saber que aquele Comitê, no uso das atribuições previstas no inciso II do art. 4o da Medida Provisória no 2.200-2, de 24 de agosto de 2001, **R E S O L V E :**

Art. 1º A solicitação de credenciamento será protocolada perante o protocolo-geral da Presidência da República e recebida, em até trinta dias, pela AC Raiz, por intermédio de despacho fundamentado.

Parágrafo único. Caso a solicitação de credenciamento não contenha todos os documentos exigidos nos CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL, aprovados na Resolução no 6, de 22 de novembro de 2001, a AC Raiz poderá determinar a intimação da candidata para que, no prazo máximo de dez dias, supra as irregularidades, sob pena de arquivamento do processo.

Art. 2º O despacho de recebimento a que se refere o artigo anterior determinará a realização das diligências de auditoria e fiscalização pelo prazo que estabelecer.

Parágrafo único. Durante as diligências de auditoria e fiscalização, a AC Raiz poderá exigir documentação adicional contendo especificações sobre equipamentos, produtos de hardware e software, procedimentos técnicos e operacionais adotados pela candidata.

Art. 3º Caso o relatório de auditoria e fiscalização aponte o não-cumprimento de quaisquer dos critérios para credenciamento exigidos pelo item 2.1. dos CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL, aprovados na Resolução no 6, de 22 de novembro de 2001, a AC Raiz intimará a candidata para que os cumpra no prazo que fixar.

Parágrafo único. Após a comunicação da candidata de que atendeu os critérios de credenciamento

apontados como não cumpridos no relatório de auditoria e fiscalização, a AC Raiz realizará auditoria complementar de modo a verificar as medidas adotadas.

Art. 4º Apresentado o relatório final de auditoria e fiscalização, a AC Raiz manifestar-se-á sobre o deferimento ou indeferimento da solicitação de credenciamento.

Art. 5º Esta Resolução entra em vigor na data de sua publicação.

MURILO MARQUES BARBOZA

Medida Provisória Nº 2200-2

Presidência da República

Casa Civil

Subchefia para Assuntos Jurídicos

MEDIDA PROVISÓRIA Nº 2.200-2, DE 24 DE AGOSTO DE 2001.

Institui a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências.

O PRESIDENTE DA REPÚBLICA, no uso da atribuição que lhe confere o art. 62 da Constituição, adota a seguinte Medida Provisória, com força de lei:

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.

Art. 2º A ICP-Brasil, cuja organização será definida em regulamento, será composta por uma autoridade gestora de políticas e pela cadeia de autoridades certificadoras composta pela Autoridade Certificadora Raiz - AC Raiz, pelas Autoridades Certificadoras - AC e pelas Autoridades de Registro - AR.

Art. 3º A função de autoridade gestora de políticas será exercida pelo Comitê Gestor da ICP-Brasil, vinculado à Casa Civil da Presidência da República e composto por cinco representantes da sociedade civil, integrantes de setores interessados, designados pelo Presidente da República, e um representante de cada um dos seguintes órgãos, indicados por seus titulares:

I - Ministério da Justiça;

II - Ministério da Fazenda;

III - Ministério do Desenvolvimento, Indústria e Comércio Exterior;

IV - Ministério do Planejamento, Orçamento e Gestão;

V - Ministério da Ciência e Tecnologia;

VI - Casa Civil da Presidência da República; e

VII - Gabinete de Segurança Institucional da Presidência da República.

§ 1º A coordenação do Comitê Gestor da ICP-Brasil será exercida pelo representante da Casa Civil da Presidência da República.

§ 2º Os representantes da sociedade civil serão designados para períodos de dois anos, permitida a recondução.

§ 3º A participação no Comitê Gestor da ICP-Brasil é de relevante interesse público e não será remunerada.

§ 4º O Comitê Gestor da ICP-Brasil terá uma Secretaria-Executiva, na forma do regulamento.

Art. 4º Compete ao Comitê Gestor da ICP-Brasil:

I - adotar as medidas necessárias e coordenar a implantação e o funcionamento da ICP-Brasil;

II - estabelecer a política, os critérios e as normas técnicas para o credenciamento das AC, das AR e dos demais prestadores de serviço de suporte à ICP-Brasil, em todos os níveis da cadeia de certificação;

III - estabelecer a política de certificação e as regras operacionais da AC Raiz;

IV - homologar, auditar e fiscalizar a AC Raiz e os seus prestadores de serviço;

V - estabelecer diretrizes e normas técnicas para a formulação de políticas de certificados e regras operacionais das AC e das AR e definir níveis da cadeia de certificação;

VI - aprovar políticas de certificados, práticas de certificação e regras operacionais, credenciar e autorizar o funcionamento das AC e das AR, bem como autorizar a AC Raiz a emitir o correspondente certificado;

VII - identificar e avaliar as políticas de ICP externas, negociar e aprovar acordos de certificação bilateral, de certificação cruzada, regras de interoperabilidade e outras formas de cooperação internacional, certificar, quando for o caso, sua compatibilidade com a ICP-Brasil, observado o disposto em tratados, acordos ou atos internacionais; e

VIII - atualizar, ajustar e revisar os procedimentos e as práticas estabelecidas para a ICP-Brasil, garantir sua compatibilidade e promover a atualização tecnológica do sistema e a sua conformidade com as políticas de segurança.

Parágrafo único. O Comitê Gestor poderá delegar atribuições à AC Raiz.

Art. 5º À AC Raiz, primeira autoridade da cadeia de certificação, executora das Políticas de Certificados e normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil, compete emitir, expedir, distribuir, revogar e gerenciar os certificados das AC de nível imediatamente subseqüente ao seu, gerenciar a lista de certificados emitidos, revogados e vencidos, e executar atividades de fiscalização e auditoria das AC e das AR e dos prestadores de serviço habilitados na ICP, em conformidade com as diretrizes e normas técnicas estabelecidas pelo Comitê Gestor da ICP-Brasil, e exercer outras atribuições que lhe forem cometidas pela autoridade gestora de políticas.

Parágrafo único. É vedado à AC Raiz emitir certificados para o usuário final.

Art. 6º Às AC, entidades credenciadas a emitir certificados digitais vinculando pares de chaves criptográficas ao respectivo titular, compete emitir, expedir, distribuir, revogar e gerenciar os certificados, bem como colocar à disposição dos usuários listas de certificados revogados e outras informações pertinentes e manter registro de suas operações.

Parágrafo único. O par de chaves criptográficas será gerado sempre pelo próprio titular e sua chave privada de assinatura será de seu exclusivo controle, uso e conhecimento.

Art. 7º Às AR, entidades operacionalmente vinculadas a determinada AC, compete identificar e cadastrar usuários na presença destes, encaminhar solicitações de certificados às AC e manter registros de suas operações.

Art. 8º Observados os critérios a serem estabelecidos pelo Comitê Gestor da ICP-Brasil, poderão ser credenciados como AC e AR os órgãos e as entidades públicos e as pessoas jurídicas de direito privado.

Art. 9º É vedado a qualquer AC certificar nível diverso do imediatamente subseqüente ao seu, exceto nos casos de acordos de certificação lateral ou cruzada, previamente aprovados pelo Comitê Gestor da ICP-Brasil.

Art. 10. Consideram-se documentos públicos ou particulares, para todos os fins legais, os documentos eletrônicos de que trata esta Medida Provisória.

§ 1º As declarações constantes dos documentos em forma eletrônica produzidos com a utilização de processo de certificação disponibilizado pela ICP-Brasil presumem-se verdadeiros em relação aos signatários, na forma do art. 131 da Lei nº 3.071, de 1º de janeiro de 1916 - Código Civil.

§ 2º O disposto nesta Medida Provisória não obsta a utilização de outro meio de comprovação da autoria e integridade de documentos em forma eletrônica, inclusive os que utilizem certificados não emitidos pela ICP-Brasil, desde que admitido pelas partes como válido ou aceito pela pessoa a quem for oposto o documento.

Art. 11. A utilização de documento eletrônico para fins tributários atenderá, ainda, ao disposto no art. 100 da Lei nº 5.172, de 25 de outubro de 1966 - Código Tributário Nacional.

Art. 12. Fica transformado em autarquia federal, vinculada ao Ministério da Ciência e Tecnologia, o Instituto Nacional de Tecnologia da Informação - ITI, com sede e foro no Distrito Federal.

Art. 13. O ITI é a Autoridade Certificadora Raiz da Infra-Estrutura de Chaves Públicas Brasileira.

Art. 14. No exercício de suas atribuições, o ITI desempenhará atividade de fiscalização, podendo ainda aplicar sanções e penalidades, na forma da lei.

Art. 15. Integrarão a estrutura básica do ITI uma Presidência, uma Diretoria de Tecnologia da Informação, uma Diretoria de Infra-Estrutura de Chaves Públicas e uma Procuradoria-Geral.

Parágrafo único. A Diretoria de Tecnologia da Informação poderá ser estabelecida na cidade de Campinas, no Estado de São Paulo.

Art. 16. Para a consecução dos seus objetivos, o ITI poderá, na forma da lei, contratar serviços de terceiros.

§ 1º O Diretor-Presidente do ITI poderá requisitar, para ter exercício exclusivo na Diretoria de Infra-Estrutura de Chaves Públicas, por período não superior a um ano, servidores, civis ou militares, e empregados de órgãos e entidades integrantes da Administração Pública Federal direta ou indireta, quaisquer que sejam as funções a serem exercidas.

§ 2º Aos requisitados nos termos deste artigo serão assegurados todos os direitos e vantagens a que façam jus no órgão ou na entidade de origem, considerando-se o período de requisição para todos os efeitos da vida funcional, como efetivo exercício no cargo, posto, graduação ou emprego que ocupe no órgão ou na entidade de origem.

Art. 17. Fica o Poder Executivo autorizado a transferir para o ITI:

I - os acervos técnico e patrimonial, as obrigações e os direitos do Instituto Nacional de Tecnologia da Informação do Ministério da Ciência e Tecnologia;

II - remanejar, transpor, transferir, ou utilizar, as dotações orçamentárias aprovadas na Lei Orçamentária de 2001, consignadas ao Ministério da Ciência e Tecnologia, referentes às atribuições do órgão ora transformado, mantida a mesma classificação orçamentária, expressa por categoria de programação em seu menor nível, observado o disposto no § 2º do art. 3º da Lei nº 9.995, de 25 de julho de 2000, assim como o respectivo detalhamento por esfera orçamentária, grupos de despesa, fontes de recursos, modalidades de aplicação e identificadores de uso.

Art. 18. Enquanto não for implantada a sua Procuradoria Geral, o ITI será representado em juízo pela Advocacia Geral da União.

Art. 19. Ficam convalidados os atos praticados com base na Medida Provisória nº 2.200-1, de 27 de julho de 2001.

Art. 20. Esta Medida Provisória entra em vigor na data de sua publicação.

Brasília, 24 de agosto de 2001; 180º da Independência e 113º da República.

FERNANDO HENRIQUE CARDOSO
José Gregori
Martus Tavares
Ronaldo Mota Sardenberg
Pedro Parente

Este texto não substitui o publicado no D.O.U. de 27.8.2001

Decreto Nº 3996

Presidência da República

Casa Civil

Subchefia para Assuntos Jurídicos

DECRETO Nº 3.996, DE 31 DE OUTUBRO DE 2001.

Dispõe sobre a prestação de serviços de certificação digital no âmbito da Administração Pública Federal.

O VICE-PRESIDENTE DA REPÚBLICA, no exercício do cargo de Presidente da República, usando das atribuições que lhe confere o art. 84, incisos II, IV e VI, alínea "a", da Constituição, e tendo em vista o disposto na Medida Provisória nº 2.200-2, de 24 de agosto de 2001,

DECRETA:

Art. 1º A prestação de serviços de certificação digital no âmbito da Administração Pública Federal, direta e indireta, fica regulada por este Decreto.

Art. 2º Somente mediante prévia autorização do Comitê Executivo do Governo Eletrônico, os órgãos e as entidades da Administração Pública Federal poderão prestar ou contratar serviços de certificação digital.

§ 1º Os serviços de certificação digital a serem prestados, credenciados ou contratados pelos órgãos e entidades integrantes da Administração Pública Federal deverão ser providos no âmbito da Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil.

§ 2º Respeitado o disposto no § 1º, o Comitê Executivo do Governo Eletrônico poderá estabelecer padrões e requisitos administrativos para a instalação de Autoridades Certificadoras - AC e de Autoridades de Registro – AR próprias na esfera da Administração Pública Federal.

§ 3º As AR de que trata o § 2º serão, preferencialmente, os órgãos integrantes do Sistema de Administração do Pessoal Civil - SIPEC.

Art. 3º A tramitação de documentos eletrônicos para os quais seja necessária ou exigida a utilização de certificados digitais somente se fará mediante certificação disponibilizada por AC integrante da ICP-Brasil.

Art. 4º Será atribuída, na Administração Pública Federal, aos diferentes tipos de certificados disponibilizados pela ICP-Brasil, a classificação de informações segundo o estabelecido na legislação específica.

Art. 5º Este Decreto entra em vigor na data de sua publicação.

Art. 6º Fica revogado o Decreto nº 3.587, de 5 de setembro de 2000.

Brasília, 31 de outubro de 2001; 180º da Independência e 113º da República.

MARCO ANTONIO DE OLIVEIRA MACIEL

Martus Tavares

Silvano Gianni

Este texto não substitui o publicado no D.O.U. 5.11.2001

Projeto de Lei Nº 2.664

DOCUMENTO ELETRÔNICO

PROJETOS DE LEI

PROJETO DE LEI Nº 2.644, DE 1996.

Dispõe sobre a elaboração, o arquivamento e o uso de documentos eletrônicos.

O Congresso Nacional decreta:

Art. 1º Considera-se documento eletrônico, para os efeitos desta Lei, todo documento, público ou particular, originado por processamento eletrônico de dados e armazenado em meio magnético, optomagnético, eletrônico ou similar.

Art. 2º Considera-se original o documento eletrônico autenticado por assinatura eletrônica, processado segundo procedimentos que assegurem sua autenticidade e armazenado de modo a preservar sua integridade.

Art. 3º No caso de transações que gerem grandes volumes de registros ou informações complexas, é admissível a aceitação de um sumário da operação para sua comprovação, desde que os registros detalhados estejam disponíveis a qualquer momento.

Art. 4º É cópia fiel a impressão em papel dos dados contidos em documento eletrônico autenticado, desde que obtida por meios que assegurem sua fidedignidade aos dados originais.

Art. 5º É obrigação do administrador de recursos computacionais que produz, armazena, processa ou transmite documento eletrônico:

I - assegurar proteção contra acesso, uso, alteração, reprodução ou destruição indevida dos documentos;

II - prover métodos e processos racionais que facilitem a busca de documentos;

III - manter registro de todos os procedimentos efetuados nos documentos para fins de auditoria;

IV - prever procedimentos de segurança a serem adotados em caso de acidentes que possam danificar, destruir ou impossibilitar o acesso aos dados armazenados ou em processamento.

Art. 6º Constitui crime:

I - utilizar ou reproduzir indevidamente documento eletrônico;

Pena - reclusão de 1 (um) a 2 (dois) anos e multa;

II - modificar ou destruir documento eletrônico de outrem;

Pena - reclusão de 2 (dois) anos a 5 (cinco) anos e multa;

III - interferir indevidamente no funcionamento do computador ou rede de computadores provocando a modificação ou destruição de documento eletrônico;

Pena - reclusão de 2 (dois) a 6 (seis) anos e multa;

IV - Impossibilitar ou dificultar o legítimo acesso a documento eletrônico;

Pena - detenção de 1 (um) a 3 (três) anos e multa;

V - Deixar o administrador de recursos computacionais de armazenar documento eletrônico:

a) em equipamento que não disponha de registro dos procedimentos efetuados;

b) sem manter procedimentos de segurança para o caso de acidente;

c) Pena - detenção de 1 (um) a 2 (dois) anos e multa.

Art. 7º Esta lei entra em vigor na data de sua publicação.

Art. 8º Revogam-se as disposições em contrário.

Sala das Sessões, em 11 de dezembro de 1996 - Deputado Jovair Arantes

Código Civil

"Art. 82. A validade do ato jurídico requer agente capaz, objeto lícito e forma prescrita ou não defesa em lei."

"Art. 129. A validade das declarações de vontade não dependerá de forma especial, senão quando a lei expressamente a exigir."

"Art. 136. Os atos jurídicos, a que se não impõe forma especial, poderão provar-se mediante:

I - Confissão;

II - Atos processados em juízo;

III - Documentos públicos ou privados;

IV - Testemunhas;

V - Presunção;

VI - Exames e vistorias;

VII - Arbitramento."

"Art. 1.079. A manifestação de vontade, nos contratos, pode ser tácita, quando a lei não exigir que seja expressa."

Código de Processo Civil

"Art. 131. O juiz apreciará livremente a prova, atendendo aos fatos e circunstâncias constantes dos autos, ainda que não alegados pelas partes; mas deverá indicar, na sentença, os motivos que lhe formaram o convecimento."

"Art. 154. Os atos e termos processuais não dependem de forma determinada senão quando a lei expressamente a exigir, reputando-se válidos os que, realizados de outro modo, lhe preencham a finalidade essencial."

"Art. 244. Quando a lei prescrever determinada forma, sem cominação de nulidade, o juiz considerará válido o ato se, realizado de outro modo, lhe alcançar a finalidade."

"Art. 332. Todos os meios legais, bem como os moralmente legítimos, ainda que não especificados neste Código, são hábeis para provar a verdade dos fatos, em que se funda a ação ou a defesa."

"Art. 368. As declarações constantes do documento particular, escrito e assinado, ou somente assinado, presumem-se verdadeiras em relação ao signatário.

Parágrafo único. Quando, todavia, contiver declaração de ciência, relativa a determinado fato, o documento particular prova a declaração, mas não o fato declarado, competindo ao interessado em sua veracidade o ônus de provar o fato."

"Art. 369. Reputa-se autêntico o documento, quando o tabelião reconhecer a firma do signatário, declarando que foi aposta em sua presença."

"Art. 371. Reputa-se autor do documento particular:

I - aquele que o fez e o assinou;

II - aquele, por conta de quem foi feito, estando assinado;

III - aquele que, mandando compô-lo, não o firmou, porque, conforme a experiência comum, não se costuma assinar, como livros comerciais e assentos domésticos."

"Art. 374. O telegrama, o radiograma ou qualquer outro meio de transmissão tem a mesma força probatória do documento particular, se o original constante da estação expedidora foi assinado pelo remetente.

Parágrafo único. A firma do remetente poderá ser reconhecida pelo tabelião, declarando-se essa circunstância no original depositado na estação expedidora."

"Art. 376. As cartas, bem como os registros domésticos, provam contra quem os escreveu quando:

I - enunciam o recebimento de um crédito;

II - contêm anotação, que visa a suprir a falta de título em favor de quem é apontado como credor;

III - expressam conhecimento de fatos para os quais não se exija determinada prova."

"Art. 383. Qualquer reprodução mecânica, como a fotográfica, cinematográfica, fonográfica ou de outra espécie, faz prova dos fatos ou das coisas representadas, se aquele contra quem foi produzida lhe admitir a conformidade.

Parágrafo único. Impugnada a autenticidade da reprodução mecânica, o juiz ordenará a realização de exame pericial."

"Art. 386. O juiz apreciará livremente a fé que deva merecer o documento, quando em ponto substancial e sem ressalva contiver entrelinha, emenda, borrão ou cancelamento."

"Art. 388. Cessa a fé do documento particular quando:

I - lhe for contestada a assinatura e enquanto não se lhe comprovar a veracidade;

II - assinado em branco, for abusivamente preenchido.

Parágrafo único. Dar-se-á abuso quando aquele, que recebeu documento assinado, com texto não escrito no todo ou em parte, o formar ou o completar, por si ou por meio de outrem, violando o pacto feito com o signatário

GLOSSÁRIO

ASCII: *American Standard Code for Information Interchange* - Código Padrão Americano para Intercâmbio de Informações.

Assinatura digital: transformação de uma mensagem com auxílio de matemática e criptografia.

Autenticação: processo que garante a fonte da mensagem.

Autenticação do usuário: é o processo que permite ao sistema verificar se a pessoa com quem está se comunicando é de fato a pessoa que alega ser.

Autenticação de remetente: é o processo que permite a um usuário certificar-se que a mensagem recebida foi de fato enviada pelo remetente, podendo-se inclusive provar perante um juiz, que o remetente enviou aquela mensagem.

Autenticação do destinatário: consiste em se ter uma prova de que a mensagem enviada foi como tal recebida pelo destinatário.

Autenticação de atualidade: consiste em provar que a mensagem é atual, não se tratando de mensagens antigas reenviadas.

Autenticidade: garantia oferecida ao usuário de que a origem não pode ser contestada.

Autoridade Certificadora: entidade que emite certificados de acordo com práticas definidas na Declaração de Regras Operacionais. Chamada de AC.

Autoridade Registradora: entidade de registro. Pode estar fisicamente localizada numa AC ou ser remota.

Bit: unidade comum de armazenamento no computador.

Byte: conjunto de 8 bits.

Certificado de chave pública: declaração assinada digitalmente por uma AC, contendo várias informações.

Chave privada: par de chaves mantidas secreta pelo seu dono e usada para criar assinaturas para cifrar e decifrar mensagens com as chaves públicas correspondentes.

Chave pública: par de chaves criptografadas usadas pelo seu dono e usada para verificar a assinatura digital criado com a chave privada.

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

Comércio Eletrônico: método de transação de negócio, tal como a emissão de um pedido ou a confirmação de recebimento, em formato de dados para processamento eletrônico, muito mais do que documentos em formato papel.

Criptografia: (kriptós = escondido, oculto; grápho = grafia) : é a arte ou ciência de escrever em cifra ou em códigos, de forma a permitir que somente o destinatário a decifre e a compreenda.

Criptoanálise: (kriptós = escondido, oculto; análysis = decomposição) : é a arte ou ciência de determinar a chave ou decifrar mensagens sem conhecer a chave. Uma tentativa de criptoanálise é chamada ataque.

Criptologia: (kriptós = escondido, oculto; logo = estudo, ciência) : é a ciência que reúne a criptografia e a criptoanálise.

Decifrar: ato de tranformar os dados criptografados na sua forma original, inteligível.

Fluxo de trabalho: Ver *Workflow.*

Imagem eletrôncia: técnica que utiliza mapeamento de *bits* ou *bit-mapping*, na captação das informações em documentos. Tais informações podem ser números, textos, gráficos, manuscritos, datilografados ou gerados eletronicamente.

Infra-estrutura de chaves púbicas: arquitetura, organização, técnicas, práticas e procedimentos que suportam a implementação e a operação de um sistema de certificação baseado em criptografia de chaves públicas.

Integridade: garantia oferecida ao usuário de que a informação correta, original, não foi alterada, nem intencionalmente, nem acidentalmente.

Jukebox: dispositivo para seleção e recuperação automática que permite um rápido

acesso a vários discos ópticos.

Mensagem: registro contendo uma representação digital da informação, como um dado criado, enviado, recebido e guardado em forma eletrônica.

Raiz: primeira AC em uma cadeia de certificação.

Repositório: sistema confiável e acessível *on line* que guarda e recupera certificados e informações a eles relacionados.

Sigilo: somente os usuários autorizados têm acesso à informação.

Workflow: conjunto de ferramentas pró-ativas para análise, compreensão e automação de ciclos de negócios baseados em informação.