Subsídios para implantação de Política de Assinatura Digital na RFB

Menção Honrosa

ANTONIO CARLOS TREVISAN*

* Bacharel em Administração e em Direito
Auditor-Fiscal da Receita Federal do Brasil – Julgamento
Delegacia da Receita Federal – Ribeirão Preto-SP

Subsídios para implantação de Política de Assinatura Digital na RFB

Resumo

1 Objetivos básicos

O presente trabalho pretende oferecer subsídios para a implantação de políticas de assinatura digital no âmbito da Receita Federal do Brasil, em consonância com as regras recentemente instituídas pelo Comitê Gestor da Infraestrutura de Chaves Públicas Brasileira (CGICP-Brasil) e pelo Instituto Nacional de Tecnologia da Informação (ITI).

O processo ao qual se atribui a denominação de assinatura digital possui características que permitem prover os documentos eletrônicos dos atributos de autenticação e integridade.

No entanto, os requisitos que determinam a validade de uma assinatura digital podem variar em face do negócio envolvido, em que se produzem documentos sujeitos a regras específicas de guarda e arquivamento, notadamente quanto ao prazo de arquivamento.

Por essa razão devem ser determinadas condições mínimas a serem observadas na implementação de políticas de assinatura digital, que consistem em um conjunto de regras capaz de estabelecer a validade de uma assinatura digital em determinado contexto, que pode ser de negócio ou jurídico dado, a qual possui o mesmo valor de uma assinatura manuscrita.

Inicialmente, o European Telecommunications Standards Institute (ETSI) propôs um modelo de política de assinatura vinculado à validação de uma assinatura digital independentemente das outras assinaturas digitais existentes no documento. Ocorreu, após isso, um alargamento da visão, com a edição de outras recomendações, além da edição das *Requests for Comments* (RFC) n. 3852 e n. 3275, que introduziram os padrões CMS Advanced Electronic Signature (CadES) e XMLdSIG-Advanced Electronic Signature (XadES), respectivamente.

Ambos os padrões proveem as assinaturas de um agregado de informações que permitem sua validação a mais longo prazo. Nesse diapasão, o CGICP-Brasil editou a Resolução n. 62, de 09/01/2009, que aprovou a versão n. 1 do documento *Visão geral sobre assinaturas digitais na ICP-Brasil*. Com base em tal norma, o ITI editou as Instruções Normativas n. 1, 2 e 3, de 09/01/2009, que tratam, respectivamente, dos requisitos mínimos para geração e verificação de assinaturas digitais, do perfil para assinaturas digitais e dos requisitos mínimos para políticas de assinatura digital.

No âmbito da RFB, em que a gama de documentos previstos nos normativos é extensa, deparamo-nos com a necessidade de aplicar sobre eles mais de uma assinatura, com atributos de autoria, compromisso, autorização, testemunhal, etc., que podem apresentar requisitos de relacionamento entre si, como ordem de geração de assinatura (por exemplo, quem autoriza assina depois de quem solicita a autorização) e prazo de arquivamento. Não se pode descurar que a maioria dos documentos é produzida sob a égide de um processo administrativo, fiscal ou não, adstrito à legislação tributária e/ou administrativa e submisso aos respectivos princípios reguladores.

2 Metodologia utilizada

Nos estreitos limites deste trabalho, partiu-se da abordagem de temas relativos à conceituação de criptografia, assinatura digital e documento eletrônico, para, ao final, oferecer subsídios para a implementação de políticas de assinatura digital no âmbito da RFB.

O trabalho de pesquisa centrou-se no estudo da literatura jurídica e técnica que trata do tema, bem assim na exposição do estágio em que se encontra o processo eletrônico na RFB. Este, por sua vez, reclama a implementação de um assinador de documentos concebido sob as regras do ITI para que os diversos documentos nele contidos possam ser originariamente produzidos em ambiente digital e para permitir seja instituído um canal de comunicação com o contribuinte, via domicílio tributário eletrônico.

Para tanto, antes de se construir o assinador, é necessário que seja aprovada uma Política de Assinatura Digital para os documentos eletrônicos produzidos.

3 Adequação do trabalho aos critérios de julgamento

A implementação de uma Política de Assinatura Digital é caminho obrigatório para o desenvolvimento de um assinador de documentos segundo as regras do ITI. Trata-se de ferramenta indispensável para que se implante um processo verdadeiramente digital no âmbito da RFB, em que o trânsito de documentos emitidos e recebidos ocorra pela rede, com a consequente redução dos custos com envio e armazenamento, além de possibilitar a redução do tempo de duração do processo.

O ganho em produtividade decorrerá da racionalização das atividades, com a eliminação de retrabalho oriundo da digitalização ou impressão de documentos, aliada à redução do prazo de vida do processo, uma vez que o tempo com a movimentação será drasticamente reduzido, haja vista que os autos seguirão em meio digital.

Os recursos para determinar a Política de Assinatura Digital e a construção do assinador de documentos demandarão trabalho de especificação do qual devem participar servidores pinçados de áreas que se utilizam do processo eletrônico, notadamente atendimento ao contribuinte, tecnológica e julgamento, e que disponham de conhecimento na área do direito da informática, além de analistas de sistemas.

Com vistas à implementação do macroprocesso tributário e em face da diretiva de interoperabilidade instituída na esfera do Poder

Executivo, deverão ser envidados esforços no sentido de envolver o Conselho Administrativo de Recursos Fiscais e a Procuradoria Geral da Fazenda Nacional.

Sob o prisma da valorização do servidor, a implantação do assinador digital irá liberar os usuários de tarefas repetitivas e monótonas e permitirá que desenvolvam a criatividade no sentido de racionalização de custos e tarefas.

A implantação da Política e do assinador possibilitará que se institua processo de comunicação totalmente digital com o contribuinte, circunstância que reduzirá filas de atendimento, liberará servidores para outras tarefas, diminuirá retrabalho e reduzirá o tempo de vida do processo, o que, em conjunto, contribui para a agilização do ingresso do crédito tributário.

Dentre os objetivos gerais que vinculam este trabalho, destacam-se*:*

- Fortalecer a imagem institucional da RFB e promover a conscientização tributária do cidadão;
- Otimizar o controle e a cobrança do crédito tributário;
- Aprimorar a qualidade e a produtividade do trabalho fiscal;
- Aumentar a eficiência e a eficácia no preparo, na análise e no julgamento dos processos administrativo-fiscais;
- Aprimorar a política de gestão da informação e de infraestrutura de tecnologia;
- Implementar gestão de excelência na RFB.

Enfim, a implementação do uso de assinatura digital, definida em Política de Assinatura Digital, possibilitará que a comunicação com o contribuinte ocorra em ambiente totalmente digital, permitindo a formação de processos totalmente digitais, daí resultando substancial redução do seu tempo de vida. Ao mesmo tempo, agilizará a resposta ao contribuinte e o ingresso do crédito tributário. Por fim, reforçará a imagem institucional da RFB como órgão de governo eficiente, eficaz e efetivo.

Abreviaturas

ACT	Autoridade de Carimbo de Tempo
CadES	CMS Advanced Electronic Signature
CGICP-Brasil	Comitê Gestor da Infraestrutura de Chaves Públicas Brasileira
ETSI	European Telecommunications Standards Institute
ICP-Brasil	Infraestrutura de Chaves Públicas Brasileira
IETF	Internet Engineering Task Force
ITI	Instituto Nacional de Tecnologia da Informação
ITSS	Information Technology Security Strategy
RFB	Receita Federal do Brasil
RFC	Request For Comments
UNCITRAL	United Nations Commission on International Trade Law
XadES	XMLdSIG – Advanced Electronic Signature

Subsídios para implantação de Política de Assinatura Digital na RFB

1 Introdução

1.1 Da tecnologia da informação

Segundo Manuel Castells (1999, p. 31), a revolução da tecnologia da informação foi essencial para a implementação de um importante processo de reestruturação do sistema capitalista a partir da década de 1980.

Marco Aurélio Greco (2000, p. 11-13) assevera que o atual estágio da tecnologia impõe o desafio de nos posicionarmos diante do fenômeno de seu avanço e da globalização e identifica quatro grandes tendências que se estruturam a partir dos fenômenos antes referidos, que são: a) separação de meio e mensagem; b) aumento do poder decisório do indivíduo isolado; c) maior realce às etnias e às realidades regionais; e d) busca da integração internacional.

No âmbito da delimitação do conceito de documento, segundo Marco Aurélio Greco, o Direito apoia-se na concepção de que o mundo é feito de átomos, e as regras que disciplinam as condutas humanas assumem como referencial conceitos ou figuras cujo substrato é constituído por átomos. Servem eles como meio físico para transporte e comunicação de mensagens, materializado no elemento papel.

Desse modo, alterar o foco de interesse do átomo para o *bit* implica profunda mudança nos padrões de comportamento da sociedade, dado que a mensagem se desatrela do meio físico para ter vida própria, valendo a representação dos *bits* pela utilidade que pode significar.

Nesse diapasão, assinaturas digitais e certificados eletrônicos emergem como os mecanismos bastantes para garantir as características antes descritas, além de atribuírem validade jurídica a tais transações.

Por esse prisma, e considerando-se a pretensão da Receita Federal do Brasil (RFB) de estabelecer a comunicação entre os contribuintes por meio de rede, em ambiente digital, verifica-se a necessidade da instituição de políticas de assinatura digital.

Como resultado, os documentos eletrônicos produzidos com o uso de assinatura digital nos moldes das regras da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) conterão atributos de autoria, integridade e força probante, além de poderem circular por rede de computadores. Isso facilitará sobremaneira o trato entre a RFB e o contribuinte, imprimirá velocidade ao fluxo de comunicação, permitirá reduzir o tempo de vida dos processos e agilizará o ingresso do crédito tributário.

1.2 Interoperabilidade

Fabiano Menke (2005) define interoperabilidade como a capacidade que aparelhos ou equipamentos, componentes de determinado sistema, têm de se comunicar entre si, a qual deve ser vista como o objetivo a alcançar por qualquer infraestrutura cujo escopo seja atingir a coletividade.

No âmbito do Poder Executivo e em consonância com as diretrizes do Comitê Executivo de Governo Eletrônico, instituiu-se a arquitetura e-Ping – Padrões de Interoperabilidade de Governo Eletrônico. Esta define um conjunto mínimo de premissas, políticas e especificações técnicas que regulamentam a utilização da Tecnologia de Informação e Comunicação (TIC), bem como estabelece condições de interação com os demais Poderes e esferas de governo e com a sociedade em geral,

assentadas nas áreas de interconexão, segurança, meios de acesso, organização e intercâmbio de informações e de integração para Governo Eletrônico, com base em quatro conceitos:

- Intercâmbio coerente de informações e serviços entre sistemas. Deve possibilitar a substituição de qualquer componente ou produto usado nos pontos de interligação por outro de especificação similar, sem comprometimento das funcionalidades do sistema.
- Habilidade de transferir e utilizar informações de maneira uniforme e eficiente entre várias organizações e sistemas de informação.
- Habilidade de dois ou mais sistemas (computadores, meios de comunicação, redes, *software* e outros componentes de tecnologia da informação) de interagir e de intercambiar dados de acordo com um método definido, de forma a obter os resultados esperados.
- Interoperabilidade, que define se dois componentes de um sistema, desenvolvidos com ferramentas diferentes, de fornecedores diferentes, podem ou não atuar em conjunto.

A ideia de interoperabilidade, além de contemplar integração de sistemas e de redes, abrange também a troca de dados entre sistemas, observando-se a tecnologia empregada e levando-se em conta eventual legado de sistemas, plataformas de *hardware* e *software* instalados, com objetivo de que atuem cooperativamente, visando à troca de informações.

A adoção de tal medida é extremamente salutar, pois permite a padronização de procedimentos e a racionalização das atividades, o que beneficiará a RFB e os contribuintes usuários dos diversos sistemas existentes.

2 Segurança, assinatura e certificação digital

2.1 Da criptografia e da assinatura digital

Pedro Antônio Dourado de Rezende, professor do Departamento de Ciências da Computação da Universidade de Brasília, no 1º Seminário

de Crimes de Alta Tecnologia, promovido pela Academia Nacional de Polícia em 2002, deixou consignado que a confiança na autoria de documentos eletrônicos foi, a princípio, preocupação de criptólogos, que buscaram meios de viabilizá-la para oferecer segurança à virtualização de processos sociais, impulsionada pela revolução digital.

Segundo o professor, o surgimento do conceito de assinatura digital deu-se pela interpretação de teoremas matemáticos na teoria da informação, uma teoria semiótica[1] desenvolvida por Claude Shannon a partir de 1949. Nessa teoria, de uma sequência de zeros e uns, que se constitui na representação digital de um documento, abre-se a questão acerca dos meios digitais de que seu autor poderá dispor para dar crédito à declaração de sua vontade ou autoria.

O ciframento de uma mensagem codificada por criptografia baseia-se em dois componentes: um conjunto de regras que determina as transformações do texto, denominado *algoritmo*,[2] e o parâmetro que determina as condições de transformação, denominado *chave*.

Por meio do uso de algoritmos criptográficos é possível tornar a informação incompreensível aos olhos de quem não possua o segredo necessário para a correta transformação e compreensão dos dados ilegíveis.

É necessário ressaltar duas espécies de técnicas criptográficas. Uma delas, a mais antiga, é a criptografia simétrica, que pressupõe que o emissor e o receptor tenham combinado antecipadamente e com segurança qual será a senha (MACARCINI, 2002, p. 21).

Segundo o *Guia oficial RSA*, a criptografia simétrica converte dados legíveis em algo sem sentido, com a possibilidade de se recuperarem os dados legíveis a partir dos dados sem sentido com o uso de um

1 Semiótica: denominação utilizada, principalmente pelos autores norte-americanos, para a ciência geral do signo; semiologia: ciência geral dos signos, segundo Ferdinand de Saussure, que estuda todos os fenômenos culturais como se fossem sistemas de signos, isto é, sistemas de significação. Em oposição à linguística, que se restringe ao estudo dos signos linguísticos, ou seja, da linguagem, a semiologia tem por objeto qualquer sistema de signos (imagens, gestos, vestuários, ritos, etc.).

2 Algoritmo: uma das definições do *Dicionário Houaiss da Língua Portuguesa* caracteriza como conjunto de regras e procedimentos lógicos perfeitamente definidos que levam à solução de um problema em um número finito de etapas.

algoritmo específico e de uma chave para converter as informações anteriormente encriptadas. O mesmo algoritmo utiliza a mesma chave para recuperar os dados originais (BURNETT; PAINE, 2002, p. 11).

Outro é o método de criptografia assimétrica, proposto por Whitfield Diffie e Martin Hellfman, em 1976, que utiliza duas chaves: uma delas, denominada *chave privada*, de conhecimento exclusivo de seu titular, e a outra, denominada *chave pública*, que deve ser de conhecimento do público. Enquanto o método de criptografia de chave simétrica opera dados como *bits* e manipula-os utilizando operações de computador, a criptografia assimétrica opera dados como números e os reproduz com números, o que torna a operação matemática como função de via única, conforme o *Guia RSA* (BURNETT; PAINE, 2002, p. 68 ss.).

Carlos Alberto Rohrmann (2005, p. 69) refere-se à assinatura digital como substituto eletrônico da assinatura manual que protege a mensagem transmitida em vista de que o texto é codificado por meio de algoritmos de criptografia. Qualquer mudança no documento impossibilita a autenticação da assinatura. Diferentemente da assinatura digitalizada, que se trata de uma imagem, a assinatura digital evidencia-se como um conjunto extenso de caracteres inseridos na mensagem eletrônica.

É importante registrar que a assinatura digital não se trata de um signo, um sinal, único por pessoa. Ela é única por documento, pois é gerada a partir de seu conteúdo. Dinemar Zoccoli (2000, p. 180) refere-se a ela como um lacre personalizado do conteúdo do respectivo documento com vistas a garantir sua integridade e sua autenticidade.

2.2 Da criptografia assimétrica

Diferentemente do que ocorre no âmbito da criptografia simétrica, que se presta para utilização em redes fechadas, em redes abertas a criptografia assimétrica é necessária exatamente para resolver o problema da identificação.

Baseia-se em algoritmos que utilizam duas chaves diferentes, uma privada e outra pública, relacionadas matematicamente, de forma que o texto cifrado por uma das chaves somente possa ser decifrado pela

outra chave do mesmo par. A chave pública deve ser colocada pelo seu titular à disposição do público em geral, enquanto a chave privada somente deve ser de seu conhecimento. A segurança da comunicação depende da garantia de segredo da chave privada.

Para que o sistema funcione, todos que desejam dele fazer uso geram uma chave de ciframento e sua correspondente chave de decifamento. Mantêm secreta a chave de ciframento (privada) e tornam de conhecimento geral a de decifamento (pública), enviando-a para quem deseja manter tráfego de documentos ou publicando-a em um repositório.

Quando alguém deseja enviar uma mensagem a determinado receptor deve inicialmente localizar sua chave pública, em seguida cifrar a mensagem com essa chave e enviá-la ao destinatário. Este, por sua vez, aplica sua chave privada e obtém o documento totalmente decodificado. A pedra de toque é a manutenção da confidencialidade da chave privada.

Ambas as chaves, que não mantêm nenhuma relação biométrica ou grafoscópica com seu titular, são constituídas de números de grande expressão, gerados aleatoriamente pelo computador, utilizando-se para esse fim um *software* específico, o que torna extremamente remota a possibilidade de que se possa repetir o processo para gerar outro par idêntico.

Assim, na troca de dados por meio do uso do par de chaves assimétrico, o emitente realiza a encriptação aplicando sua chave privada. O resultado somente será legível para o destinatário se ele o decriptar com a chave pública do titular.

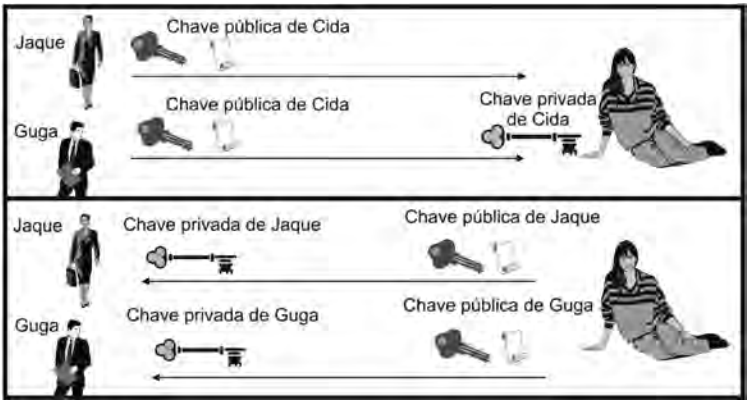
O fato de se possuir a chave privada de cifragem não permite a alteração da mensagem com o seu uso. Significa dizer que, se o arquivo for cifrado com a chave pública, ela não poderá ser utilizada para a decifração da mensagem, pois seu resultado não coincidirá com a informação original (VOLPI, 2001).

Augusto Marcacini (2002, p. 25) ressalta uma importante característica da criptografia assimétrica no que diz respeito à aplicação da

fórmula para codificação do texto. De fato, diferentemente da criptografia simétrica, em que se aplica a fórmula reversa para decriptar o arquivo, na criptografia assimétrica, para se converter o documento codificado em texto legível, utiliza-se a *mesma fórmula;* trata-se, portanto, de funções matemáticas sem retorno, que não comportam operação inversa.

O mesmo autor, em outro texto, refere-se à criptografia assimétrica como "o único meio conhecido e demonstrado de atribuir-se ao documento eletrônico duas qualidades essenciais, para que possa ser racionalmente aceito como meio de prova: a autenticidade e a integridade" (MARCACINI, 2003).

Davi Monteiro Diniz (1999, p. 30) entende ser possível imputar, com razoável segurança, a autoria da criação do arquivo ao detentor da chave pública se a chave privada permanecer em sigilo, se houver a garantia de que o par de chaves pode ser atribuído a um sujeito determinado e se confiarmos nas máquinas e nos programas de computador utilizados.



Criação Agnaldo Ribeiro

Figura 1. Cifração com chave assimétrica

2.3 Da assinatura digital e da função hash

É possível estender ao tema da assinatura digital as palavras de Augusto Marcacini, que de forma precisa delimitou o cerne do problema

quando arguiu que a questão prática a ser resolvida é de se substituir documento em papel por eletrônico. De fato, resta saber se a tradicional assinatura cursiva aposta em papel pode ser substituída por aquela obtida em meio eletrônico.

Assinaturas são geralmente usadas para se provar a autoria de documentos. Dinemar Zoccoli (2000, p. 178) traz o entendimento de Flavia Lozzi, que preconiza ser a assinatura um gesto de próprio punho que contém forte significado simbólico, suficiente, por si só, para declarar próprias as afirmações externadas, sob as quais a firma vem aposta, dificilmente esquivando-se o signatário do reconhecimento dela como sua.

Augusto Tavares Marcacini (2003) aduz que, em vista de que documentos eletrônicos podem ser alterados sem deixar vestígios e dada a impossibilidade de se lançar sobre eles assinatura autógrafa, a literatura jurídica produzida até meados da década de 1990 não os aceitava como prova documental.

Da mesma forma que se podem forjar assinaturas em documentos em papel, por meio de falsificação, muito mais facilmente se pode alterar a sequência de *bits* que compõe o arquivo digital, tornando indetectável a contrafação (REZENDE, 2002).

Desse modo, uma marca única e pessoal, constituída de *bits*, como a presença de uma imagem digital de assinatura em uma imagem de um documento digitalizado não garante que o texto do documento ou a assinatura sejam os mesmos do original impresso.

A credibilidade, no âmbito de declarações de vontade virtuais, só ocorrerá por meio de um processo autenticatório, que controle a presunção de confiança nos intermediadores da comunicação digital. Uma marca pessoal, feita de *bits*, não pode ser aposta no documento para autenticá-lo, dado que permitirá fraudes perfeitas.

Dinemar Zoccoli (2000, p. 179) traz o entendimento do ITSS, grupo de trabalho sobre matérias legais patrocinado pelo governo do Canadá, segundo o qual a necessidade da assinatura em um documento eletrônico é tratada sob o enfoque seguinte:

> *No mundo eletrônico, o original de um documento eletrônico é indistinguível de uma cópia, não existe assinatura escrita de próprio punho e ele não está sobre o papel. O potencial para fraudes é grande, devido à facilidade de interceptação e alteração dos documentos eletrônicos e à velocidade de processamento de múltiplas transações. Sempre que as partes tratem entre si com muita frequência, ou onde não existam consequências legais, uma assinatura pode não ser necessária. Todavia, existindo um alto potencial para disputa, ou uma assinatura tradicional ou uma assinatura digital é requerida.*

Resta estabelecer que assinatura digital é espécie da qual é gênero a assinatura eletrônica. Significa esta qualquer mecanismo cuja finalidade seja preencher um ou alguns dos requisitos das assinaturas tradicionais, como, por exemplo, a biométrica – que se utiliza de atributos físicos –, a senha pessoal, o cartão eletrônico, etc.

Pode-se definir assinatura digital como o resultado da operação de cifragem do documento eletrônico aplicando-se-lhe a chave privada de seu titular. Sua conferência processa-se com o uso da chave pública, reputando-se autêntica e íntegra se puder ser decifrada sem inconsistências.

Considerando-se que a utilização de algoritmos assimétricos para criptografia é contraproducente, dado que tal método é lento e demanda significativos recursos computacionais, em vez de se cifrar toda a mensagem, utiliza-se uma função matemática específica unidirecional – *hash function* –, ou função digestora, também denominada *message digest*, *one-way function* ou função de espalhamento unidirecional, que gera um valor pequeno, de tamanho fixo, derivado da mensagem e pode ser entendido como seu resumo.

Esse código pode ser reproduzido por qualquer pessoa que tenha o mesmo conjunto de dados, mas é impossível criar-se outro conjunto que produza o mesmo código *hash*. Aplicando-se a analogia, pode-se dizer que esse valor está para o conteúdo da mensagem assim como o dígito verificador de uma conta bancária está para seu número.

O código serve para garantir a integridade do conteúdo da mensagem que representa. Não garante, entretanto, privacidade, dado que o código *hash* é anexado ao texto e não o modifica. Desse modo, após seu cálculo, qualquer modificação no conteúdo da mensagem será detectada, pois um novo cálculo do valor *hash* sobre o arquivo modificado resultará em um valor *hash* distinto, ressaltando-se que não é possível realizar operação inversa para, a partir do resumo da mensagem, chegar-se à mensagem que o produziu.

Augusto Marcacini (2002, p. 35) esquematiza a produção da assinatura de um documento eletrônico, que após assinado continua legível:

> *[...] a princípio calcula-se o "resumo da mensagem", aplicando-se a função digestora ao documento; em seguida, o "resumo da mensagem" é criptografado com a chave privada do emitente. O resultado é a assinatura digital.*

A assinatura assim obtida será anexada ao documento eletrônico original, compondo a mensagem que será transmitida ao receptor.

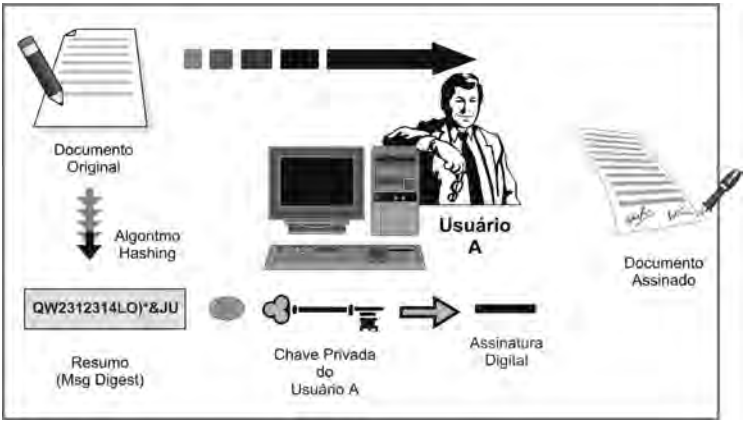
Em outra etapa, o destinatário recebe a mensagem (documento original mais a assinatura) e aplica a função *hash* ao documento original, obtendo um resultado *(resumo 1).* Em seguida, a assinatura é decifrada utilizando-se a chave pública do emissor, obtendo-se assim outro *resumo.* Compara-se, então, o *resumo* com o *resumo 1.* Caso os resultados sejam iguais, pode-se concluir que o documento está íntegro e que foi realmente enviado pelo emissor, pois a chave pública do receptor o decifrou.

No âmbito da competência que lhe foi outorgada pela Medida Provisória n. 2.200-2, de 2001, o secretário executivo do CGICP-Brasil editou a Resolução n. 62, de 09/01/2009, que aprovou a versão 1.0 do documento *Visão geral sobre assinaturas digitais na ICP-Brasil*. Dentre as inúmeras definições que o referido documento apresenta, vale ressaltar as seguintes:

Assinatura eletrônica: o conjunto de dados sob forma eletrônica, ligados ou logicamente associados a outros dados eletrônicos, utilizado como método de comprovação da autoria.

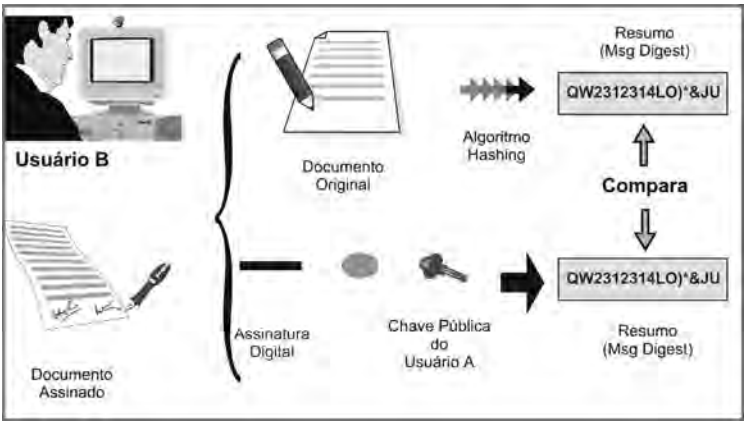
Assinatura digital ICP-Brasil: é a assinatura eletrônica que: a) esteja associada inequivocamente a um par de chaves criptográficas que permita identificar o signatário; b) seja produzida por dispositivo seguro de criação de assinatura; c) esteja vinculada ao documento eletrônico a que diz respeito, de tal modo que qualquer alteração subsequente neste seja plenamente detectável; e d) esteja baseada em um certificado ICP-Brasil, válido à época da sua aposição.

Função hash: uma transformação matemática que faz o mapeamento de uma sequência de bits de tamanho arbitrário para uma sequência de bits de tamanho fixo menor – conhecido como resultado hash ou resumo criptográfico – de forma que seja muito difícil encontrar duas mensagens produzindo o mesmo resultado hash (resistência à colisão) e que o processo reverso também não seja realizável (dado um resultado hash, não é possível recuperar a mensagem que o gerou).



Criação Agnaldo Ribeiro

Figura 2-A. Assinatura digital



Criação Agnaldo Ribeiro

Figura 2-B. Assinatura digital

2.4 Da certificação digital

Ao se utilizar um sistema que envolva chave pública, o gerenciamento de chaves passa a ter dois novos aspectos: primeiro, deve-se previamente localizar a chave pública de qualquer pessoa com quem se deseja comunicar e, segundo, deve-se obter uma garantia de que a chave pública encontrada seja proveniente daquela pessoa. Sem essa garantia, um terceiro (intruso) pode convencer os interlocutores de que chaves públicas falsas pertencem a eles.

Assim, quando um interlocutor envia uma mensagem a outro solicitando sua chave pública, um terceiro (intruso) poderá interceptá-la e devolver-lhe uma chave pública forjada por ele. Tal procedimento pode ocorrer com o emissor e o receptor da mensagem.

A garantia para se evitar esse tipo de ataque é representada pelos certificados de chave pública, que consistem em chaves públicas assinadas por uma pessoa de confiança, chamada terceiro confiável (TTP – *Trusted Third Party*) e servem para evitar tentativas de substituição de uma chave pública por outra.

O certificado, além da chave pública, contém informações pessoais sobre seu titular, é assinado digitalmente por uma terceira parte

confiável (autoridade certificadora), que associa o nome (e atributos) de uma pessoa ou instituição a uma chave criptográfica pública.

Augusto Marcacini (2003), no contexto que envolve os aspectos de autenticidade e integridade, define o certificado eletrônico como a forma mais prática de se demonstrar a titularidade da chave pública.

Fabiano Menke (2005, p. 49) conceitua o certificado digital como uma estrutura de dados sob a forma eletrônica, com prazo de validade determinado, assinada digitalmente por uma terceira parte confiável que associa o nome e os atributos de uma pessoa a uma chave pública. Aduz que o interessado na sua obtenção é identificado mediante presença física e documentalmente pelo terceiro de confiança, que emite o respectivo certificado. Atualmente regula os requisitos para política de certificados no âmbito da ICP-Brasil a Resolução nº 41, de 18/04/2006, do CGICP-Brasil.

Sob a óptica jurídica, o certificado digital pode ser entendido como uma declaração de uma pessoa (ente certificante), em relação à chave pública de uma outra pessoa, atestando essa titularidade. No campo técnico, trata-se de arquivo eletrônico, assinado pelo certificante com sua chave privada contendo a chave pública e informações pessoais do titular dessa chave pública.

2.5 Do carimbo de tempo

O mecanismo que se presta a criar um vínculo temporal em uma assinatura digital é o carimbo de tempo, que possibilita provar que o documento eletrônico existia na data incluída no carimbo de tempo. Para resguardar a confiabilidade de tal sistemática, é importante que ele seja emitido por uma terceira entidade confiável, denominada Autoridade de Carimbo de Tempo (ACT).

As normas do ITI estabelecem que os documentos eletrônicos assinados digitalmente conforme as regras da ICP-Brasil são válidos independentemente de ser aplicado a eles carimbo de tempo. Significa dizer que sua utilização é facultativa.

Segue visão esquemática do modelo, extraído do documento *Visão geral do sistema de carimbos de tempo na ICP-Brasil*, colhido do sítio do ITI:

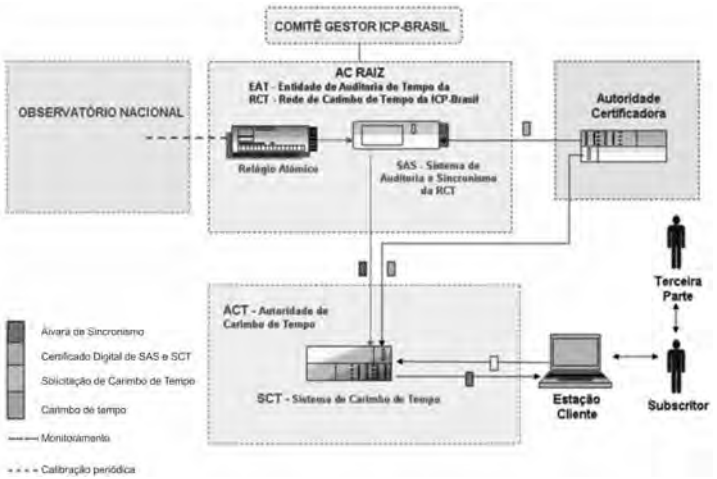


Figura 3. Carimbo de Tempo na ICP-Brasil

A utilização do carimbo de tempo assegura um instante confiável de tempo, pois prova que o documento ou a assinatura digital existiam no momento em que ele foi aposto no documento.

3 Do documento eletrônico

Embora a doutrina seja uníssona em associar a representação do fato em si ao meio material em que se veicula, é absolutamente necessário que tenhamos em mente a circunstância de que o uso do papel nas últimas centúrias fez com que se confundisse o meio e a mensagem, a ponto de associarmos o documento ao instrumento que a conduz.

Obviamente o termo *instrumento* aqui caracterizado não quer significar aqueles escritos celebrados por oficial público com o objetivo de fazer prova de determinado ato jurídico. Presta-se apenas a definir o

objeto considerado que serve como intermediário para conduzir o que nele se acha inscrito.

Nesse diapasão, é imprescindível definir se podemos considerar o documento eletrônico, essa sequência de *bits*, como sendo espécie do gênero documento. Em seu desfavor pesa o fato de tratar-se de algo novo, timidamente previsto no ordenamento jurídico, passível de ser, ainda, culturalmente assimilável.

O documento é a própria representação do fato em si;[3] traz consigo toda a carga semiótica de significado. Ao tratar da prova civil, Carnelutti (2003, p. 179) entende que o documento é uma coisa capaz de representar um fato que se pode materializar em objeto que contém manifestação do pensamento ou apenas a própria exposição do fato em si, como um documento fotográfico ou fonográfico.

Entende o jurista, ainda, que a apreensão da ideia do documento encerra três elementos básicos, que são:

> *[...] autor, considerado não quem materialmente o elabora, mas aquele por conta de quem se forma (tanto o executor material quanto uma terceira pessoa), daí decorrendo merecer o documento a fé que goze seu autor; a implicação direta diz respeito à distinção entre documento público e privado, considerando-se o primeiro quando firmado no âmbito de atividade pública e o segundo quando o autor não esteja investido de função pública;*
>
> *conteúdo, vale dizer, o fato de representar uma declaração, abstraindo-se a concepção de continente, isto é, o meio em que é veiculada a declaração, que pode ser testemunhal ou constitutiva, conforme pretenda o declarante representar ou modificar determinada situação jurídica;*
>
> *meio, entendido como o resultado da elaboração de uma matéria cuja maior se incidência verifica na elaboração em papel, nada obstando, entretanto, que sejam utilizados*

3 Francesco Carnelutti (2003, p. 181) define documento como uma coisa capaz de representar um fato.

> *outros meios como metal, pedra, tela, cera, etc. (CARNELUTTI, 2000, p. 289).*

Interessa-nos, sobremaneira, tecer considerações acerca do último aspecto, haja vista que aí reside a nota distintiva entre documento em papel e documento eletrônico.

Hodiernamente, documento encontra-se associado à ideia de coisa, submetido ao regime jurídico aplicável às coisas corpóreas patrimoniais, passível de recepcionar sinais particulares que o irão individualizar, tornando-o singular e infungível, conforme bem o disse o advogado Davi Monteiro Diniz (1999, p. 16).

Quanto ao documento eletrônico, para delimitá-lo deve-se afastar o aspecto da materialidade, sob a mitigação do conceito de forma, particularizando o conteúdo que se quer perpetuar, consubstanciado na sequência de *bits*, captado por nossos sentidos com o apoio de ferramental específico.

Embora a doutrina proponha inúmeras classificações de documentos, para o escopo deste trabalho vale considerar as definições de documento público e particular adiante expostas, dado que o entendimento da Medida Provisória 2.200-2/2001 restringe-se a considerar os documentos eletrônicos abrangidos por certificação digital como públicos ou particulares:

- *públicos*, aqueles firmados por uma autoridade pública, apresentam fé pública, gozam de presunção legal de autenticidade quanto aos elementos de formação do ato e autoria da declaração dos envolvidos; relativamente ao conteúdo das declarações neles apostas, apenas os autores respondem;
- *particulares*, são aqueles que se originam de particulares ou por quem age nessa qualidade; inexiste intervenção do oficial público.

À luz do que se registrou acerca de documento, é bastante oportuna a definição de Newton de Lucca (2000, p. 65), que conceitua documento eletrônico como “qualquer objeto capaz de propiciar a outro objeto (o suporte representativo) condições de obter a representação de um fato presente ou passado”.

No âmbito do comércio eletrônico, a Lei Modelo da UNCITRAL, que propõe uniformização internacional da legislação sobre o tema, estabelece em seu artigo 5º que "não se negarão efeitos jurídicos, validade ou eficácia à informação apenas porque esteja na forma de mensagem eletrônica".

Por seu turno, o Projeto de Lei nº 1.589/1999 caracteriza-o como "a informação gerada, enviada, recebida, armazenada ou comunicada por meios eletrônicos, ópticos, optoeletrônicos ou similares".

Marcacini (2002) refere-se ao documento eletrônico como sendo um sequencial de *bits* traduzido por um programa computacional e representativo de determinado fato, que pode ser tanto um texto redigido como um som, desenho, fotografia, etc.

Antônio Terêncio Marques (2008, p. 130), ao mesmo tempo em que conclui que o documento eletrônico é totalmente desvinculado do meio em que foi originalmente armazenado, salienta que as características de conservação, transmissibilidade e segurança de que se reveste têm importância significativa para demonstrar sua autonomia e preponderância em relação ao documento em papel.

Calcado na definição que César Viterbo Matos Santolim (1995, p. 35-36) empresta ao documento eletrônico, cita o autor três características que deve possuir, a saber:

> *[...] permitir livremente a inserção dos dados ou a descrição dos fatos que se quer registrar;*
>
> *permitir a identificação das partes intervenientes, de modo inequívoco, a partir de sinal ou sinais particulares;*
>
> *não pode ser adulterado sem deixar vestígios localizáveis, ao menos através de procedimentos técnicos sofisticados, assim como ocorre com o suporte cartáceo.*

É necessário levar em conta que, em vista de ser passível de adulteração sem deixar rastro, deve o documento eletrônico, para que possa fazer prova, apresentar assinatura digital, pois apenas nessa circunstância é que se lhe pode atribuir as características de autenticidade e de integridade.

Entretanto, não se pode descurar, também, que experimentamos um progresso notável na área da informática, em que inovações ocorrem diariamente. Dessa forma, embora nos dias de hoje possa afirmar-se que a certificação e a assinatura digitais por meio de criptografia assimétrica revestem o documento eletrônico de segurança quanto aos aspectos de autenticidade e integridade, nada garante que não seja desenvolvido sistema que desvende o conteúdo criptográfico dos algoritmos hoje aplicados.

4 Da força probante do documento eletrônico

Delimitadas as questões acerca de criptografia e certificação digital, resta definir se o documento eletrônico emitido sob processo criptográfico e de certificação digital presta-se a servir como meio de prova, oponível contra terceiros ou no âmbito do processo judicial.

Para tanto é necessário termos em mente que:

a. a certificação digital presta-se a associar o titular de um certificado a uma chave pública correspondente;

b. o método de criptografia assimétrica assegura autenticidade e integridade ao documento eletrônico;

c. documento eletrônico é a representação de um ato ou fato jurídico, manifestada no ambiente digital.

4.1 Da autenticidade do documento eletrônico

Humberto Theodoro Júnior (2000, p. 394) realça a necessidade de o documento ser autêntico e trazer a subscrição de seu autor para servir como meio eficaz de prova, ressaltando que apenas ocorre autenticidade se houver certeza sobre a veracidade da assinatura nele contida.

A Medida Provisória nº 2.200-2/2001 instituiu a Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) para garantir a *autenticidade*, a *integridade* e a *validade jurídica* de documentos em forma eletrônica, a teor de seu artigo 1º.

O processo de certificação digital apenas vincula uma chave pública a um certificado.

É a assinatura digital que pode garantir a autenticidade do documento eletrônico e, consequentemente, sua força probante. Tal afirmação não tem caráter absoluto, dado que pode ocorrer a prática de ilícito, como o vazamento da chave privada ou uma certificação espúria. Sua credibilidade acha-se vinculada diretamente à qualidade do aplicativo que gerará o par de chaves, à distribuição correta da chave pública e à preservação da chave privada.

4.1.1 Da assinatura e da assinatura digital

A esta altura poderia restar a dúvida se a assinatura digital presta-se a substituir a assinatura de próprio punho, cujo uso se acha sedimentado em nossa sociedade.

Neves e Castro (2000, p. 359) leciona que o étimo da palavra *assinar* se assenta na expressão *signum facere*, embora entendesse que a assinatura das partes devia ser feita por letra, pelas “próprias pessoas ou por outras, quando não saibam ou não possam escrever”.

Há que se registrar que o jurista considerava a necessidade de se lavrar a assinatura pelas próprias pessoas em vista da existência da assinatura de cruz, hoje em desuso, dado que a maioria da população é alfabetizada.

Impõe-se destacar que a assinatura se trata de um signo cuja função, sedimentada culturalmente, é a de designar autoria ou aprovação do conteúdo de um escrito, segundo uma das acepções que lhe emprega o *Dicionário Houaiss da Língua Portuguesa.*

A propósito, Umberto Eco (2000, p. 39), ao tratar da função sígnica dentro da Teoria dos Códigos, entende existir signo sempre que ocorrer correlação entre elementos de um plano da expressão convencionalmente relacionado a um ou mais elementos de um plano do conteúdo, reconhecido pela sociedade humana. Assim, explica-se perfeitamente por que, durante décadas, a assinatura de próprio punho foi plenamente aceita como condição da autenticidade de um documento.

Sob tal enfoque, é perfeitamente aceitável que, se a utilização da assinatura digital for culturalmente chancelada, será ela outra forma de se atribuir autenticidade aos documentos por essa forma lavrados, assim como se atribuiu autenticidade àqueles em que se apunha marca por meio de sinete, por exemplo.

Nesse diapasão, o CGICP-Brasil expressamente reconheceu que a assinatura digital gerada em conformidade com as normas que regulam a ICP-Brasil tem o mesmo valor de uma assinatura manuscrita (Resolução nº 62, de 09/01/2009, do CGICP-Brasil).

4.2 Da equivalência funcional

Fábio Ulhoa Coelho (2008) leciona que a Lei Modelo da UNCITRAL recomendara que os países nela se inspirassem com vistas a disciplinar a matéria nas respectivas legislações internas. O modelo da lei em referência acha-se acompanhado de um *Guia para incorporação ao direito interno* que explicita cada um dos artigos nela enumerados (BLUM, 2001, p. 258).

No que diz respeito ao critério da equivalência funcional, ao qual Fábio Ulhoa Coelho atribui a dignidade de princípio norteador da Lei Modelo,[4] segundo o *Guia* acha-se assentado no fato de que o maior óbice para o desenvolvimento dos modernos meios de comunicação ocorre nos requisitos legais que estabelecem o uso de documentação tradicional impressa ou escrita em papel, expressamente formulado no preceptivo que emana de seu artigo 5º, que prescreve:

> *Artigo 5º Reconhecimento jurídico das mensagens de dados*
>
> *Não se negarão efeitos jurídicos, validade ou eficácia à informação apenas porque esteja na forma de mensagem eletrônica.*

4 Robert Alexy (2008, p. 90) considera princípios como mandamentos de otimização que podem ser satisfeitos em graus variados a depender das possibilidades fáticas e jurídicas.

Um dos escopos na preparação da lei foi o de ampliar conceitos como o de “escrito”, “assinatura” e “original” com vistas a contemplar o emprego de técnicas baseadas em informática, sob a premissa de que na seara eletrônica existe o atendimento das mesmas funções que exerce o papel relativamente ao registro de informações de pertinência jurídica. Assim, descabe negar-se o atributo de juridicidade a um documento eletrônico apenas em face da natureza de seu suporte.

De acordo com o *Guia* e em conformidade com o que leciona Fábio Ulhoa Coelho (2008), o papel desempenha as seguintes funções relativamente ao documento jurídico que o adota por suporte:

a. permite a leitura do documento por todos os interessados;
b. assegura a integridade do documento ao longo do tempo;
c. permite a reprodução, para que todas as partes possam ter um exemplar idêntico do escrito;
d. permite a autenticação por meio da assinatura das partes;
e. serve à produção de prova perante o Juiz e a Autoridade Administrativa.

No desempenho dessas funções, o meio eletrônico pode oferecer segurança igual à do papel e, em alguns casos, maior confiabilidade e rapidez no que se refere à determinação da origem e conteúdo dos dados, desde que atendidos requisitos técnicos e jurídicos suficientes para tanto. Não há, por isso, fundamento para se exigir, em relação ao documento eletrônico, o atendimento de outros requisitos de validade e eficácia além do que se exige para o documento em papel.

Significa dizer, com base em Fábio Ulhoa Coelho (2008), que tanto o suporte em papel como o eletrônico desempenham, relativamente ao documento jurídico, as funções a seguir:

- **Acessibilidade** – As partes e, se o documento for público, todos os interessados podem ter acesso às informações registradas. No documento em papel é suficiente que o leitor conheça a linguagem em que fora escrito e disponha do respectivo suporte. No eletrônico, o acesso é garantido mediante processamento em computador que traduza para a linguagem do leitor.

- **Integridade** – Sabemos que as informações constantes em papel podem ser adulteradas, em que pese a confiança que depositamos na integridade das informações nele consignadas. Assegura-se a integridade em face das pistas que eventual adulteração produz, à luz do trabalho técnico pericial. Um arquivo eletrônico adulterado ou simplesmente acessado também deixa pistas que podem ser aferidas por perícia técnica, ressalvando-se que naqueles as pistas são físicas e neste são eletrônicas.
- **Reprodutibilidade** – O documento em papel pode ser copiado em outro papel, a fim de possibilitar que todas as partes tenham seu próprio exemplar, idêntico ao original. Cópia de documento no ambiente eletrônico pode ser obtida tanto por escaneamento do original em papel quanto pela produção de arquivo eletrônico, que também permite às partes terem seu próprio exemplar. No caso de arquivo eletrônico, ressalte-se que não há como distinguir cópia do original.
- **Função probatória** – Os documentos eletrônicos são admitidos como prova em juízo ou perante a Autoridade Administrativa tais como os que têm o papel como suporte.
- **Autenticação por assinatura** – O documento eletrônico pode ser autenticado por assinatura digital, baseada em criptografia assimétrica, no contexto da ICP-Brasil. O uso de tal sistemática garante a autenticidade e a integridade do documento. Desde que observado tal meio de autenticação ou outro que eventualmente venha a ser criado e que ofereça semelhante grau de segurança, o documento eletrônico cumpre função idêntica à daquele em papel. Assegura-se que a declaração partiu de determinada pessoa, foi recebida por outra e conservou-se íntegra durante o trajeto.

O princípio da *equivalência funcional* é o principal argumento da tecnologia jurídica dos documentos virtuais. Por esse conceito, o documento eletrônico cumpre as mesmas funções do documento em suporte papel e não pode ser rejeitado pelo simples fato de se encontrar em meio magnético ou eletrônico.

O ordenamento jurídico preocupou-se em atribuir garantias ao documento comum em papel para que sua função seja considerada

válida. Dessa forma, o documento precisa conter a devida autenticidade, integridade e perenidade, para efeitos de prova eficaz. Com assinatura e certificação digitais o documento eletrônico cumpre todos os requisitos bastantes para atribuir força probante, sob o manto do princípio da equivalência funcional.

4.2.1 Do Projeto de Lei nº 7.316/2002

Tramita no Congresso Nacional o Projeto de Lei nº 7.316, de 2002, que dispõe sobre o uso de assinaturas eletrônicas, certificados digitais, ICP-Brasil e prestação de serviços de certificação.

O texto atual, após algumas emendas e o substitutivo do deputado Maurício Rands, apresenta, em linhas gerais, os aspectos a seguir delimitados:

- incorpora as normas da MP 2.200-2/2001 e a revoga;
- sintetiza diversas definições que já se acham consolidadas em normas editadas pelo Comitê Gestor da ICP-Brasil e pelo ITI;
- equipara serviços notariais e de registro a pessoa jurídica, para fins de prestação de serviços de certificação, de carimbo de tempo e de entidade de registro;
- estabelece como a hora a ser utilizada pelos prestadores de serviço de carimbo de tempo a Hora Legal Brasileira;
- prevê a utilização de certificado qualificado de pessoa jurídica, que será objeto de posterior regulamentação pelo Comitê Gestor da ICP-Brasil;
- estende a aplicação aos serviços de carimbo de tempo e de certificação, no que couber, da legislação de defesa do consumidor e das normas processuais sobre validade e prova documental.

5 Política de Assinatura Digital

5.1 Instituição e motivação

Dentre as definições que o CGICP-Brasil estabeleceu, figura a da política de assinatura, entendida como as regras que formalizam processos de criação e verificação de uma assinatura digital e definem a base para que ela possa ser considerada válida.

Desse modo, o signatário lança em um documento eletrônico uma assinatura digital criada em conformidade com a política de assinatura definida, a qual será utilizada pelo verificador para aferir a validade da assinatura.

Ressalte-se que as políticas podem ser criadas pelo signatário, pelo verificador ou por qualquer outra entidade que entenda apropriado fazê-lo.

Com a finalidade de se atribuir confiabilidade e credibilidade ao processo de criação e validação de assinaturas digitais, o CGICP-Brasil editou a Resolução nº 62, de 09/01/2009, complementada por outras normas veiculadas em instruções normativas editadas pelo ITI. Visando a estabelecer um padrão de assinatura digital e políticas de assinatura digital para o país, tais documentos definiram formatos e processos que deverão ser utilizados na geração e na verificação de assinaturas digitais em documentos eletrônicos.

As resoluções da ICP-Brasil em vigor encontram-se catalogadas sob a forma de documentos, denominados DOC-ICP, e estão organizadas de modo que facilitem a leitura e a compreensão de quem as estuda. No caso da política de assinaturas digitais, trata-se do DOC-ICP 15 e acessórios.[5]

5 DOC-ICP-nn são os documentos principais, que trazem as diretrizes gerais sobre os diversos assuntos normatizados na ICP-Brasil. Sua criação e alteração dependem sempre de aprovação do Comitê Gestor da ICP-Brasil, por meio de Resoluções. DOC-ICP-nn.mm são os documentos acessórios, destinados a suplementar, quando necessário, os DOC-ICP-nn. São aprovados por meio de Instruções Normativas do Instituto Nacional de Tecnologia da Informação – ITI, que recebeu essa competência do Comitê Gestor da ICP-Brasil conforme Resolução nº 33, de 21 de outubro de 2004.

A dita norma determinou que as entidades integrantes da ICP-Brasil adaptem seus sistemas ao novo padrão no prazo de um ano. A validação de assinaturas que não estejam em conformidade com o padrão, produzidas antes do prazo referido, deverá ter seus critérios estabelecidos pelas partes interessadas.

Além disso, o documento ressaltou que o padrão aprovado é uma referência genérica que poderá ser substituído por formato diverso desde que tecnicamente justificável, para uso restrito e acordado entre as partes interessadas. Significa dizer que para ser oponível a terceiros o documento eletrônico deverá ser assinado segundo os padrões estabelecidos pelo CGICP-Brasil.

A razão por que se instituiu o conjunto de normativos acha-se assentada nos seguintes objetivos:

- auxiliar entidades na adoção de normas e condutas técnicas comuns que possam ser utilizadas em sistemas de assinatura digital;
- consolidar e popularizar o uso seguro da assinatura digital;
- desenvolver a interoperabilidade entre sistemas que utilizam a assinatura digital para agilizar seus processos e aplicações;
- uniformizar os esforços na definição dos requisitos técnicos de segurança e interoperabilidade para assinaturas digitais, possibilitando maior pragmatismo e concentração de esforços na implementação dos sistemas de assinatura digital;
- aprimorar a relação custo-benefício em processos e aplicações de TI;
- melhorar a competência técnica de entidades na utilização de assinaturas digitais.

5.2 Padrões de assinatura digital

No contexto de elaboração de documento em papel, a assinatura aplicada sobre ele pode ter diferentes tipos de propósitos. Pode haver, inclusive, a necessidade de se aplicar mais de uma assinatura com a função de assinatura conjunta (quando regulamentos, estatutos ou con-

tratos exigem que figure mais de um signatário) ou função chancelatória (quando a segunda assinatura aposta tem o atributo de autorizar ou ratificar o que consta do documento). Pode haver a necessidade de que a aposição de determinada assinatura exija que o assinante comprove que está autorizado a fazê-lo. No ambiente digital tal situação também se observa, uma vez que o documento eletrônico apenas substitui o documento em papel sem que tal circunstância signifique alteração de sistemáticas legitimadas pelo uso e costume e chanceladas pelo regramento jurídico.

O ITI relaciona os tipos de compromissos de assinaturas digitais a serem utilizados no âmbito da ICP-Brasil, definidos pelo IETF na RFC 3126 e pelo ETSI TS 101 733, além de que, a depender da espécie de documento e de sua natureza jurídica, eles poderão classificar-se em:

> *Prova de origem: indica que o signatário reconhece a criação, a aprovação e o envio de uma mensagem.*
>
> *Prova de recebimento: indica que o signatário reconhece o recebimento do conteúdo de uma mensagem.*
>
> *Prova de envio: indica que o fornecedor do serviço confiável emissor da indicação disponibilizou uma mensagem em uma área de armazenamento local acessível ao destinatário da mensagem.*
>
> *Prova de envio: indica que a entidade emissora da indicação enviou a mensagem (mas não necessariamente a criou).*
>
> *Prova de aprovação: indica que o signatário aprovou o conteúdo da mensagem.*
>
> *Prova de criação: indica que o signatário criou a mensagem (mas não necessariamente a aprovou ou a enviou).*
>
> *Concordância: a assinatura aposta indica que o signatário concorda com o conteúdo assinado.*
>
> *Autorização: a assinatura aposta indica que o signatário autoriza o constante no conteúdo assinado.*
>
> *Testemunho: a assinatura aposta indica o compromisso de testemunho do signatário (não necessariamente indica concordância do signatário com o conteúdo).*

Autoria: a assinatura aposta indica que o signatário foi autor do conteúdo assinado (não necessariamente indica concordância do signatário com o conteúdo).

Conferência: a assinatura aposta indica que o signatário realizou a conferência do conteúdo.

Revisão: a assinatura aposta indica que o signatário revisou o conteúdo assinado (não necessariamente indica concordância do signatário com o conteúdo).

Ciência: a assinatura aposta indica que o signatário tomou ciência do conteúdo assinado (não necessariamente indica concordância do signatário com conteúdo).

Publicação: a assinatura tem o propósito de indicar que o signatário publicou o documento em algum meio de comunicação externo à entidade que o originou.

Protocolo: a assinatura aposta indica a intenção do signatário em protocolar o conteúdo.

Integridade: a assinatura aposta indica a intenção do signatário em garantir somente a integridade da mensagem.

Autenticação de usuário: a assinatura aposta é utilizada somente como prova de autenticação do signatário.

Teste: a assinatura aposta indica a intenção do signatário em realizar um teste.

5.3 Assinador digital de documentos e e-Processo

Há que se observar que o leque de documentos produzidos nos diversos procedimentos e processos tratados no âmbito da RFB é significativo.

Tarefa importante é mapear os diversos documentos produzidos pela RFB, que em uma análise preliminar podem ser divididos em dois grandes grupos:

- documentos produzidos em papel;
- documentos produzidos em ambiente digital.

Relativamente aos documentos produzidos em papel, creio ser antes necessário definir as especificações para que sejam elaborados em meio eletrônico. Exemplo disso são os despachos decisórios prolatados nos processos administrativos.

Importa ressaltar que a eventual inclusão de documentos produzidos em papel por meio de escaneamento produzirá apenas uma cópia do original. Resulta daí que a assinatura digital eventualmente aplicada a tais documentos apenas declara estarem as cópias em conformidade com o original.

No caso de documento eletrônico, ele será um documento original, cuja reprodução em outras cópias não afasta sua condição de originalidade. Para que tal situação se verifique, indispensável é aplicar sobre o documento o processo de assinatura digital. Embora, no âmbito da RFB, presentemente tais documentos sejam transformados em papel, o fato é que originalmente são produzidos em ambiente digital. A ocasião é propícia para definirem-se as regras de uso de assinatura digital na sua elaboração.

Por expressa determinação legal, os diversos processos tratados na RFB subsumem-se às regras do Decreto nº 70.235, de 1972, que instituiu o Processo Administrativo Fiscal (PAF), ou da Lei nº 9.784, de 1999, que regula o processo administrativo no âmbito da Administração Pública Federal.

5.3.1 e-Processo

Tanto em sede de PAF quanto em sede de Processo Administrativo Federal, o sistema e-Processo surge como instrumento hábil para substituir os autos em papel, com a vantagem de que ele integra as funcionalidades próprias de sistemas de gerenciamento eletrônico de documentos e de fluxo de trabalho. Deve ser ressaltada a circunstância de que cada um dos diversos sistemas existentes na RFB produz documentos a eles afetos. O e-Processo surge apenas como agregador de tais documentos. Nada obsta que a aposição de assinatura digital ocorra quando os documentos forem anexados ao e-Processo, com o uso de assinador digital.

Como exemplo, documentos elaborados em processos de restituição e compensação, no âmbito do SCC, poderão ser criados por meio de uma impressora virtual e incorporados ao e-Processo, utilizando-se assinatura digital. Após o despacho decisório ter sido prolatado, assinado digitalmente e anexado aos autos, o e-Processo encarrega-se de seu envio ao domicílio eletrônico do contribuinte.

A assinatura digital aplicada aos documentos deve ser produzida por meio de um aplicativo específico, o assinador digital de documentos, com a função de assinar e verificar a assinatura de documentos eletrônicos. Ele poderia ser configurado para dispor de todo o conjunto de Políticas de Assinatura, com os respectivos compromissos (seção 5.2), além de dar a opção de qual espécie de assinatura seria aplicada: simples, co-assinatura, contra-assinatura, assinatura em lote, conforme previsto no DOC-ICP-15, itens 5.8 e 5.9 (seção 5.4).

Significa dizer que ao acionar o assinador o usuário teria à sua disposição todas as espécies de assinaturas e a partir daí escolheria a correspondente ao documento que pretende assinar. Entretanto, para que tal cenário seja factível, além da integração dos sistemas, é necessário definir quais Políticas de Assinatura a RFB irá implementar.

5.4 Alguns aspectos de Política de Assinatura

As regras que especificam os processos de criação e verificação de uma assinatura digital e definem a base para que ela possa ser considerada válida devem ser estabelecidas em uma Política de Assinatura.

Desse modo, o signatário do documento aplica a respectiva assinatura em conformidade com a Política de Assinatura definida, cuja validade é aferida pelo verificador com base na mesma política utilizada na criação da assinatura digital.

O ITI estabeleceu dois padrões para assinatura digital, ao mesmo tempo em que definiu um perfil de assinatura para uso geral, baseado nos padrões antes referidos, que sintetizam os principais atributos e propriedades que devem ser utilizados nas assinaturas digitais no país. Os padrões estabelecidos são:

• CadES – CMS Advanced Electronic Signature

O padrão CMS (Cryptographic Message Syntax) trata-se de evolução do padrão PKCS#7, criado com o objetivo de prover assinaturas digitais com informações que permitam sua validação a mais longo prazo. O padrão CMS descreve uma estrutura para armazenamento de diversos conteúdos. A abordagem normativa do ITI cuida apenas da parte que se refere a dados da assinatura.

Permite realizar assinatura com conteúdo digital anexado ou separado, ou seja, o conteúdo pode ou não estar incluído na estrutura CMS. Possibilita a geração de assinaturas em paralelo e em lote, ressalvando-se que no último caso há o risco de o signatário não ter conhecimento do conteúdo que está sendo assinado.

• XadES – XMLdSIG Advanced Electronic Signature

Derivado da linguagem Extensible Markup Language (XML), o padrão XadES possibilita a criação de *tags* (termo associado a uma informação, que o descreve e permite classificar a informação com base em palavras-chave) de forma arbitrária, desde que observadas as regras de aninhamento.

Permite gerar uma assinatura digital apenas sobre uma parte de um documento eletrônico. No que diz respeito ao armazenamento do conteúdo digital, possibilita três representações:

- estrutura assinada com conteúdo digital separado, não incluído, portanto, na estrutura XML Signature;
- estrutura assinada com conteúdo digital anexado, incluído, portanto, na estrutura XML Signature;
- estrutura assinada incluída no conteúdo digital; a assinatura está inclusa no conteúdo digital assinado.

O ITI criou dois grupos de cinco Políticas de Assinaturas-padrão, derivadas dos padrões CadES e XadES e combinadas com os formatos de assinatura digital admitidos na ICP-Brasil, a saber:

- assinatura digital de curto prazo (AD-CP);

- assinatura digital com carimbo de tempo (AD-T);
- assinatura digital com referências para validação (AD-R);
- assinatura digital com referências completas (AD-C);
- assinatura digital com informações para arquivamento (AD_A); ou
- combinação dos formatos anteriores.

A necessidade de uma Política de Assinatura diferente das que foram estabelecidas pelo ITI deve ser objeto de pedido de aprovação que apresenta rito próprio, definido em regras do Instituto.

6 Visão da RFB

No atual estágio, a comunicação da RFB com o contribuinte, na maioria das vezes, ainda ocorre por meio da troca de papéis. Uma das partes veicula sua pretensão consubstanciada em registros apostos em papel (auto de infração, comunicação de cobrança, impugnações e recursos, etc.) e a outra responde por meio da elaboração de um documento em papel. Existem alguns avanços em que parte da comunicação acontece pela troca de arquivos eletrônicos, como no envio de declarações de renda de pessoas físicas e de informações das pessoas jurídicas, envio de PER/D-Comp, procedimentos de exportação e importação, etc.

Nesse contexto, os sistemas informáticos atuam como arquivos de banco de dados (Sief, Safira, Malha, etc.), enquanto o ideal é que além disso permitam tanto à RFB quanto ao contribuinte exercer a atividade de comunicação, caracterizada pela troca de arquivos eletrônicos.

Alguns sistemas da RFB foram concebidos sob a óptica de que o fluxo de documentos ocorra com a utilização dos recursos de rede de comunicação. Exemplos são o Portal de Acesso da RFB, o Sistema de Controle de Créditos, que opera o PER/D-Comp, e o e-Processo. Embora apresentem funcionalidades avançadas, como o acesso por certificação digital, o que acontece na prática é a formação de documentos eletrônicos destituídos de assinatura digital, que não se enquadram nas regras da Medida Provisória nº 2.200-2/2001.

Em face dessa circunstância limitativa, todo processo que se forma sob a égide de qualquer dos sistemas prossegue com a transformação do documento eletrônico em documento em papel. Exemplos são o auto de infração do Sistema de Malha e os despachos decisórios emitidos em processos tratados pelo Sistema de Controle de Créditos. A notificação ao contribuinte dá-se com os documentos em papel, "baixados" dos respectivos sistemas e depois impressos.

Se houver tratamento de tais documentos no âmbito do e-Processo, formam-se autos digitalizados, que, entretanto, não cumprem o atributo de força probante, dado que sobre o original eletrônico não fora aposta assinatura digital.

Registre-se que o e-Processo, que tem como um de seus principais objetivos a redução do uso do papel, ainda não conseguiu alcançar tal intento, em face de que os documentos tratados no âmbito do sistema são cópias digitalizadas, escaneadas de outros documentos originalmente produzidos em papel.

O ideal, portanto, é que todos os documentos, em vez de serem escaneados e digitalizados para juntada nos autos, sejam originariamente produzidos em forma digital.

6.1 Fluxo em papel

Como exemplo de fluxo em papel, cita-se o procedimento de malha em que, em linhas gerais, após ser destacado o contribuinte sujeito ao procedimento, efetua-se o cadastramento no sistema Comprot e em seguida procede-se à emissão do auto de infração com seu envio para o domicílio tributário do contribuinte, utilizando-se do sistema Sucop (que envelopa os documentos para encaminhamento ao contribuinte).

Intimado o contribuinte e havendo impugnação, protocolizam-se os documentos apresentados, que logo após são autuados no processo respectivo. A partir daí os autos seguem para julgamento administrativo. Se não for utilizado o sistema e-Processo, instaura-se um processo totalmente em papel, quando, no início, foi utilizado sistema (malha) que poderia ser integrado para fornecer documento eletrônico.

Se for utilizado o sistema e-Processo, os documentos serão escaneados e digitalizados, e a partir daí há redução do tempo de vida do processo decorrente do ganho na movimentação, dado que internamente não haverá necessidade de uso do serviço de malote. Nesse caso haverá processo *digitalizado*. Entretanto, toda e qualquer comunicação com o contribuinte é efetuada da forma tradicional.

Se não for utilizado o e-Processo, os autos correrão em papel, com perda do tempo de vida do processo, em face de que as movimentações ocorrerão por meio do serviço de malote convencional.

6.2 Fluxo em sistema digital

A forma de se dar um passo significativo na direção do uso do documento eletrônico reside na adoção da sistemática de assinatura digital para que sejam produzidos.

Como contraponto ao exemplo dado no item anterior, partindo-se da premissa de que os autos serão formalizados no âmbito do e-Processo, após ter sido criado o arquivo eletrônico correspondente ao auto de infração, procede-se ao cadastramento no sistema Comprot. O auto de infração é anexado no e-Processo, assinado digitalmente, ao mesmo tempo em que uma via é remetida para o domicílio eletrônico do contribuinte.

O contribuinte apresenta impugnação em arquivo eletrônico, assinada digitalmente, que transita pelo seu domicílio tributário eletrônico e em seguida é anexada no e-Processo.

Conforme se pode verificar, a grande diferença reside no fato de que não há emissão de documento em papel e, por decorrência, não se utiliza de serviço de Correio. Vale ressaltar que o e-Processo, por ser um sistema que contempla gerenciamento eletrônico de documentos e *workflow*, permite automatizar um fluxo estruturado dos documentos, com significativo ganho de tempo e redução do uso de mão de obra em tarefas repetitivas, de mera execução.

Quando a assinatura digital for implantada nos documentos, em consonância com as regras do ITI, eles poderão ser totalmente produzidos

em ambiente digital, prescindirão da função de escaneamento, eliminarão a necessidade de arquivo físico em papel, eliminarão a necessidade de transporte, em vista de que os arquivos circularão pela rede, agilizarão a movimentação de processos e facilitarão a comunicação entre a RFB e o contribuinte, que se valerá do domicílio eletrônico para sua implementação.

O resultado decorrente da implementação do cenário antes delineado é a redução do tempo de vida do processo, o que permitirá agilizar o ingresso do crédito tributário, além de assegurar mais rapidez à resposta ao contribuinte.

Ademais, como itens de redução de custos, podem-se citar os decorrentes de manutenção de arquivos, os de serviços de malote e ganho de espaço físico.

Certamente não se trata de panaceia que vai resolver todos os problemas. O ganho mais significativo ocorrerá com a redução do tempo de movimentação do processo, com a racionalização dos procedimentos, que prescindirão do retrabalho decorrente de se converter arquivos eletrônicos em documentos em papel, além da desnecessidade de se escanear documentos em papel para serem posteriormente digitalizados.

Entretanto, especial atenção deverá ser dada à manutenção de rede de comunicação que opere de maneira eficiente, segura e com capacidade de absorver o fluxo de dados que por ela transitará. A comunicação entre a RFB e o contribuinte ocorrerá com o uso do domicílio eletrônico, conforme ressaltado anteriormente.

Em suma, deixaremos de ter processo digitalizado, em que os documentos inicialmente são produzidos em papel e posteriormente escaneados e anexados aos autos, para ingressarmos no mundo do processo digital, em que os documentos são originariamente produzidos em arquivos eletrônicos.

Uma pergunta que surge é por que ainda não se implantou tal método na RFB. A questão é que assinatura digital é tema relativamente recente. As recomendações do ETSI principiaram em 2002. O ITI, responsável pela sua regulação, editou as coordenadas sobre assinatura digital recentemente.

Nesse diapasão, o momento é oportuno para a RFB iniciar o processo de estabelecer sua política de assinatura digital.

7 Conclusão

As mudanças introduzidas com o advento dos recursos informáticos, materializadas na criação do documento eletrônico, implicam a redefinição do conceito de documento, abandonando-se a concepção materialista que o associa à sua base física – o papel – e voltando-se para o fato de que o documento eletrônico é, em essência, uma sequência de *bits* cuja identificação da cópia e do original é impossível e, a princípio, pode sofrer alteração sem deixar vestígios.

O documento eletrônico atende aos requisitos que apreendem a sua ideia que, segundo Carnelutti, são: autor, conteúdo e meio. Para representar um ato ou fato jurídico, deve estar amparado por sistema que preserve a autenticidade e a integridade do suporte respectivo.

A criptografia, tanto simétrica quanto assimétrica, garante os requisitos de autenticidade e integridade ao documento eletrônico.

Por autenticidade entende-se a certeza quanto à pessoa que criou o documento, que, juridicamente, presta a declaração nele inserida.

Por integridade entende-se a não adulteração de um documento posteriormente à sua criação.

A assinatura digital é um sinal individualizador, obtido utilizando-se criptografia assimétrica por meio da aplicação da chave privada do titular ao resumo da mensagem, obtido com a função digestora. O resultado assim alcançado é único para cada documento.

O processo de certificação digital apenas vincula determinada chave pública ao certificado correspondente.

O que garante a força probante do documento eletrônico é a assinatura digital. Tal afirmação tem que ser entendida com reservas, em vista de que pode ocorrer vazamento da chave privada ou certificação espúria. Sua credibilidade vincula-se ao aplicativo gerador do

par de chaves, correta distribuição da chave pública e preservação da chave privada.

A implementação do uso de assinatura digital, definida em Políticas de Assinaturas, possibilita que a comunicação com o contribuinte ocorra em ambiente totalmente digital, o que representa avanço em relação ao modelo atual, em que os documentos são produzidos em papel e depois digitalizados. Permite a formação de processos totalmente digitais, daí resultando substancial redução do seu tempo de vida; possibilita agilizar o ingresso do crédito tributário correspondente, além de imprimir rapidez à resposta ao contribuinte.

Referências

ALEXY, Robert. *Teoria dos direitos fundamentais*. Trad. Virgílio Afonso da Silva. São Paulo: Malheiros. 2008.

ALMEIDA FILHO, José Carlos de Araújo. *Processo eletrônico e Teoria Geral do Processo Eletrônico*: a informatização judicial no Brasil. Rio de Janeiro: Forense, 2007.

BLUM, Renato Ópice (Coord.). *Direito eletrônico*: a internet e os tribunais. São Paulo: Edipro, 2001.

BRASIL. Medida Provisória n. 2.200-2, de 24 de agosto de 2001. *Diário Oficial da União.* Poder Executivo. Brasília, DF, 27 ago. 2001.

BURNETT, Steve; PAINE, Stephen. Criptografia e segurança. *O Guia Oficial RSA*. Tradução integral aprovada por RSA Press. Rio de Janeiro: Campus, 2002.

CARNELUTTI, Francesco. *A prova civil*. Trad. e notas por Amilcare Carletti. São Paulo: Livraria e Editora Universitária de Direito, 2003.

_____. *Sistema de direito processual civil.* Trad. de Hiltomar Martins Oliveira. Vol. II. São Paulo: Classic Book, 2000.

_____. *Arte do direito*. Trad. Ricardo Rodrigues Gama. Campinas: Bookseller, 2003.

CASTELLS, Manuel. *A sociedade em rede.* 2. ed. São Paulo: Paz e Terra, 1999.

CLEMENTINO, Edilberto Barbosa*. Processo judicial eletrônico*. Curitiba: Juruá, 2007.

COELHO, Fábio Ulhoa. *Títulos de crédito eletrônicos.* Disponível em: <http://dircoml.blogspot.com/2008/04/artigo-do-fabio-ulhoa-coelho.html>. Acesso em 2008.

COSTA, Marcos da; MARCACINI, Augusto Tavares Rosa. *Direito em* bits. São Paulo: Fiuza, 2004.

DE LUCCA, Newton; FILHO, Adalberto Simão (Org.). *Direito & internet.* Bauru: Edipro, 2000.

DINIZ, Davi Monteiro. *Documentos eletrônicos, assinaturas digitais*: da qualificação jurídica dos arquivos digitais como documentos. São Paulo: LTR Editora, 1999.

ECO, Umberto. *Tratado geral de semiótica*. 3. ed. São Paulo: Perspectiva, 2000.

FERNANDES, Murilo Rivau. *SIPEX*: uma proposta de modelo de política de assinatura. Dissertação (Mestrado em Engenharia Elétrica) – Escola Politécnica, Universidade de São Paulo, São Paulo, 2006.

FERREIRA, Pinto. *Curso de direito processual civil.* São Paulo: Saraiva, 1998.

GRECO, Marco Aurélio. *Internet e direito*. 2. ed. São Paulo: Dialética, 2000.

MARCACINI, Augusto Tavares Rosa. *Direito e informática*: uma abordagem jurídica sobre criptografia. Rio de Janeiro: Forense, 2002.

MARCACINI, Augusto Tavares Rosa. *A certificação eletrônica na legislação brasileira atual.* Disponível em:< http://www.cebeji.com.br/br/novidades/artigos/index.asp?id=1424>. Acesso em: 26/3/ 2003.

MARQUES, Antônio Terêncio G. L. *A prova documental na internet*. 3. reimpressão. Curitiba: Juruá, 2008.

MENKE, Fabiano. *Assinatura eletrônica no direito brasileiro*. São Paulo: RT, 2005.

NEVES E CASTRO, Francisco Augusto das. *Teoria das provas e suas aplicações aos atos civis.* Edição atualizada por Pontes de Miranda. Campinas: Servanda, 2000.

PARENTONI, Leonardo Netto. *Documento eletrônico*: aplicação e interpretação pelo Poder Judiciário. Curitiba: Juruá, 2007.

REZENDE, Pedro Antonio Dourado de. *Entidades certificadoras, assinaturas*

eletrônicas e projetos de lei. Disponível em: <http://www1.jus.com.br/doutrina/texto.asp?id=2704>. Acesso em: 19/3/2002.

ROHRMANN, Carlos Alberto. *Curso de direito virtual.* Belo Horizonte: Del Rey, 2005.

ROVER, Aires José (Org.). *Direito, sociedade e informática*: limites e perspectivas da vida digital. Florianópolis: Fundação Boiteaux, 2000.

SANTOLIM, César Viterbo Matos. *Formação e eficácia probatória dos contratos por computador.* São Paulo: Saraiva, 1995.

TANEMBAUM, Andrew S. *Redes de computadores.* 4. ed. Trad. Vandenberg D. de Souza. São Paulo: Campus, 2003.

THEODORO JÚNIOR, Humberto. *Curso de direito processual civil*. 33. ed. vol. 1. Rio de Janeiro: Forense, 2000.

VOLPI, Marlon Marcelo. *Assinatura digital*: aspectos técnicos, práticos e legais. Rio de Janeiro: Axcel Books, 2001.

WAKAMURA, Emilio Tissato; GEUS, Paulo Lício de. *Segurança de redes em ambientes cooperativos*. 3. ed. São Paulo: Futura, 2004.

ZOCCOLI, Dinemar. Autenticidade e integridade dos documentos eletrônicos: a firma eletrônica. In: ROVER, Aires José (Org). *Direito, sociedade e informática:* limites e perspectivas da vida digital. Florianópolis: Fundação Boiteaux, 2000.