CERTIFICAÇÃO DIGITAL E SEGURANÇA

Por Marcia Benedicto Ottoni

Um sistema de documentação integralmente eletrônico, desde a formação do documento - as versões, as comunicações entre as partes, as adesões (assinaturas), incluindo o seu registro e guarda, não é apenas inexorável como promete benefícios em todos os setores da economia e da sociedade.

O processo de migração da documentação em papel para a digital está acontecendo aceleradamente. Há tempos nossos documentos são gerados em arquivos eletrônicos do tipo .doc ou .pdf ou .txt. Os contratos, os textos artísticos, os pareceres, os trabalhos em geral, são produzidos, enviados, discutidos e acertados eletronicamente. Em que momento deste processo cada um de nós interrompe a atividade digital e retoma o papel? Quando e porque um contrato tem que ser impresso? E uma petição? E uma proposta comercial? A resposta a estas perguntas indica o estágio de adesão de cada setor da economia às práticas eletrônicas.

A adesão à documentação exclusivamente eletrônica depende de uma infra-estrutura técnica e legal normatizando práticas que suportem as transações eletrônicas com técnicas eficientes de combate à insegurança própria do meio digital – vulnerabilidade dos sistemas, instabilidade, impessoalidade e imateriabilidade dos registros – técnicas capazes de minimizar as fraudes e promover relações mais seguras.

Durante esta transição, os advogados serão freqüentemente consultados sobre as conseqüências jurídicas de criar, receber, transmitir, destruir, registrar, guardar e converter cópias materiais em documentos eletrônicos. Afinal, não é a todo momento que nos movemos para um novo paradigma.

Segurança efetiva e segurança jurídica

A Internet e o mundo digital apresentam, pelas mesmas razões e na exata proporção em que trazem facilidade, risco e insegurança. O meio eletrônico é instável e vulnerável, e tem se mostrado um ambiente favorável para fraude e outros crimes afetos. Milita, ainda, pela insegurança, o fato de que a fraude digital pode ser reproduzida numa escala e ritmo que a fraude manual jamais atingiria.

O preço do conforto, da agilidade, da eficiência e assim da economia gerada com o uso da comunicação e da documentação digitais é o investimento constante e generoso na segurança. Hardwares, softwares, sistemas e serviços de segurança da informação devem ser continuamente desenvolvidos, superados, substituídos ou somados e sempre atualizados, neste esforço incessante que é fazer deste meio notoriamente instável e aberto, um ambiente seguro para instrumentalizar relações sociais, culturais e econômicas.

O sucesso do e-commerce e do e-government - a eficiência dos sistemas empresariais e a própria viabilidade da prestação eficiente dos serviços públicos - incluindo a implantação do sonhado processo judicial eletrônico, dependem de uma comunicação segura na Internet, que garanta a eficácia probatória das transações realizadas e registradas eletronicamente.

As leis e demais sistemas regulatórios precisam apoiar a eficiência desta migração. Para tanto, a lei deve integrar-se à tecnologia, os juristas e legisladores devem compreender os recursos da tecnologia e os técnicos devem desenvolver controles técnicos que atendam às necessidades regulatórias do sistema, pois, como ensina Lawrence Lessig[1], a arquitetura do software é lei no ciberespaço. De nada adiantam leis desvinculadas dos sistemas de controle, que pretendam impor condutas inexigíveis e, por vezes, sequer verificáveis.

1. CERTIFICAÇÃO DIGITAL

Por não serem presenciais nem testemunhadas, as comunicações eletrônicas causam certa estranheza e insegurança no ser humano.

Um e-mail ou uma interação na Internet podem perfeitamente comunicar a vontade de alguém. Mas o e-mail pode não ter sido enviado por aquele que nomeia a caixa postal e na mensagem, assim como a interação pode ter sido realizada de modo fraudulento, por criminosos virtuais, por meio do uso indevido da informação de acesso compartilhada. Sem ferramentas tecnológicas apropriadas, não é certo que o que se vê numa “tela” ou em outro elaborador eletrônico pode ser considerado, com razoável grau de certeza, a vontade de alguém.

Assim, embora nosso sistema preveja, a teor do artigo 107 do CC, a liberdade das formas, não existindo qualquer obstáculo legal para a validade das transações realizadas no meio eletrônico, a eficácia probatória das declarações virtuais de vontade depende de um processo autenticatório capaz de substituir o testemunho dos nossos sentidos.

Certificação Digital é uma tecnologia de segurança para as relações eletrônicas, que provê um sistema de identificação de pessoas e entidades no meio eletrônico, que combate o anonimato, a despersonalização e a insegurança em relação ao interlocutor.

PKI (Public Key Infrastruture) ou ICP (Infra-estrutura de Chaves Publicas)

PKI é a solução apresentada pela tecnologia de segurança da informação para dar segurança jurídica às comunicações e documentos eletrônicos. O objetivo das

[1] The Code and Other Laws of Ciberpace – Lawrence Lessig – Basic Books/1999 - EUA

tecnologias de PKI disponíveis é fornecer, através da Internet, meios técnicos para identificação segura de pessoas, para garantia da integridade dos registros e para o sigilo da informação no meio eletrônico.

As senhas, como se sabe, não atendem ao requisito essencial de identificação segura com relação à exigência de conhecimento e acesso exclusivo, por tratar-se de segredo necessariamente compartilhado. A PKI substitui a senha, que é uma assinatura eletrônica[2], pela assinatura digital.

Assinatura digital significa uma assinatura numérica, matemática, realizada por meio de um algoritmo, com a utilização de uma chave privada de criptografia assimétrica. A chave privada de assinatura deve ser de posse e uso exclusivos do subscritor. A chave privada não pode ser deduzida a partir da chave pública. A operação de assinatura é realizada com a chave privada, mas pode ser confirmada com a utilização da chave pública correspondente, excluindo a necessidade e assim os riscos do compartilhamento da informação, do compartilhamento de hardwares e, especialmente, compartilhamento da informação através de invasão de softwares, todos veículos que favorecem as fraudes.

A função própria da PKI é associar, com segurança, pessoas a chaves (ou outros tipos de dados), para criação de uma assinatura, permitindo a realização de negócios eletrônicos eficazes e seguros, entabulados entre partes conhecidas com utilização de comunicações eletrônicas, registrados e guardados eletronicamente.

Emissão e gerenciamento de certificados

As Autoridades Certificadoras (AC) emitem “documentos virtuais”, chamados certificados digitais. Os certificados associam pessoas a pares de chaves de criptografia assimétrica. Cada chave pública de assinatura é associada a uma pessoa ou entidade jurídica. Em conseqüência, a chave privada de assinatura correspondente à chave pública certificada também fica associada ao titular, de forma que o seu uso, dentro do prazo de validade de um certificado que não tenha sido revogado, passa a ser considerada uma prova da manifestação da vontade do titular do certificado.

Validação presencial

Para usufruir da velocidade e economia dos negócios eletrônicos, bem como das facilidades de transmissão e armazenamento das comunicações e suportes eletrônicos, abdica-se da segurança do contato físico entre as partes, corporificada na assinatura “física” dos documentos.

[2] *...as assinaturas digitais devem ser entendidas como parte da definição mais ampla de que a das assinaturas eletrônicas. Pode-se dizer que a assinatura digital é um meio de realizar uma assinatura eletrônica* - Digital Signatures - WU Stephen and others.

A identificação presencial, neste contexto, como requisito para a emissão do certificado, suportará muitas outras manifestações eletrônicas, tornando-se um instrumento importante na proteção contra fraudes e simulações de identidade no meio digital. Nem todas as relações eletrônicas, porém, precisam ser validadas por identificação presencial de terceiros. Relacionamentos pré-existentes e registros em bancos de dados podem ser suficientes para a identificação de indivíduos.

A regra de identificação do titular de um certificado é um elemento essencial de uma ICP. A identificação exigida dos indivíduos e das empresas pode ser mais ou menos "forte". Tem-se por identificação forte a identificação presencial de pessoas naturais conjugada com a apresentação de documentos.

Confiabilidade

O problema da validação da tecnologia de ICP é exatamente a confiança depositada na entidade emissora. Como saber se a entidade emissora está sendo supervisionada ou foi credenciada por alguém e se está de acordo com a legislação? Como saber se seus serviços são confiáveis e se ela permanecerá no mercado? Nas aplicações comerciais privadas, as partes freqüentemente preferem indicar diretamente uma AC a confiar numa cadeia pública de certificação. Em aplicações públicas, porém, dependemos de certificadoras digitais "institucionais" que forneçam verdadeiras identidades virtuais. Tais entidades devem ser supervisionadas e submeter-se à regulamentação e fiscalização de organismos técnicos.

Uma lista de status das ACs é uma lista emitida e divulgada pelos organismos de supervisão e/ou fiscalização, contendo informação sobre as AC ativas em determinado território e seu status em relação ao atendimento dos requisitos técnicos e jurídicos fixados na legislação. Este é o sistema adotado na Itália e em diversos países da Europa. Já o credenciamento consiste no gerenciamento direto e no rígido controle estatal da atividade de certificação digital, através de um sistema de autorização prévia e fiscalização de manutenção de funcionamento que garanta o atendimento às normas e práticas definidas nos documentos regulatórios.

Documentos regulatórios

Grandes comunidades de usuários são difíceis de gerenciar com uma única AC. A solução de PKI recomendada para grandes comunidades é co-existência de ACs, relacionando-se como uma estrutura hierárquica. Apenas o certificado da AC Raiz é auto assinado. A AC Raiz emite certificados para as ACs, Intermediárias.

A tecnologia e a atividade empregadas pelas entidades integrantes de uma PKI são regradas por normas e práticas controladas pela AC Raiz da hierarquia.

Cada AC deve publicar sua Declarações de Práticas de Certificação (DPC) e as suas Políticas de Certificados (PC). As DPCs e as PCs são documentos padronizados para facilitar a compreensão dos usuários de uma ICP, tanto os titulares de certificados

como as partes confiantes, que devem averiguar as principais regras de emissão de cada certificado, as eventuais limitações de uso e a validade do certificado antes de confiar na identificação certificada.

2. APLICAÇÕES

Certificados digitais são utilizados em de forma e em aplicações variadas. Como aplicações típicas, os certificados servem para a identificação de remetentes e sigilo de conteúdo de correio eletrônico, para autenticação de pessoas e servidores ou endereços na Internet, para sigilo das comunicações e transações eletrônicas na *web* e para assinatura digital e confidencialidade dos documentos eletrônicos.

Correio eletrônico

A aplicação de maior sucesso na Internet é o e-mail. A comunicação eletrônica rápida, eficiente e barata, encaminhada diretamente para os arquivos eletrônicos e demais ferramentas de trabalho faz parte de nossa vida profissional e pessoal. O correio eletrônico tornou-se indispensável. O e-mail, porém, funciona como uma porta para o perigo eletrônico, para os ataques de serviço dos provedores, para a disseminação de vírus e para o roubo de informação, servindo, enfim, como via de invasão aos sistemas. A utilização do e-mail hoje está condicionada a utilização de sistemas proteção que associem os recursos disponíveis: hardwares, softwares e demais aplicativos.

A assinatura digital da correspondência eletrônica é um aplicativo de segurança da fonte e do conteúdo da mensagem. A assinatura com a chave privada permite a identificação segura do remetente, obstando o envio de mensagens maliciosas anônimas e a utilização fraudulenta de identidade, e garante, matematicamente, a integridade do conteúdo.

O uso comercial indiscriminado do e-mail também atenta contra a utilização deste aplicativo. A quantidade de mensagens indesejáveis ou não solicitadas que trafega hoje na *web* ameaça o sistema de colapso. O spam está se transformando num obstáculo ao funcionamento da Internet, superlotando as rotas de comunicação, a infra-estrutura dos provedores e as caixas postais dos usuários.

A certificação digital serve como instrumento no combate a esta praga moderna, na medida em que as aplicações e os sistemas passem a exigir, como vem sendo discutido em alguns segmentos e sugerido em alguns projetos de lei, a identificação do remetente para processar o encaminhamento da mensagem.

A certificação digital serve, ainda, como instrumento de sigilo nas comunicações e registros eletrônicos. A utilização da Internet, esta rede pública de transmissão de dados a tão baixo custo, potencializa a comunicação de negócios, mas coloca a informação sob o risco de interceptação, roubo e adulteração. A utilização de chaves públicas para criptografia das mensagens ou dos documentos anexos nos e-mails garante o sigilo da comunicação e do documento, impedindo o acesso e o roubo da informação.

Estes recursos podem colaborar com a manutenção do uso comercial deste aplicativo tão caro e essencial no nosso dia-a-dia.

Navegação e interatividade - browser

A outra aplicação de sucesso na Internet é a navegação interativa das transações on-line. A segurança dos mecanismos de realização de negócios on-line – operações financeiras, operações comerciais, depende de autenticação dos usuários para permissão de acesso. Também os endereços web, as máquinas servidoras, devem identificar-se, na qualidade de fornecedores, perante os usuários. Por fim, os provedores de serviço respondem pelo sigilo da informação que coletam.

A autenticação do usuário garante a segurança do sistema e da informação. Os usuários, clientes, fornecedores, funcionários devem autenticar-se nos sistemas para acessá-los e tal autenticação deve ser segura o suficiente para comprovar o seu acesso. A certificação digital provê esta autenticação de pessoas e servidores. A certificação não altera qualquer norma do direito do consumidor, apenas instrumentaliza o consumidor para verificar a identidade do fornecedor pela titularidade do endereço web, fornece canal seguro de transmissão de dados e instrumentaliza a prova eletrônica.

Os sistemas de arrecadação e controle de tributos, por exemplo, estão sendo informatizados no mundo todo. A certificação digital atende bastante bem às necessidades de autenticação dos sistemas tributários de registro e pagamento. Documentos virtuais de identificação de contribuintes tem sido uma das primeiras aplicações de certificação digital implementada em diversos países. No Brasil, de braços com a Receita Federal, as fazendas públicas estaduais e municipais estão informatizando e regulamentando seus sistemas eletrônicos de registro e arrecadação[3].

O internet banking, como se sabe, é instrumento de eficiência econômica incomensurável para as instituições financeiras. A autenticação do usuário do netbanking é outra aplicação interativa de Internet que depende de identificação forte de usuários e registro eficaz das transações realizadas on-line.

[3] O Estado de Pernambuco, por exemplo, implantou um sistema de registros digitais do ICMS. Os documentos enviados a SEFAZ de Pernambuco devem ser assinados digitalmente pelo responsável pelo estabelecimento ou pelo contabilista indicado pela empresa, com chaves certificadas na ICP-Brasil,. LEI Nº 12.333, de 23 de janeiro de 2003. *Estabelece a escrituração fiscal digital para contribuintes do ICMS.* PORTARIA SF Nº 073, de 30.05.2003. Outras fazendas estaduais estão implementando sistemas semelhantes.

Documentos eletrônicos

Não há diferença ontológica entre o documento tradicional e o documento eletrônico. Ambos representam um ato. A estreita ligação entre o papel e a própria noção de documento decorre, em parte, do fato de que no mundo físico a existência do documento depende do suporte de papel. O documento em papel está preso ao seu suporte original. A destruição do suporte significa a destruição do documento.

No ciberespaço é diferente. O documento é uma seqüência de bits, intangível, que pode ser infinitamente reproduzida. A fixação em variados suportes não gera "cópias". Não há cópias no mundo virtual, apenas vias, em diferentes suportes. Original e cópias são indistintos. Uma das razões da insegurança que tem dificultado a ampla adoção das transações eletrônicas é a facilidade com que, por não estarem presos aos suportes em que são registrados, os documentos eletrônicos podem ser interceptados, acessados e alterados.

Para ter força probatória, o documento não pode ser passível de adulteração. O documento com eficácia probatória é autêntico: conteúdo integro, origem ou fonte e autor identificáveis. Uma ICP deve prover sistemas de integridade e identificação capazes e suficientes para fazer esta prova.

Assinaturas Digitais

Outro obstáculo para a plena utilização do documento eletrônico nos negócios tem sido a impossibilidade de subscrevê-los. O ato de lançar no papel o nome, a firma ou sinal, de punho próprio, tem um valor importante no nosso sistema jurídico. O ato de assinar comprova o recebimento, atesta a ciência, atesta a obrigação. O signatário se dá por citado. O signatário se obriga aos termos fixados no documento e pode ser forçado a cumpri-los. A assinatura manual autentica o documento, não atesta apenas a identidade, mas também atesta a vontade do signatário.

Assinaturas são sinais distintivos, únicos e exclusivos de uma pessoa, que permitem identificar a autoria do documento. Graças a esta exclusividade, a assinatura manuscrita aposta sobre o papel atesta a autoria do documento. A assinatura manuscrita não pode ser reutilizada, copiada ou reaproveitada em outro documento, tentativas de reutilização destroem o próprio original.

Mas não basta simplesmente colocar uma "marca digital" no documento eletrônico para autenticá-lo, porque esta marca, ao contrário da assinatura manual, pode ser facilmente copiada e fraudulentamente reproduzida. É preciso, em primeiro lugar, garantir que a posse ou conhecimento e o uso desta "marca" seja de exclusividade do subscritor. Isto é um requisito essencial em qualquer sistema de "assinatura eletrônica", ainda que ao custo de impor ao usuário sérias obrigações de proteção e guarda do repositório de assinaturas. Apenas a exclusividade na posse e uso do instrumento

pode caracterizar a marca pessoal e satisfazer o atributo que a assinatura manuscrita provê ao documento em papel e ao direito.

Juridicamente, se o documento for íntegro para comprovar a declaração de vontade do signatário, não há porque distinguir a assinatura manuscrita de outro sinal que permita, com significativo grau de certeza, identificar o sujeito que o realizou. Qualquer instrumento capaz de conferir razoável certeza sobre a identidade do autor e a integridade do conteúdo de um documento servirá ao objetivo de assegurar-lhe a autenticidade, como faz a assinatura manual.

A assinatura digital deve integrar uma marca única e pessoal do autor à seqüência de bits que é o documento, para obter efeito semelhante à assinatura no papel. O resultado matemático entre a marca pessoal exclusiva e o conteúdo do documento autentica a autoria e a integridade do documento eletrônico.

O ato de assinar, ou a cerimônia de assinaturas tem um conteúdo social que não deve ser desprezado. Para equipararem-se realmente as assinaturas eletrônicas às manuscritas, o ato de assinar eletronicamente deve ter o mesmo significado e efeito para o signatário que o ato lançar uma assinatura de punho próprio.

3. LEGISLAÇÃO

Assinaturas digitais, contratos de licenças e serviços associados aos sistemas digitais terão um papel chave na atividade jurídica.

Embora haja um consenso jurídico de que as leis não devem contemplar tecnologias específicas, uma vez que as tecnologias são superadas ou alteradas com muito mais rapidez do que são aprovadas as leis, e de que as normatizações devem permanecer em regulamentos - normas de menor nível e assim mais fáceis de serem alteradas, o fato é que a adoção de lei regulamentando a utilização da criptografia assimétrica organizada em infra-estrutura de chaves públicas (PKI), fixando padrões obrigatórios de controles técnicos e procedimentais, tem se mostrado, até agora, a única alternativa capaz de prover ao documento eletrônico os mesmos efeitos da assinatura no documento tradicional, equiparando-lhes, de fato, os efeitos legais.

Seja através de lei, seja em nível regulamentar, a utilização deste recurso matemático para identificação de usuários de meios eletrônicos - pares de chaves criptográficas associados a pessoas[4] - normatizado em infra-estruturas públicas que regulam a tecnologia e os procedimentos confiáveis para a emissão de certificados digitais vinculando chaves de

[4] However, a public- and private-key pair has no intrinsic association with any person; it is simply a pair of numbers. An additional mechanism is necessary to associate reliably a particular person or entity to the key pair. If public-key cryptography is to serve its intended purposes, it needs to provide a way to make keys available to a wide variety of persons, many of whom are not known to the signatory, where no relationship of trust has developed between the parties. To that effect, the parties involved must have a degree of confidence in the public and private keys being issued. Guide to Enactment of the UNCITRAL Model Law on Electronic Signatures (2001) – item 45 .

assinatura a pessoas, está sendo adotada em inúmeros países, tanto na Europa como nas Américas.

Diretiva Européia 93/99

A Diretiva adotou uma regulamentação tecnologicamente neutra, afastando menções às *chaves criptográficas de assinatura*, que indicam a adoção da tecnologia da criptografia assimétrica, substituindo-as pelos conceitos genéricos de *dados de criação de assinatura* e *dispositivos de criação* e *dispositivos de verificação de assinaturas*.

As regulamentações da Diretiva ou das Leis nacionais de transposição, no entanto, disciplinam o uso da criptografia assimétrica que é, até agora, a única tecnologia conhecida que atende aos requisitos de PKI impostos pela Diretiva. A utilização de nomenclatura genérica pela Lei, porém, permite que novas tecnologias possam ser assimiladas nos sistemas de infra-estruturas que estão sendo implementados hoje.

Certificado Qualificado e Assinatura Digital Avançada

Apenas uma assinatura eletrônica altamente padronizada será considerada equivalente a uma assinatura manual em qualquer país da comunidade européia. Os Anexos da Diretiva indicam os requisitos suficientes da prestação de serviços de certificação digital para caracterizar tecnicamente a assinatura equiparável à manuscrita.

O sistema de identificação preconizado na Diretiva institui um tipo de assinatura digital diferenciado pela tecnologia utilizada - Assinaturas Eletrônicas Avançadas[5], e um certificado com eficácia legal pré-definida - o Certificado Qualificado[6]. Os certificados qualificados e as assinaturas eletrônicas avançadas têm por objetivo a obtenção de um nível de segurança harmonizado na comunidade européia, que agilize e incentive o livre trânsito dos negócios nos países da comunidade, permitindo o relacionamento comercial eletrônico e a interoperabilidade transfronteiriça.

Para tanto, os Estados-Membros devem instituir um sistema adequado de controle de prestadores de serviços de certificação estabelecidos no seu território que procedem à emissão de certificados qualificados destinados ao público.

A necessidade de desenvolvimento e estudo de padões levou a criação do EESSI – European Eletronic Signatures Standartization Iniciative, na qualidade de um corpo técnico para padronização dos recursos de PKI na Europa. O EESSI é uma iniciativa

[5] "Assinatura eletrônica avançada", uma assinatura eletrônica que obedeça aos seguintes requisitos: a) Estar associada inequivocamente ao signatário;b) Permitir identificar o signatário;c) Ser criada com meios que o signatário pode manter sob seu controlo exclusivo e d) Estar ligada aos dados a que diz respeito, de tal modo, que qualquer alteração subsequente dos dados seja detectável; (art. 2º – Definições – item 2).

[6] Os Estados-Membros assegurarão que as assinaturas eletrônicas avançadas baseadas num certificado qualificado e criadas através de dispositivos seguros de criação de assinaturas: a) Obedecem aos requisitos legais de uma assinatura no que se refere aos dados sob forma digital, do mesmo modo que uma assinatura manuscrita obedece aqueles requisitos em relação aos dados escritos, e b) São admissíveis como meio de prova para efeitos processuais (art. 5.1 – efeitos legais das assinaturas).

aberta que congrega a indústria, revendedores, autoridades públicas e especialistas, técnicos e jurídicos, formada por solicitação da Comissão e trabalhando com o respaldo do Parlamento Europeu.

4. ICP-BRASIL

A ICP-Brasil apresenta grande influência do sistema europeu, embora a nomenclatura utilizada na MP 2200-02, nas Resoluções e nas demais normativas da ICP-Brasil, utilize os nomes empregados pela indústria da tecnologia americana. Os termos *Autoridade Certificadora* (AC) e *Autoridade de Registro* (AR) não são utilizados na regulamentação européia.

O Modelo da ICP-Brasil

O Brasil adotou a tecnologia de certificação digital implementando uma infra-estrutura de chaves públicas hierarquizada, fortemente centralizada e vinculada ao Governo Federal, a ICP-Brasil[7].

Um Comitê Gestor indicado pela Presidência e Ministérios relacionados exerce a função de autoridade gestora de políticas da ICP-Brasil. Ao Comitê compete adotar as medidas necessárias e coordenar a implantação e o funcionamento da ICP-Brasil; estabelecer a política de certificação e as regras operacionais da AC-Raiz e estabelecer os critérios e as normas para o credenciamento das Autoridades Certificadoras - AC, das Autoridades de Registro - AR e dos demais prestadores de serviço de suporte da ICP-Brasil.

Optou-se pelo sistema da AC-Raiz[8], valorizando o aspecto da interoperabilidade tecnológica que é obtida com a ampla distribuição de uma chave única pública, da AC-Raiz, em browsers e em outros aplicativos, por meio de um certificado raiz auto-assinado que contém a chave correspondente à chave com a qual AC-Raiz assinará os certificados das demais entidades credenciadas, criando assim uma cadeia de reconhecimento até o usuário, titular do certificado.

A Autoridade Certificadora Raiz da ICP-Brasil é o Instituto Nacional de Tecnologia da Informação (ITI)[9], autarquia pertencente à administração pública federal, ligado à Casa Civil da Presidência da República. [10]

---

[7] Implementada pela MP 2.200-02/2001.

[8] 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 – MP 2200-02

[9] Conforme art. 7º. da MP 2200-02

[10] Decreto 4.566 de 1º de janeiro de 2003

A AC-Raiz brasileira determina as regras operacionais técnicas das demais entidades da ICP e exerce a função de órgão fiscalizador do cumprimento e manutenção dos procedimentos e normas, auditorando as práticas das entidades que se candidatam a atuar nesta hierarquia pública, para deferir ou negar o pedido de credenciamento que autoriza a emissão de certificados na ICP-Brasil.

A ICP-Brasil é formada através um sistema de credenciamento voluntário das entidades prestadoras de serviços, mas se enquadra na espécie de legislação em que a fiscalização e supervisão da conformidade aos requisitos técnicos significam o controle detalhado e estrito da operação das AC credenciadas pela AC-Raiz, incluindo autorização prévia para funcionamento.

****

A MP 2200-02 instituiu uma PKI de âmbito nacional com aplicabilidade irrestrita e normatizou a eficácia destas assinaturas digitais. A ICP-Brasil não ficou limitada ao âmbito da administração pública, embora esteja claramente inserida no contexto da política de segurança e divulgação da informação, mas, ingressando no campo da inicitiva privada, assumiu o objetivo de estancar a insegurança jurídica geral, disciplinando sobre a validade dos documentos eletrônicos.

Nos termos de seu artigo art. 1º, a finalidade da Medida Provisória é garantir a autenticidade, integridade e validade jurídica dos documentos e aplicações que utilizem certificados digitais.

Certamente não é a norma jurídica que garante integridade e autenticidade dos documentos. É o procedimento de identificação e associação de titulares de certificados adotado e a segurança do sistema e da tecnologia dos gerenciadores dos certificados que farão isto. Quem garante a autenticidade e a integridade do documento eletrônico é o conjunto dos sistemas e dispositivos de criação e verificação de assinaturas apropriadas e dos procedimentos adequados para a operação de uma Infra-estrutura de Chaves Públicas.

Para tanto, está legalmente instituida esta PKI nacional, com estrita regulamentação e forte fiscalização do governo sobre os sistemas tecnológicos reconhecidos como aptos e confiáveis.

Como os requisitos técnicos e os procedimentos da ICP-Brasil respeitam os requisitos mínimos fixados na Diretiva, o certificado emitido na ICP-Brasil é um Certificado Qualificado. O enquadramento nestes padrões pode colocar o Brasil num contexto de interoperabilidade internacional, essencial à viabilidade da atividade eletrônica, que não respeita as tradicionais barreiras territoriais em que se funda o direito moderno.

***