UNIVERSIDADE ESTADUAL VALE DO ACARAÚ
ESCOLA SUPERIOR DE MAGISTRATURA DO CEARÁ
CURSO DE ESPECIALIZAÇÃO EM ADMINISTRAÇÃO JUDICIÁRIA

Francisco Moacir da Silva Medeiros Júnior

CERTIFICAÇÃO DIGITAL NO PODER JUDICIÁRIO DO ESTADO DO CEARÁ

FORTALEZA – 2008

CERTIFICAÇÃO DIGITAL NO PODER JUDICIÁRIO DO ESTADO DO CEARÁ

Monografia apresentada à Universidade Estadual Vale do Acaraú como requisito parcial para obtenção do título de Especialista em Administração Judiciária.

Orientador: Prof. Dr. Edilson Baltazar Barreira Júnior

Fortaleza – 2008

Francisco Moacir da Silva Medeiros Júnior

CERTIFICAÇÃO DIGITAL NO PODER JUDICIÁRIO DO ESTADO DO CEARÁ

Monografia apresentada à Universidade Estadual Vale do Acaraú como requisito parcial para obteção do título de Especialista em Administração Judiciária.

Monografia aprovada em: 08 / 08 / 2008

Orientador: _____
Prof. Dr. Edilson Baltazar Barreira Júnior (ESMEC)

1º Examinador: _____
Prof. MSc Flávio José Moreira Gonçalves (ESMEC)

2º Examinador: _____
Prof. José de Anchieta Silveira

Coordenador do Curso:

_____
Prof. Dr. Edilson Baltazar Barreira Júnior (ESMEC)

RESUMO

Esforços para elevar os níveis de eficiência, eficácia e qualidade da prestação jurisdicional tem sido efetudas pelo Poder Judiciário através da virtualização dos processos e acesso às informações disponibilizadas pelos órgãos da administração pública de forma eletrônica. Sistemas e procedimentos totalmente informatizados implicam na utilização de mecanismos capazes de prover a segurança das operações realizadas garantindo a autenticidade e integridade de documentos e transações através da identificação inequívoca de seus participantes. A Certificação Digital é um dos mecanismos utilizados para garantir a identidade digital de um indivíduo ou equipamento, através de um documento eletrônico seguro denominado Certificado Digital, que permite ao seu portador executar operações de assinatura de documentos e acesso a sistemas como o Renajud, permitirá a penhora on line de veículos, e o InfoJud, que permitirá acesso a Receita Federal para verificar informações sobre os contribuintes. O Conselho Nacional de Justiça, através de sua Resolução nº 12 de 11 de setembro de 2007, recomendou que os Tribunais de Justiça regulamentem e efetivem o uso de formas eletrônicas de assinatura. Este trabalho teve por objetivo demonstrar o funcionamento da tecnologia de certificação digital, bem como propor a forma como poderá ser regulamentada no Poder Judiciário do Estado do Ceará.

Palavras-chave: Poder Judiciário do Estado do Ceará. Certificação Digital Segurança da Informação.

LISTA DE ILUSTRAÇÕES

SUMÁRIO

1. INTRODUÇÃO

A utilização da informática e da comunicação de dados através da Internet para a troca de mensagens e documentos entre cidadãos, governo e empresas constitui-se em uma realidade inequívoca e permeia todas as atividades cotidianas das pessoas.

A elaboração de um sistema que possibilite a adoção de documentos integralmente eletrônicos, desde a sua formação, permitindo o gerenciamento de 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.

A adesão à prática das transações eletrônicas e o uso da documentação exclusivamente eletrônica depende de uma infra-estrutura técnica e legal normatizando procedimentos através de técnicas eficientes de combate à insegurança própria do meio digital como a vulnerabilidade dos sistemas, instabilidade, impessoalidade e imateriabilidade dos registros, técnicas essas capazes de minimizar as fraudes e promover relações mais seguras.

Este trabalho pretende pretende analisar a infra-estrutura necessária para prover os mecanismos de segurança capazes de garantir autenticidade, confidencialidade e integridade às informações eletrônicas através do uso da certificação digital.

Para tanto, o trabalho foi dividido em quatro capítulos. O primeiro capítulo preocupa-se em tecer considerações acerca do conceito do documento físico tradicional em papel e o estabelecimento de um comparativo com o documento eletrônico.

O segundo capítulo trata dos fundamentos das técnicas de criptografia e as funcionalidades decorrentes de sua aplicação, como a assinatura digital, cujas técnicas são esseciais para garantir a segurança das informações armazenadas e trafegadas em meio digital e trazer ao documento eletrônico os elementos capazes de lhe atribuir eficácia probante.

O terceiro aborda a infra-estrutura de Chaves Públicas e a Certificação Digital que estabelecem uma tecnologia de segurança para as relações eletrônicas ao prover um sistema de identificação de pessoas e entidades no meio digital, que combate o anonimato, a despersonalização e a insegurança em relação ao

interlocutor. Neste capítulo foi mostrada a estrutura da ICP-Brasil e seus aspectos técnicos e legais.

O quarto e último capítulo discorre sobre as aplicações da certificação digital no Poder Judiciário do Estado do Ceará e propõe uma regulamentação para seu uso.

2. DOCUMENTO TRADICIONAL E DOCUMENTO ELETRÔNICO

A Certificação Digital constitui o mecanismo mais seguro, definido em lei, para prover a presunção de veracidade dos documentos eletrônicos.

Neste sentido, este capítulo propõe-se a esclarecer os conceitos que cercam o documento físico tradicional, de modo que seus elementos sejam compreendidos, e estabelecer um paralelo com o documento eletrônico, especificando os requisitos para que possa alcançar validade e eficácia jurídica.

2.1. Documento Tradicional

O termo documento tem sua origem derivada do latim *documentum*, que por sua vez deriva do verbo *docere*, cujo significado pode ser traduzido como ensinar, demonstrar[1]. Essa definição indica a característica primordial de um documento que é sua finalidade de transmitir informações.

A disseminação das informações tornou-se possível graças a utilização de materiais resistentes que suportassem o documento, como pedra, cerâmica, papiro e, posteriormente, o papel, permitindo sua portabilidade e reprodução.

O documento tradicional ou físico, portanto, é aquele cuja principal característica está na vinculação a um suporte físico, ou seja, a união inseparável de seu conteúdo a algo material ou corpóreo.

Segundo o Novo Dicionário da Língua Portuguesa[2] a palavra "documento" possui o seguinte significado:

1. Qualquer base de conhecimento, fixada materialmente e disposta de modo que se possa utilizar para consulta, estudo, prova etc.
2. Escritura destinada a comprovar um fato; declaração escrita, revestida de forma padronizada, sobre fato(s) ou acontecimento(s) de natureza jurídica.
3. Qualquer registro gráfico.

Para Michaelis em seu Moderno Dicionário da Língua Portuguesa[3], a palavra "documento" possui a seguinte definição:

---

[1] Verbete *documento* disponível em: http://pt.wikipedia.org/wiki/Wiki. Acesso em 07.07.200às 09:00.
[2] FERREIRA, Aurélio Buarque de Holanda. **Novo Dicionário da Língua Portuguesa**. 2. Ed. Rio de Janeiro: Nova Fronteira, 1986.p. 605.
[3] **Dicionário Michaelis**. Acessado através do programa Babylon versão 7.0 em 07.07.2008.

1. Direito: Instrumento escrito que, por direito, faz fé daquilo que atesta; escritura, título, contrato, certificado, comprovante.
2. Escrito ou impresso que fornece informação ou prova.
3. Qualquer fato e tudo quanto possa servir de prova, confirmação ou testemunho.

As definições citadas indicam as características inerentes ao documento tradicional. O documento possui um suporte físico que é o material do qual o documento é formado (papel, papiro,cera, pergaminho, metal) e que permite fixar a representação de uma informação através da escrita, simbolos, gravuras, mapas etc.

Outras definições que fortalecem a associação do conteúdo do documento ao seu suporte físico podem ser encontradas na doutrina jurídica. Para Chiovenda[4], documento seria toda a *"representação material destinada a reproduzir determinada manifestação do pensamento"*. Humberto Theodoro Júnior[5] define documento como prova documental, como sendo *"em sentido estrito, quando se fala de prova documental, cuida-se especificamente de documentos escritos, que são aqueles em que o fato vem registrado através da palavra escrita, em papel ou outro material adequado"*.

A vinculação de um documento tradicional ao seu suporte físico impossibilita sua reprodução sem a destruição do documento original. As reproduções do conteúdo serão relizadas em outro suporte físico através de uma imitação, portanto não será idêntico ao original.

2.2. A Força Probante do Documento

Para que um documento possa ser considerado como elemento de prova é necessário que tenha autoria identificável (autenticidade), que não possa ser alterado de modo imperceptível (integridade) e o momento em que foi criado (tempestividade). Esses elementos, portanto, são os requisitos básicos que deve conter um documento para servir como prova.

---

[4] CHIOVENDA *apud* GANDINI, João Agnaldo Donizeti; SALOMÃO, Diana Paola da Silva et al. **A segurança dos documentos digitais**. Jus Navigandi, Disponível em: http://jus2.uol.com.br/doutrina/texto.asp?id=2677. Acesso em: 07.07.2008 às 09:00.

[5] THEODORO, Humberto Jr. **Curso de Direito Processual Civil**. 44 ed. Rio de Janeiro. Forense. 2006.p.486.

A autenticidade pode ser definida como a certeza de que o documento provém do autor nele indicado[6]. Autor do documento é a pessoa a quem se atribui a sua formação, isto é, a quem se atribui a sua paternidade. O artigo 371, do Código de Processo Civil diz que: "*Reputa-se autor do documento particular: I - aquele que o fez e o assinou; II - aquele, por conta de quem foi feito, estando assinado; III - aquele que, mandando compô-lo, não o firmou, porque, conforme a experiência comum, não se costuma assinar, como livros comerciais e assentos domésticos*".

O principal meio de comprovação da autoria de um documento se dá por meio da assinatura. No documento tradicional, a assinatura é aposta no meio físico em que está registrada a informação. Como o conteúdo e o suporte no documento tradicional são inseparáveis, e uma vez que essa marca é também inseparável, a assinatura permite validar o conteúdo ali fixado.

A integridade é a propriedade daquilo que se apresenta ileso, intacto. Um documento pode ser considerado integro quando não houve alterações em seu conteúdo após sua criação. O suporte material do documento, portanto, deve ser indelével, não sendo possível qualquer tipo de adulteração, desagregação ou cancelamento sem que possa ser percebido.

A tempestividade de um documento é utilizada para verificar o momento em que foi produzido através da análise do suporte físico em que foi fixado seu conteúdo, com a utilização de técnicas apropriadas[7]. A tempestividade visa garantir que um documento não tenha sido produzido para comprovação de um fato anterior a ele.

2.3. Evolução do Documento Tradicional

O progresso alcançado pela ciência implica em uma constante mudança de hábitos e comportamentos nas pessoas e organizações. Os novos relacionamentos e procedimentos ocasionados por estas mudanças induzem ao aparecimento de novas relações jurídicas, ou novos fatos jurídicos a serem objeto de regulação por

---

[6] SANTOS, Moacyr Amaral *apud* MARCACINI, Augusto Tavares Rosa. **Documento Eletrônico como Meio de Prova**. Disponível em: http://www.infodireito.com.br/info/index.php?option=com_content&task=view&id=44&Itemid=42. Acesso em: 07.07.2008 às 15:00.

[7] GANDINI, João Agnaldo Donizeti; SALOMÃO, Diana Paola da Silva et al. **A segurança dos documentos digitais**. Jus Navigandi, Disponível em: http://jus2.uol.com.br/doutrina/texto.asp?id=2677. Acesso em: 07.07.2008 às 09:00.

parte do Direito. A velocidade da evolução das tecnologias de informação e comunicação alterou de forma significativa o modo de vida em sociedade.

O futuro da justiça depende fortemente da evolução da informática, pois, sem modernização e adequação tecnológica, o Judiciário não suportará o avanço da demanda social.

Segundo o levantamento feito pela ministra Ellen Gracie Northfleet[8], no Supremo Tribunal Federal, 70% do tempo gasto no processo é consumido em burocracia, ou seja, utilizando sistemas para cadastrar as partes, registrar movimentações, anotar que o advogado levou o processo em carga, anotar que o advogado trouxe o processo de volta, elaborar intimação e mandado para o oficial de Justiça. Este tempo foi denominado pela ministra Ellen de tempo neutro. Em seu estudo a ministra conclui que somente em 30% do tempo gasto no processo é utilizado pelos operadores para a efetiva prestação jurisdicional.

A busca de novas alternativas aos documentos tradicionais e sua migração para um documento eletrônico manipulado pelas tecnologias atualmente disponíveis trarão ganhos com custo, transporte, armazenamento e segurança das informações que se deja registrar.

Os custos relacionados com o documento tradicional estão diretamente ligados à quantidade de informação que se quer registrar. Os gastos para aquisição do suporte sobre o qual se assentará a informação (principalmente papel). Além disso, o custo ecológico do consumo de toneladas de papel trazem sérios prejuízos ao meio ambiente com a derrubada de florestas, emissão de poluentes na atmosfera, poluição de águas e geração de lixo.

A necessidade da criação de novas alternativas tecnológicas que permitam o uso racional dos recursos naturais vem ao encontro do novo modelo de organização ecologicamente sustentável proposto por Capra[9]:

> A meta central da teoria e da prática econômicas atuais – a busca de um crescimento econômico contínuo e indiferenciado – é claramente insustentável, pois a expansão ilimitada num planeta finito só pode levar a uma catástrofe. Com efeito, nesta virada de século, já está mais do que evidente que nossas atividades econômicas estão prejudicando a biosfera e a vida humana de tal modo que, em pouco tempo, os danos poderão tornar-se irreversíveis. Nessa precária situação, é essencial que a humanidade

[8] TEJADA,Sérgio. **Só a Tecnologia Reduz Custos e Agiliza os Processos**. Disponível em: http://www.serpro.gov.br/imprensa/publicacoes/Tema/tema_190/materias/entrevista/. Acesso em 08.07.2008 às 13:00.

[9] CAPRA, Fritjof. **As Conexões Ocultas**. São Paulo. Pensamento-Cultrix. 2002.p.157.

> reduza sistematicamente o impacto das suas atividades sobre o meio ambiente natural.

O Poder Judiciário do Estado do Ceará consumiu no mês de julho/2008 a quantidade de 6.726 resmas de papel A4 totalizando 3.363.000 folhas. Somente o custo com papel foi orçado em R$ 58.919,76. O projeto para implantação dos serviços de impressão através de empresas terceirizadas levou o Departamento de Informática a realizar um estudo onde foi estimado em R$ 0,04 (quatro centavos) o custo médio para reproduzir uma página. Tomando-se por base o mês de julho de 2008, portanto, o gasto total de impresão, incluindo o papel e os serviços, girou em torno de R$ 193.439,76.

O transporte dos documentos físicos implicam em gastos elevados e problemas de manuseio e segurança. Segundo dados do Supremo Tribunal Federal[10], tramitaram 680 toneladas de papel em recurso extraordinário no ano de 2006. A maior parte destes documentos não são sequer analisados, pois o Supremo somente examina matérias jurídicas de Direito Constitucional. O grande volume que existe nesse processo é matéria de prova, contendo informações sobre audiências e transcrição de depoimentos.

A armazenamento de enormes quantidades de documentos tem sido um problema tão grande quanto a própria quantidade de documentos sendo gerada. Os espaços para sua guarda são rapidamente exauridos. A catalogação, acesso e preservação destes documentos são complexos e de custo elevado. O simples deslocamento de um processo em um arquivo público pode torná-lo praticamente inacessível.

Diante das demandas impostas pela evolução da sociedade os documentos tradicionais em meio físico evoluíram para o formato eletrônico mantendo sua função básica de registro fiel de um fato ou informação e seu caráter probatório.

Um conceito mais amplo de documento foi proposto por Marcacini:

> A característica de um documento é a possibilidade de ser futuramente observado; o documento narra, para o futuro, um fato ou pensamento presente. Daí ser também definido como prova histórica. Diversamente, representações cênicas ou narrativas orais, feitas ao vivo, representam um fato no momento em que são realizadas, mas não se perpetuam, não registram o fato para o futuro. Se esta é a característica marcante do documento, é lícito dizer que, na medida em que a técnica evolui permitindo registro permanente dos fatos sem fixá-lo de modo inseparável em alguma

[10] TEJADA,Sérgio. **Só a Tecnologia Reduz Custos e Agiliza os Processos**. Disponível em: http://www.serpro.gov.br/imprensa/publicacoes/Tema/tema_190/materias/entrevista/. Acesso em 08.07.2008 às 13:00.

> coisa corpórea, tal registro também pode ser considerado documento. A tradicional definição de documento enquanto coisa é justificada pela impossibilidade, até então, de registrar fatos de outro modo, que não apegado de modo inseparável a algo tangível[11].

2.4. O Documento Eletrônico

Os elementos básicos que compõem e informam o documento tradicional podem ser ampliados para fundamentar o conceito de um documento que seja formado sobre uma base material distinta, qual seja o meio eletrônico. Giannantonio, conceitua o documento eletrônico, ou documento informático, como "o documento produzido pelo computador eletrônico. Distinguem-se documentos eletrônicos stricto sensu, memorizados em forma digital e não perceptíveis ao homem se não por meio do computador, e documentos eletrônicos lato sensu, isto é, todos os documentos formados pelo computador mediante dispositivos de saída"[12].

Este trabalho utilizará o conceito de documento eletrônico no sentido estrito, ou seja, o documento codificado por meio de dígitos binários, perceptíveis somente através do uso de computador em conjunto com a utilização de um programa (software) adequado.

O documento eletrônico está dissociado do suporte físico no qual está armazenado. No documento tradicional temos o conceito de documento original e suas cópias que não possuem as mesmas propriedades do original. No meio eletrônico a sequencia de bits que compõe o documento pode ser reproduzida mantendo-se exatamente as mesmas características, ou seja, todas as reproduções do documento eletrônico serão idênticas independente do local de armazenamento. No documento eletrônico, portanto, os elementos necessários para sua validação devem estar vinculados ao conteúdo, e não ao suporte, como ocorre no documento tradicional onde há a inseparabilidade entre conteúdo e suporte.

A informação em formato digital posui a característica de ser facilmente alterável, e consequentemente suscetível a intervenções não autorizadas (perda, adulteração e destruição), degradação física e obsolescência tecnológica (hardware, software e formatos), o que compromete sua qualidade e integridade.

---

[11] MARCACINI, Augusto Tavares Rosa. **Documento Eletrônico como Meio de Prova**. Disponível em: http://www.infodireito.com.br/info/index.php?option=com_content&task=view&id=44&Itemid=42. Acesso em: 07.07.2008 às 15:00.

[12] GIANNANTONIO, E. Manuale *apud* TRUJILLO, Elcio. **O Mercosul e a documentação eletrônica**. Disponível em: www.senado.gov.br/web/cegraf/ril/Pdf/pdf_135/r135-22.pdf. Acesso em 08.07.200às 18:00.

A evolução tecnológica permitiu a criação de mecanismos, procedimentos e práticas para assistir às organizações e apoiá-las a criarem e manterem documentos eletrônicos integros, autênticos, acessíveis e preserváveis.

O documento eletrônico apenas terá eficácia probante se atender às mesmas exigências demandadas do documento tradicional, ou seja, se for possível a verificação da autenticidade, integridade e tempestividade. A garantia do atendimento a essas exigências se dá por meio da utilização da criptografia, assinatura digital, certificação digital e a criação de uma infra-estrutura de chaves públicas que serão detelhados nos capítulos a seguir.

3. CONCEITOS DE CRIPTOGRAFIA E ASSINATURA DIGITAL

Este capítulo aborda os fundamentos e técnica de criptografia e os serviços por ela oferecidos, como a assinatura digital, cujas técnicas são primordiais para garantir a segurança das informações armazenadas e trafegadas em meio digital e trazer ao documento eletrônico os elementos capazes de lhe atribuir eficácia probante.

3.1. Criptografia

A segurança de uma informação em meio digital está ligada a certeza de que as informações serão acessadas somente por pessoas autorizadas. As técnicas de criptografia são utilizadas "esconder/ocultar" de forma embaralhada as informações sigilosas[13].

A palavra criptografia é derivada do grego *kryptós* que significa escondido, e *gráphein* que significa escrita. A criptografia pode ser definida como o estudo dos princípios e técnicas pelas quais a informação pode ser transformada da sua forma original, através de um processo de cifragem, para outra ilegível, de forma que possa ser conhecida, através do processo de decifragem, apenas por seu destinatário, o que a torna difícil de ser lida por alguém não autorizado. Esse processo permite que somente o receptor da mensagem possa ler a informação com facilidade.

O imperador romano Júlio César criou um método de criptografia por substituição que consistia em emitir mensagens trocando as letras do alfabeto pelas três letras subsequentes. Por exemplo a letra A seria sibstituida pela letra D[14].

A comunicação somente pode ser efetivada porque os interlocutores sabiam previamente o segredo ou código secreto que seria utilizado ocultar a informação. A criptografia pré-computacional era constituida por um conjunto de métodos de substituição e transposição dos caracteres de uma mensagem que pudessem ser executados manualmente pelo emissor e pelo receptor da mensagem[15].

---

[13] MONTEIRO, Emiliano S. **Certificados Digitais: conceitos e práticas**. 1. Ed. São Paulo: Brasport, 2007.p. 5.
[14] SILVA, Lino Sarlo. **Public Key Infrastructure**. 1 Ed. São Paulo: Novatec Editora, 2004.p.44.
[15] Verbete *criptografia* disponível em: http://pt.wikipedia.org/wiki/Wiki. Acesso em 09.07.200às 09:00.

As informações que utilizam o meio digital, sendo representadas por bits, utilizam o processo de encriptação feito por algoritmos que fazem o embaralhamento desses bits a partir de uma determinada chave ou par de chaves, dependendo do sistema criptográfico escolhido. As chaves, portanto, são parâmetros atribuídos a um algoritmo criptográfico para que produza um criptograma específico.

O nível de segurança alcançado pela criptografia depende da chave utilizada. as chaves na criptografia também possuem diferentes tamanhos, sendo seu grau de segurança relacionado ao tamanho da chave. Os algorítmos empregados são, geralmente, de domínio público para permitir análise e validação da comunidade científica, visando a correção de falhas e melhorias.

Os sistemas criptográficos são utilizados para prover recursos que garantam os seguintes serviços[16]:

1. Confidencialidade: Garante que somente os destinatários autorizados serão capazes de extrair o conteúdo da informação da sua forma cifrada.
2. Integridade: Assegura que o destinatário será capaz de determinar se a informação foi alterada durante a transmissão.
3. Autenticação: Garante a orígem da informação permitindo ao destinatário identificar o remetente e verificar que foi mesmo ele quem enviou a mensagem.
4. Não-repúdio ou irretratabilidade: Assegura que nenhum dos participantes da comunicação possa negar que essa tenha ocorrido.

Os sistemas criptográficos baseados na utilização de chaves criptográficas são classificados em criptografia simétrica, que usa uma única chave conhecida somente pelo emisor e o recepor da mensagem, e criptografia assimétrica, que usa um par de chaves, sendo uma pública, conhecida por todos e utilizada para cifrar a mensagem e outra chave privada, conhecida apenas pelo destinatário e utilizada para decifrar a mensagem.

3.2. Criptografia Simétrica

A criptografia simétrica é fundamentada em operações (algoritmos) que dependem da mesma chave, conhecida como “chave secreta”. Na criptografia

[16] Verbete *criptografia* disponível em: http://pt.wikipedia.org/wiki/Wiki. Acesso em 09.07.200às 09:00.

simétrica, uma única chave é utilizada para codificar (cifrar) e decodificar (decifrar) uma mensagem.

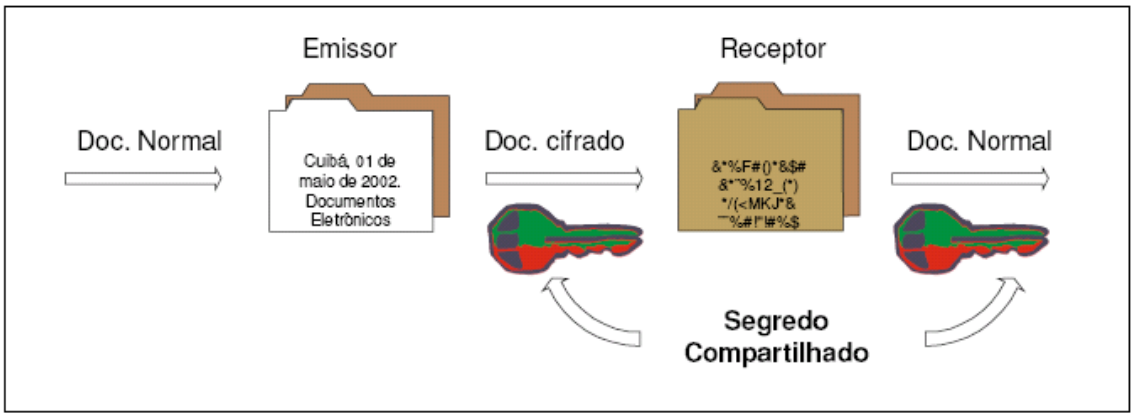

Ilustração 1. Fonte: adaptado de TADANO, Katiucia Yumi. **GED: Assinatura Digital e Validade Jurídica de Documentos Eletrônicos**.

A chave secreta deve ser compartilhada somente pelo emissor e receptor da mensagem. A segurança deste método criptográfico depende do segredo dessa informação.

O Data Encryption Standard (DES) é uma cifra (método de encriptação) selecionado como FIPS oficial (Federal Information Processing Standard) pelo governo dos EUA em 1976 e que foi utilizado como padrão na criptografia simétrica[17], sendo posteriormente substituido pela AES.

O DES utiliza chaves de 64 bits, porém somente 56 deles são realmente utilizados pelo algoritmo. Os oito bits restantes são utilizados para checar a paridade e depois são descartados, portanto o tamanho efetivo da chave é de 56 bits.

A eficiência desta solução está baseado no tempo que um terceiro levaria para descobrir a chave criptográfica utilizada para cifrar uma mensagem. Para uma chave de 56 bits teríamos 2^{56} possibilidades. Caso um computador realizasse um bilhão de testes por segundo para descobrir a chave seriam necessários dois anos para encontrá-la[18].

A exigência do conhecimento prévio da chave por cada participante da comunicação representa uma desvantagem dos algoritmos de chave-simétrica, onde uma cópia é mantida em cada extremidade. Quanto mais pessoas tiverem acesso a essa chave maiores serão riscos de segurança. Para minimizar este risco torna-se

[17] Verbete *DES* disponível em: http://pt.wikipedia.org/wiki/Wiki. Acesso em 09.07.2008 às 09:00.
[18] SILVA, Lino Sarlo. **Public Key Infrastructure**. 1 Ed. São Paulo: Novatec Editora, 2004.p.44.

necessário a constante troca da chave secreta e a adoção de uma política de segurança para a troca, armazenamento e distribução das chaves.

O gerenciamento das chaves constitui uma dificuldade adicional, pois para garantir a comunicação segura entre um grupo de n pessoas, um total de n(n − 1)/2 chaves são necessárias, ou seja, para um grupo de 1.000 usuários seriam necessárias 499.500 chaves.

Outro problema seria a distribuição da chave antes da primeira comunicação que irá utilizar a criprografia. Devem ser criados mecanismos para identificar cada portador da chave simétrica.

Os algorítimos simétricos menos intensivos computacionalmente, ou seja, mais rápidos, que os algoritmos assimétricos. Uma das aplicações da criptografia simétrica ocorre ao acessarmos uma página segura na Internet através do procolo de comunicação SSL. Nesse caso é utilizado o algiritimo assimétrico, mais lento, para ditribuir uma chave simétrica gerada automaticamente. Após a troca segura das chaves simétricas a comunicação poderá ocorrer com maior velocidade.

3.3. Criptografia Assimétrica

A criptografia por chave pública ou criptografia assimétrica, é baseada no uso de pares de chaves de caráter complementar para cifrar/decifrar mensagens. Estas chaves são matematicamente relacionadas, usando funções matemáticas unidirecionais para a codificação da informação[19].

O usuário que gera um par de chaves assiméticas permanece com uma das chaves em seu poder, chamada de chave privada e mantida em sigilo por seu criador, e outra chave distribuida livrimente para qualquer pessoa, chamada de chave pública. Utiliza-se uma chave para cifrar a mensagem e outra chave para decifrá-la.

A confidencialidade pode ser verificada quando enviamos uma mensagem utilizando a criptografia assimétrica. O emissor da mensagem utiliza a chave pública do receptor, conhecida por todos, para cifrá-la. Somente o receptor poderá decifrar a mensagem, pois somente ele possui a chave privada utilizada para decifar e mensagem, garantindo o seu sigilo.

---

[19] TADANO, Katiucia Yumi. **GED: Assinatura Digital e Validade Jurídica de Documentos Eletrônicos**. Disponível em: http://www.arquivar.com.br/espaco_profissional/sala_leitura/teses-dissertacoes-e-monografias/GED_Assinatura_Digital.pdf. Acesso em 12.07.2008 às 13:00.

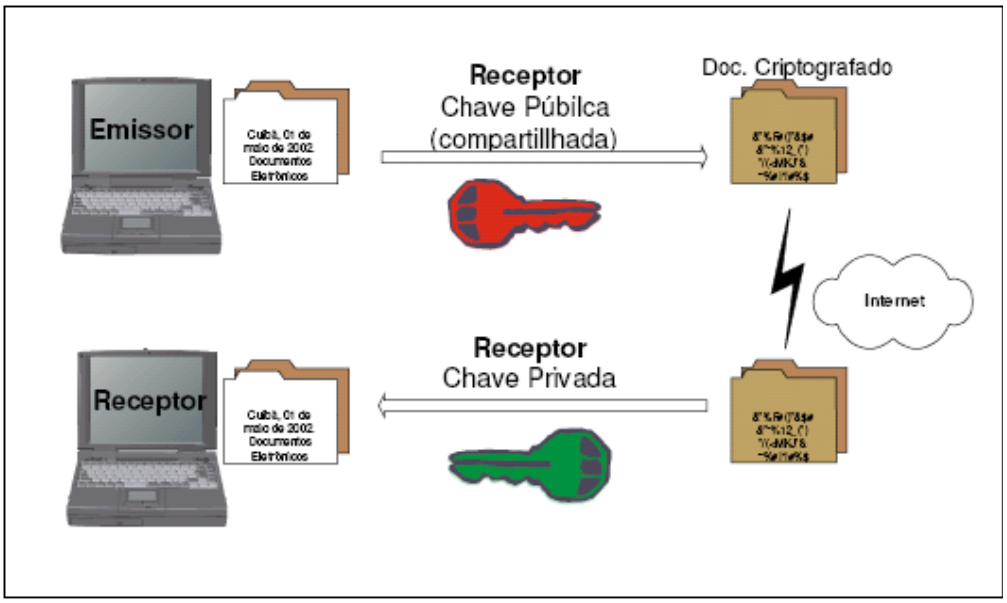

Ilustração 2: Fonte: adaptado de TADANO, Katiucia Yumi. **GED: Assinatura Digital e Validade Jurídica de Documentos Eletrônicos**.

O par de chaves assimétricas pode ser utilizado para funcionalidade de assegurar a autenticidade de uma mensagem. Nesse caso o emissor cifra a mensagem com sua chave privada. O receptor da mensagem irá utilizar a chave pública do emissor para decifrá-la. Como a chave privada é sigilosa e somente o emissor a conhece, pode-se imputar, com razoável grau de segurança, a autoria da criação do arquivo ao detentor da chave privada, a qual compõe, com a chave pública, o par necessário às operações de cifar e decifrar a mensagem.

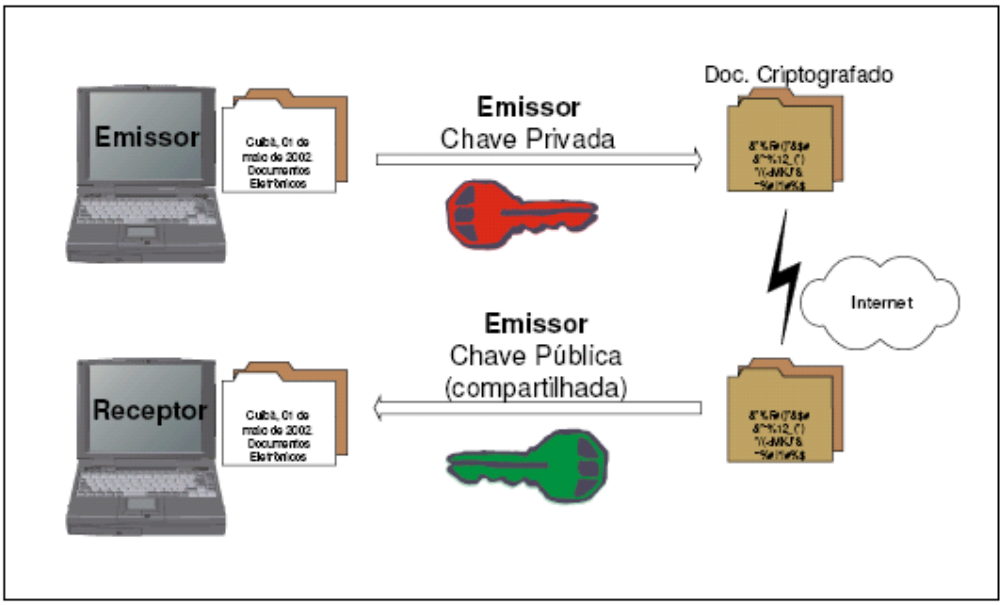

Ilustração 3. Fonte: adaptado de TADANO, Katiucia Yumi. **GED: Assinatura Digital e Validade Jurídica de Documentos Eletrônicos**.

O RSA é algoritmo padrão utilizado pela criptografia assimétrica, tendo sido desenvolvido por Ron Rivest, Adi Shamir e Leonard Adleman em 1977. A eficiência do RSA está baseada na fatoração de grandes números primos, como por exemplo, da ordem de 10^{100}. A multiplicação dos dois números pode ser executada rapidamente por com computador, porém não existe um método eficiente capaz de realizar a operação inversa[20].

3.4. Função Resumo (Hash)

Visando permitir a verificação da integridade de uma mensagem criou-se um mecanismo denominado Função Resumo ou Função Hash que, quando aplicada ao conteúdo de uma mensagem, gera um resumo.

A Função Resumo recebe como entrada uma mensagem ou documento de qualquer tamanho e gera um resumo de tamanho fixo também chamado de Message Digest ou valor hash. O objetivo da Função Resumo é produzir algo equivalente a uma “impressão digital” da mensagem[21].

O resumo calculado pela Função Resumo será único para cada mensagem, portando mensagens diferentes gererão resumos diferentes e uma dada mensagem gerará sempre o mesmo resumo. Qualquer alteração na mensagem será detectada, pois ao ser aplicada novamente a função o resumo gerado será diferente. Outra propriedade dessa função é que não se pode recompor a mensagem original a partir do resumo, ou seja, a função possui apenas um único sentido.

Para garantir a integridade de uma mensagem o emissor enviará o resumo em anexo. O receptor irá recalcular o resumo da mensagem recebida e comparar com o resumo recebido. Se os resumos forem iguais a mensagem poderá ser considera integra, pois seu conteúdo não foi alterado.

---

[20] SILVA, Lino Sarlo. **Public Key Infrastructure**. 1 Ed. São Paulo: Novatec Editora, 2004.p.58.
[21] MONTEIRO, Emiliano S. **Certificados Digitais: conceitos e práticas**. 1. Ed. São Paulo: Brasport, 2007.p. 8.

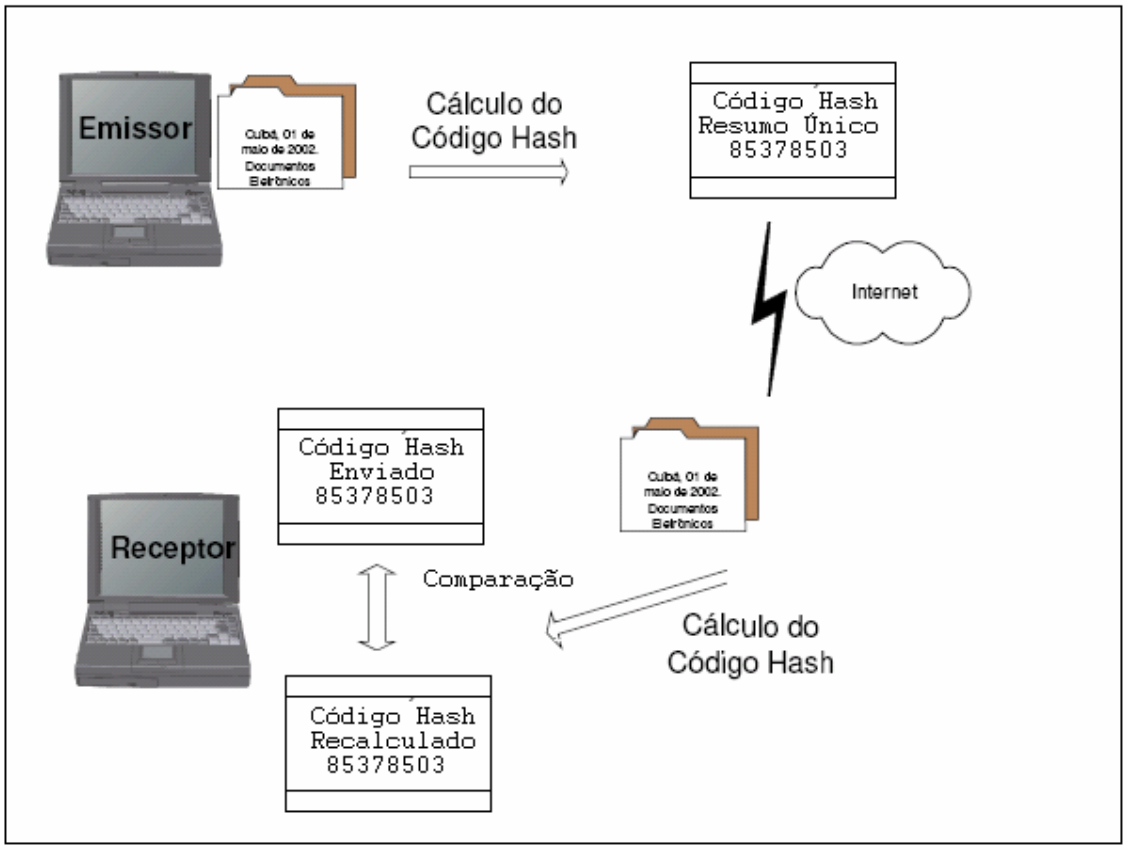

Ilustração 4. Fonte: adaptado de TADANO, Katiucia Yumi. **GED: Assinatura Digital e Validade Jurídica de Documentos Eletrônicos.**

As funções resumo que são mais utilizadas e consideredas seguras são o SHA-1 (Secure Hash Algorith-1) e MD5 (Message Digest-5).

O SHA-1 recebe como entrada uma mensagem de qualquer tamanho, menor que 2^{64} bits, e gera um resumo de 160 bits chamado *message digest*. O resumo pode ser anexado a mesagem original formando o bloco de informações que será transmitido. O receptor retira o resumo do bloco de informações recebido e recalcula o resumo da menagem recebida e compara o resultado com o resumo recebido. Se os dois valores forem iguais pode-se garantir que a mensagem não sofreu alterações no seu trajeto.

3.5. Autenticação

A autenticação é a capacidade de garantir que alguém ou alguma coisa, é de fato quem diz ser, dentro de um contexto definido[22]. As pessoas ou equipamentos devem ser identificados quando envolvidos em uma transação eletrônica.

O processo de autenticação é sempre realizado entre duas entidades. O usuário ou cliente que necessita do acesso a determinada informação e o autenticador que validará ou não a identidade do solicitante. Para o usuário ser validado deve ser fornecida uma informação de indentificação ao autenticador.

Uma autenticação pode ser realizada através do fornecimento das seguintes informações de identificação[23]:

1. Algo que você sabe: a autenticação é feita através de algum conhecimento específico do indivíduo. Este conhecimento pode ser uma senha ou um número de identificação pessoal.
2. Algo que você tem: a entidade é identificada através da posse de algo, o objeto pode ser, por exemplo, um token USB ou um smart card com a chave privada armazenada.
3. Algo que você é: ele utiliza alguma medida biométrica para identificação. Por exemplo a impressão digital ou a íris.
4. Onde você está: Este tipo de autenticação leva em consideração a posição geográfica do indivíduo no momento da autenticação. A verificação deste tipo de autenticação pode ser feita utilizando, por exemplo, algo semelhante a um dispositivo de Global Positioning System (GPS).
5. Momento da autenticação: esta autenticação baseia-se na validação da data e hora que o usuário está autenticando-se perante um sistema. A data e hora serão atribuídas por uma protocolizadora digital. Assim não será possível burlar o sistema porque somente um horário assinado por um dispositivo válido será reconhecido.
6. Presença de testemunha: A autenticação é realizada apenas com a presença de uma ou mais testemunhas. Este tipo de autenticação possui uma segurança muito grande devido à necessidade de duas ou mais pessoas autenticarem-se no sistema.

---

[22] SILVA, Lino Sarlo. **Public Key Infrastructure**. 1 Ed. São Paulo: Novatec Editora, 2004.p.66.
[23] IGNACZAK, Luciano. Dissertação de Mestrado. **Um Novo Modelo de Infra-estrutura de Chaves Públicas para Uso no Brasil Utilizando Aplicativos com o Código Fonte Aberto**. Universidade Federal de Santa Catarina, 2002.

A autenticação realizada através da combinação de duas ou mais formas de identificação é denominada autenticação forte, por fornecer um acréscimo no nível de segurança. Por exemplo, a autenticação pode ser feita digitando uma senha (algo que sabemos), junto com a verificação da impressão digital do indivíduo (algo que somos).

A segurança do processo de autenticação depende do sigilo das informações utilizadas, devendo-se prevenir que pessoas não autorizadas tenham acesso as informações de autenticação.

3.6. Assinatura Digital

O ato de assinar um documento no papel, está efetivando a ligação entre a assinatura propriamente dita e a informação ali impressa. Na assinatura manuscrita, existe uma ligação entre a pessoa que assina e o documento, pois no ato em que se assina é impressa no papel uma escrita que possui dependência das biocaracterísticas da pessoa. Nos documentos eletrônicos, este efeito não ocorre, pois não há meio físico que estabeleça uma ligação entre o assinante e a assinatura[24].

A assinatura eletrônica pode ser entendida como toda forma de se autenticar um documento eletrônico através da identificação inequívoca de seu signatário. A identificação do usuário e autenticação do seu acesso pode ser feito através dos métodos de autenticação listados no item anterior.

A assinatura digital é a forma de assinatura eletrônica mais segura onde se utiliza um algoritmo de autenticação, que possibilita o criador de um objeto, unir ao objeto criado, um código que irá agir como uma assinatura.

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

As propriedades da assinatura digital são[25]:

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

---

[24] MIGNONI, Maria Eloísa. Dissertação de Mestrado. **Políticas e Declaração de Práticas de Certificação Digital para UFSC**. Universidade de Santa Catarina, 2002.

[25] TADANO, Katiucia Yumi. **GED: Assinatura Digital e Validade Jurídica de Documentos Eletrônicos**. Disponível em: http://www.arquivar.com.br/espaco_profissional/sala_leitura/teses-dissertacoes-e-monografias/GED_Assinatura_Digital.pdf. Acesso em 12.07.2008 às 13:00

b) assinatura não pode ser falsificada: o emissor assinou o documento, pois somente ele conhece a chave privada;

c) documento assinado não pode ser alterado: qualquer alteração no documento será detectada através do uso da chave pública do emissor e do resumo do documento;

d) assinatura não reutilizável: assinatura é única para cada documento e não poder ser transferida para outro documento, uma vez que ela deve estar vinculada ao conteúdo do documento, o que pode ser garantido através do uso da função resumo;

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

A assinatura digital permite demonstrar a autoria e verificar a integridade de um documento eletrônico, bem como estabelece uma "imutabilidade lógica" do seu conteúdo. A definição de "imutabilidade lógica" exposta por Marcacini[26] diz que o documento continua podendo ser alterado, sem deixar vestígios no meio físico onde está gravado (esta, aliás, é uma importante característica do documento eletrônico, que vai permitir desvinculá-lo do meio físico e transmiti-lo, via Internet); entretanto, a posterior alteração do documento invalida a assinatura, o que faz com que o documento deixe de ter valor como prova.

Para assinar digitalmente um documento o emissor, signatário do documento, deve gerar o resumo a partir do documento original e cifrá-lo usando sua chave privada, obtendo assim, uma assinatura digital que será anexada ao documento, gerando um documento assinado. O receptor por sua vez, deve decifrar a assinatura anexada ao documento com a chave púbica do emissor obtendo assim o resumo originalmente enviado. Em seguida o receptor gera o novo resumo do documento recebido e compara o resultado obtido com o resumo enviado. Se forem iguais, a integridade está garantida, e como apenas o emissor do documento pode ser identificado pela sua chave pública, pois somente o mesmo detêm posse de sua chave privada, a autenticidade também está garantida.

---

[26] MARCACINI, Augusto Tavares Rosa. **Documento Eletrônico como Meio de Prova**. Disponível em: http://www.infodireito.com.br/info/index.php?option=com_content&task=view&id=44&Itemid=42. Acesso em: 07.07.2008 às 15:00

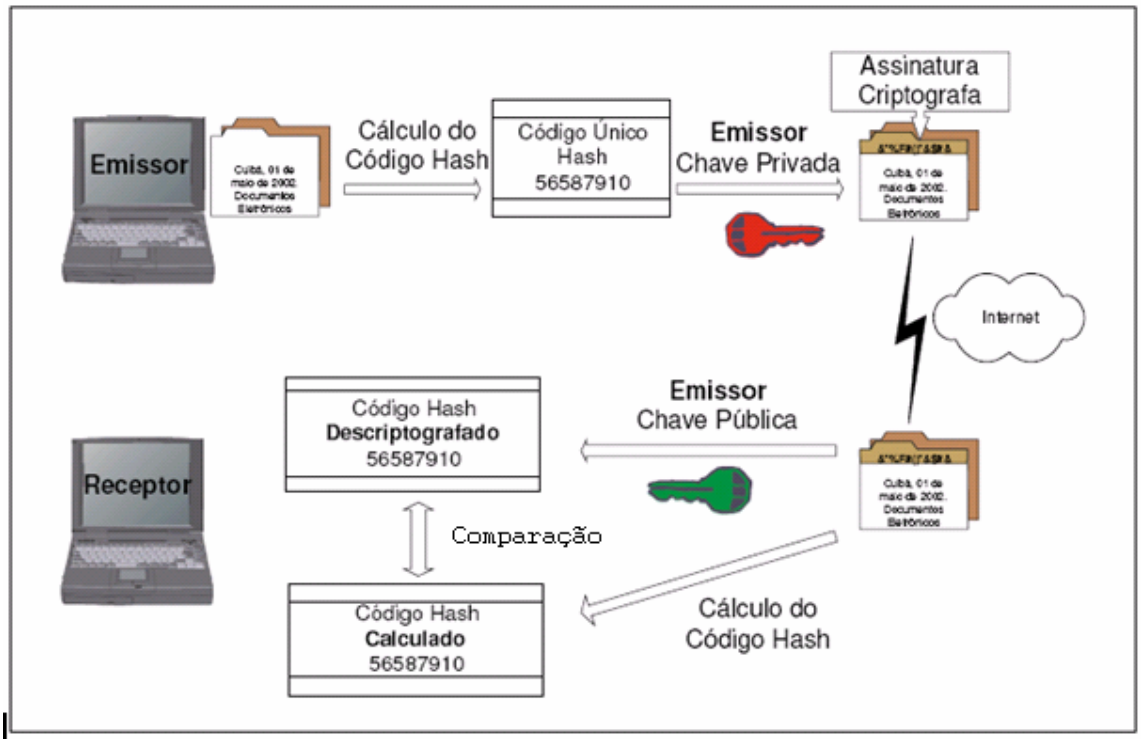

Ilustração 5. Fonte: adaptado de TADANO, Katiucia Yumi. **GED: Assinatura Digital e Validade Jurídica de Documentos Eletrônicos.**

A assinatura digital não é utilizada para fornecer sigilo ao documento, uma vez que a chave pública deve ser de conhecimento de todos, portando qualquer pessoa terá acesso ao conteúdo do documento.

Para garantir, além da integridade e autenticidade, forcedidas pela assinatura digital, a confidencialidade do documento, deve-se cifrar o documento, após ser assinado pelo emissor, com a chave pública do receptor.

O receptor por sua vez, deve decifrar o documento assinado com sua chave privada e, somente depois, executar o procedimento verificação da assinatura digital conforme já explanado.

O algoritmo de criptografia assimétrica RSA é utilizado por 2/3 das companhias americanas para implementar as funcionalidades todas as assinatira digital descritas neste item.

Uma alternativa ao RSA é o algoritmo de assinatura digital DSA - Digital Signature Algorithm, que foi proposto em agosto de 1991 pelo Instituto Nacional de Padrões e Tecnologia Norte Americano (NIST) para ser utilizado como o padrão para assinatura digital. A fórmula matemática usada como base do DSA é

diferenciada do RSA. O DSA aplica um sistema de chave pública irreversível e a sua segurança depende da dificuldade de cálculo do algoritmo[27].

O DSA é utilizado somente para assinatura digital, não podendo ser usado para cifragem e distribuição de chaves.

3.7. Tempestividade

Os documentos eletrônicos devem ser datados para que possam ser possuir a mesma eficacia probante dos documentos tradicionais em papel. O requisito da tempestividade pode ser obtido através do processo de datação do documento eletrônico que fornece uma referência temporal permitindo determinar a existência de um documento em determinado instante do tempo.

A datação do documento também é necessária para garantir que o par de chaves utilizados para assinar digitalmente um documento estavam válidas no momento da assinatura.

A datação é estabelecida por uma entidade confiável que produz uma marcação temporal denominada carimbo de tempo (timestamp). Esta entidade é chamada de Protocolizadora Digital de Documentos Eletrônicos - PDDE (Time Stamping Authority)[28].

A datação pode ser realizada utilizando-se métodos absolutos, relativos ou híbridos. Na datação absoluta, a data e a hora são obtidas de alguma fonte de tempo, e anexadas ao documento digital. Na datação relativa, utiliza-se um conceito de determinar qual documento existia primeiro, sem preocupar-se com a data e a hora reais. Neste caso, os documentos são encadeados, sendo possível determinar através da análise da cadeia qual o documento é mais antigo. Nos métodos híbridos há uma composição, utilizando-se as datações absoluta e relativa simultaneamente.

A forma mais segura de garantir a tempestividade de um documento eletrônico será alcançada através da utilização de uma autoridade de datação hibrida, apresentando um esquema de datação relativa e absoluta simultaneamente.

A datação de um documento eletrônico através do processo de procolização inicia-se com a gereção do resumo do documento a ser datado. O resumo, e não o

---

[27] MIGNONI, Maria Eloísa. Dissertação de Mestrado**. Políticas e Declaração de Práticas de Certificação Digital para UFSC**. Universidade de Santa Catarina, 2002.

[28] DIAS, Júlio da Silva. Tese de doutorado. **Confiança no Documento Eletrônico**. Universidade de Santa Catarina, 2003.

documento completo, é enviado a uma PDDE que procotoliza o documento gerando um recibo, assinado digitalmente pela PDDE, contendo a data e hora, um número sequencial do documento, e o resumo. O recibo é enviado ao cliente, que verifica a validade da assinatura digital da PDDE e a ingegridade do resumo, confirmando a protocolação do seu documento.

3.8. Segurança do Processo de Assinatura Digital

Para garantir a segurança do processo de assinatura digital deve-se estabeler procedimentos de obetenção da chave pública de maneira confiável. A validação de uma assinatura digital, ou o estabelecimento de uma comunicação sigiliosa, pressupõe a garantia da identificação inequívoca do proprietário da chave pública que será utilizada no processo.

As chaves públicas podem ser armazenadas em um repositório confiável como um catálogo telefônico que conterá as chaves de todos os participantes. Quando houver necessidade de utilizar uma chave pública deve-se acessar o catálogo para buscá-la. A entrega da chave pública solicitada deve ser fornecida íntegra e com a garantia de quem é seu proprietário.

Devem ser estabelecidos procedimentos que determinem a pertinência do par de chaves e seu prazo de validade, com o correlato direito a repudiá-las, caso estejam vencidas ou seja detectada fraude.

A forma de resolver as dificuldades apontadas é atribuir a um terceiro, por lei ou por acordo entre os interessados, poderes para certificar que as chaves são válidas e a identidade de seu titular. Para tanto foram criadas as infra-estruturas de chaves públicas e certificação digital que consistem em um sistema de autenticidade das chaves públicas, ou seja, uma estrutura que confirma que aquela chave pública que está sendo utilizada para validar a assinatura digital de alguém ou para criptografar um documento é de fato desta pessoa. O principal objetivo desta solução, que será detalhada no capítulo seguinte, é vincular uma assinatura digital a um indivíduo, organização ou qualquer entidade.

4. A INFRA-ESTRUTURA DE CHAVES PÚBLICAS E A CERTIFICAÇÃO DIGITAL

As infra-estruturas de chaves públicas (ICP's) é um ambiente criado para autenticar as chaves públicas utilizadas para validação de assinaturas digitais. O objetivo da ICP é garantir que os sistemas que utilizem um par de chaves para assinar documentos digitais possam confirmar inequivocamente que as chaves públicas que serão utilizadas para validar as assinaturas digitais são de fato de determinado signatário. O certificado digital é o instrumento utilizado para a validação das chaves públicas nestas estruturas, sendo ele próprio um documento eletrônico, assinado digitalmente por uma autoridade certificadora, que contém diversos dados sobre o emissor e o titular do certificado, como nome do titular, identificação do algoritmo de assinatura, assinatura digital do emissor, validade do certificado, além da própria chave pública vinculada ao titular do certificado.

4.1. Certificação Digital

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

No cerne da certificação digital está o certificado digital que é um documento assinado digitalmente por uma entidade certificante confiável e que cumpre a função de associar uma pessoa ou entidade a uma chave pública. As informações públicas contidas num certificado digital são o que possibilita colocá-lo em repositórios públicos para que terceiros possam conferir a autenticidade das assinaturas digitais que vierem examinar.

O certificado digital possui informações sobre o nome da pessoa ou entidade a ser associada à chave pública, o período de validade do certificado, o código da chave pública, o nome e assinatura da entidade emitente do certificado, e um número de controle interno de série de emissão. O certificado opera como uma espécie de chancela afirmando que a chave pública tem por titular quem denota sê-lo.

Pode-se entender o Certificado Digital como a tecnologia que permite comprovar a identidade tanto de pessoas físicas como jurídicas, garantindo transações comerciais e financeiras, a troca de mensagens eletrônicas e a assinatura de documento eletrônicos, com total segurança, sigilo e agilidade, dispensando o uso de documentos físicos[29].

Certificação digital é a tecnologia utilizada para dar força probante aos documentos eletrônicos, isto é, torná-los passíveis de serem autenticados e com firma reconhecida como é no mundo real.

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

Conforme explica Marcacini[30]:

> O certificado eletrônico é uma forma - não a única, mas talvez a mais prática - de se demonstrar a titularidade da chave pública utilizada para conferir a assinatura. Pode ser entendido, sob o ângulo jurídico, como uma declaração de uma pessoa - o ente certificante - em relação à chave pública de uma outra pessoa, atestando essa titularidade. Tecnicamente falando, o certificado é um arquivo eletrônico, assinado pelo certificante com a sua chave privada, contendo a chave pública e informações pessoais do titular desta chave pública.

O certificado digital passa por várias fases, desde seu requerimento até o fim de sua validade. A autoridade certificadora é responsável pelo gerenciamento do ciclo de vida dos certificados por ela emitidos.

O ciclo de vida de um certificado digital é constituído das seguintes etapas[31]:

1. Requerimento: é o pedido de expedição do certificado digital feito pela pessoa interessada à Autoridade Certificadora;
2. Validação do requerimento: é função da AC garantir que o requerimento seja válido e que os dados do requerente sejam corretos;
3. Emissão do certificado: é o ato de reconhecimento do título do certificado digital pelo requerente e sua emissão;
4. Aceitação do certificado pelo requerente: após emitido, o requerente deve retirá-lo da AC e confirmar a validade do certificado emitido;

---

[29] TRAIN, Sheila. **Identidade Digital**. Disponível em: https://www.certisign.com.br/treinamento/guias-gratuitos/pdf/livro_id_digital_certificado.pdf. Acesso em 15.07.2008 às 21:00.

[30] MARCACINI, Augusto Tavares Rosa. **Documento Eletrônico como Meio de Prova**. Disponível em: http://www.infodireito.com.br/info/index.php?option=com_content&task=view&id=44&Itemid=42. Acesso em: 07.07.2008 às 15:00.

[31] TADANO, Katiucia Yumi. **GED: Assinatura Digital e Validade Jurídica de Documentos Eletrônicos**. Disponível em: http://www.arquivar.com.br/espaco_profissional/sala_leitura/teses-dissertacoes-e-monografias/GED_Assinatura_Digital.pdf. Acesso em 12.07.2008 às 13:00.

5. Uso do certificado: é o período em que o certificado pode ser utilizado, sendo seu uso de total responsabilidade do requerente;
6. Suspensão do certificado digital: é o ato pelo qual o certificado se torna temporariamente inválido para operações por algum motivo especificado pela AC, como o comprometimento da chave pública;
7. Revogação do certificado: é o processo pelo qual o certificado se torna definitivamente inválido pelo comprometimento da chave privada do titular ou quando ocorrer algum fato que torne o certificado digital pouco seguro para uso. Um certificado suspenso ou revogado deve ser publicado na lista de certificados revogados (LCR) e estar sempre disponível para consulta;
8. Término da validade e renovação do certificado: o certificado digital tem um período preestabelecido de validade atribuído pela AC. Em geral, este período é de um a três anos, dependendo da importância e finalidade da chave.

4.2. Padrões de Certificados Digitais

Os certificados digitais foram inicialmente padronizados no esquema X.509. Das várias propostas de codificação de certificados, a mais conhecida, aceita e utilizada, tendo se tornado o padrão de fato, é a recomendação ITU-T X.509 (International Telecomunication Union).

A recomendação encontra-se, atualmente, na terceira versão. O ITU-T emitiu esta versão com a seguinte estrutura:

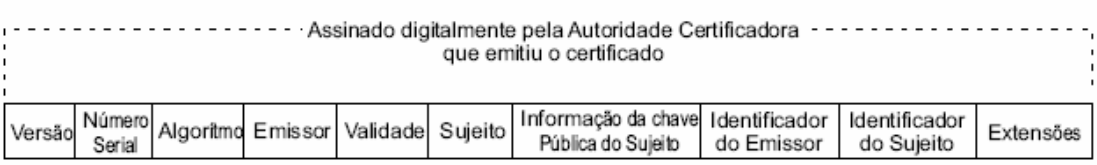

Ilustração 6. IGNACZAK, Luciano. Dissertação de Mestrado. **Um Novo Modelo de Infra-estrutura de Chaves Púublicas para Uso no Brasil Utilizando Aplicativos com o Código Fonte Aberto.**

Um certificado digital, de acordo com a recomendação, X.509v3 é formado pelo seguinte conjunto de campos[32]:

1. Versão: identifica a versão do certificado. A versão pode ser 1, 2 ou 3;
2. Número Serial: Identificador único de um certificado em relação à AC que o emitiu;
3. Identificador do Algoritmo de Assinatura: campo que identifica o algoritmo usado pela AC para assinar o certificado;
4. Nome do Emissor: Informações que identificam a AC emissora do certificado;
5. Período de Validade: intervalo de tempo que um certificado pode ser considerado válido. Este campo possui a data que o certificado foi emitido pela AC e a data de expiração do certificado;
6. Sujeito: Dados de identificação do indivíduo ou dispositivo ao qual o certificado foi emitido;
7. Informações sobre a Chave Pública do Sujeito: a chave pública do certificado, juntamente com identificador do algoritmo que a chave pública deve utilizar em suas operações;
8. Identificador do Emissor: valor único para a identificação do emissor do certificado;
9. Identificador do Sujeito: valor usado para a identificação do possuidor do certificado;
10. Extensões: a Versão 3 da recomendação X.509 definiu utilização de campos de extensões com a finalidade de tornar mais flexível a utilização dos certificados digitais. Estes campos serão abordados em seguida.

Um certificado digital é sempre assinado digitalmente por uma AC. Esta entidade deve possuir a confiança do indivíduo que utilizará o certificado, pois é ela que assegura a validade dos dados contidos no certificado digital.

As extensões dos certificados digitais oferecem controles gerenciais e administrativos através da inclusão de informações que não são fornecidas pelo conteúdo básico de um certificado. Qualquer organização pode definir suas próprias

[32] IGNACZAK, Luciano. Dissertação de Mestrado. **Um Novo Modelo de Infra-estrutura de Chaves Púublicas para Uso no Brasil Utilizando Aplicativos com o Código Fonte Aberto**. Universidade Federal de Santa Catarina, 2002.

extensões de acordo com suas necessidades, porém existem extensões que são incluídas por padrão como informações sobre políticas e chaves.

As extensões de certificados possuem três componentes[33]: um identificador, um sinalizador de importância e um valor. O identificador define o formato e a semântica do campo valor. O sinalizador que indica se a extensão é crítica ou não crítica. A extensão do tipo crítica não poderá ser ignorada pelo usuário de certificados, portanto se o valor não for o esperado o certificado não será aceito. A extensão do tipo não-crítica pode ser ignorada pelo usuário de certificados. Uma extensão não crítica pode ser, por exemplo, o endereço de e-mail.

4.3. Infra-estrutura de Chaves Públicas

A Infra-estrutura de Chaves Públicas é composta de uma rede de protocolos, padrões e serviços destinada ao uso e obtenção de certificados digitais, que tem como função básica certificar, isto é, vincular uma chave pública a um indivíduo, organização ou qualquer entidade, e verificar a validade de um certificado emitido.

Para viabilizar o uso de uma ICP é necessária a criação de uma estrutura que possibilite a correta operação da parte técnica. Os elementos que fazem parte da infra-estrutura de chaves públicas são[34]:

1. O titular do certificado: aquele que faz uso do certificado digital;
2. A autoridade certificadora raiz (AC-Raiz): define e normatiza o funcionamento da ICP e realiza o licenciamento das ACs, emite , mantêm e cancela os certificados das ACs;
3. A autoridade certificadora (AC): responsável pela emissão do certificado digital, pela identificação do titular do certificado e pelo gerenciamento da lista de certificados revogados;
4. A autoridade de registro (AR): responsável pela identificação do usuário final, por receber solicitações de emissão ou de revogação dos certificados, disponibilizar os certificados emitidos pela AC aos seus respectivos solicitantes e serve como intermediária entre o usuário e a AC;

---

[33] SILVA, Lino Sarlo. **Public Key Infrastructure**. 1 Ed. São Paulo: Novatec Editora, 2004.p.147.
[34] TADANO, Katiucia Yumi. **GED: Assinatura Digital e Validade Jurídica de Documentos Eletrônicos**. Disponível em: http://www.arquivar.com.br/espaco_profissional/sala_leitura/teses-dissertacoes-e-monografias/GED_Assinatura_Digital.pdf. Acesso em 12.07.2008 às 13:00

5. O repositório de certificados e LCR: é um repositório que pode ser acessado por todos os membros da ICP e onde ficam armazenados os certificados emitidos, bem como os revogados;
6. As terceiras partes: considera-se terceira parte, a parte que confia no teor, validade e aplicabilidade do certificado digital emitido por uma AC;
7. Auditorias independentes: As empresas de Auditoria Independentes são contratadas pelas autoridades certificadoras para realizarem auditorias operacionais em entidades a elas subordinadas.

Segundo Lino Sarlo a ICP têm três processos principais[35]:

1. Certificação: criação do certificado digital autenticado por uma entidade confiável denominada autoridade certificadora.
2. Validação: é o processo que verifica a autenticidade do certificado para que o conteúdo deste possa ter credibilidade. Esse processo verifica a assinatura da autoridade certificadora usando a própria chave pública da AC e checando o certificado na lista de certificados revogados (LCR). O processo de validação também verifica o período de validade contido dentro do próprio certificado.
3. Revogação de certificados: é o processo que adiciona um certificado à lista de certificados revogados antes que este expire. A revogação ocorre quando um ou mais aspectos, contidos no certificado, são modificados. È de responsabilidade da AC manter todos os certificados emitidos por ela e publicar a LCR.

4.4. Autoridade Certificadora

A identidade do titular de um certificado digital é garantida pela autoridade que o emitiu (assinou) denominada de Autoridade Certificadora (AC).

Para se conferir a validade de um certificado digital é necessário que se conheça a chave pública da AC que o assinou para conferir se o certificado foi realmente assinado por ela. Como devem existir milhares de ACs é inviável que um único repositório contenha todas as chaves públicas emitidas por essas autoridades. Portanto, por motivos de escalabilidade, a Infra-estrutura de Chave Pública foi

[35] SILVA, Lino Sarlo. **Public Key Infrastructure**. 1 Ed. São Paulo: Novatec Editora, 2004.p.139.

organizada obedecendo a um modelo de confiança que define em quem cada AC deve confiar.

O modelo que iremos analisar é formado por uma hierarquia constituída por AC no topo, alguns níveis de AC, denominadas ACs intermediárias, e as entidades finais[36].

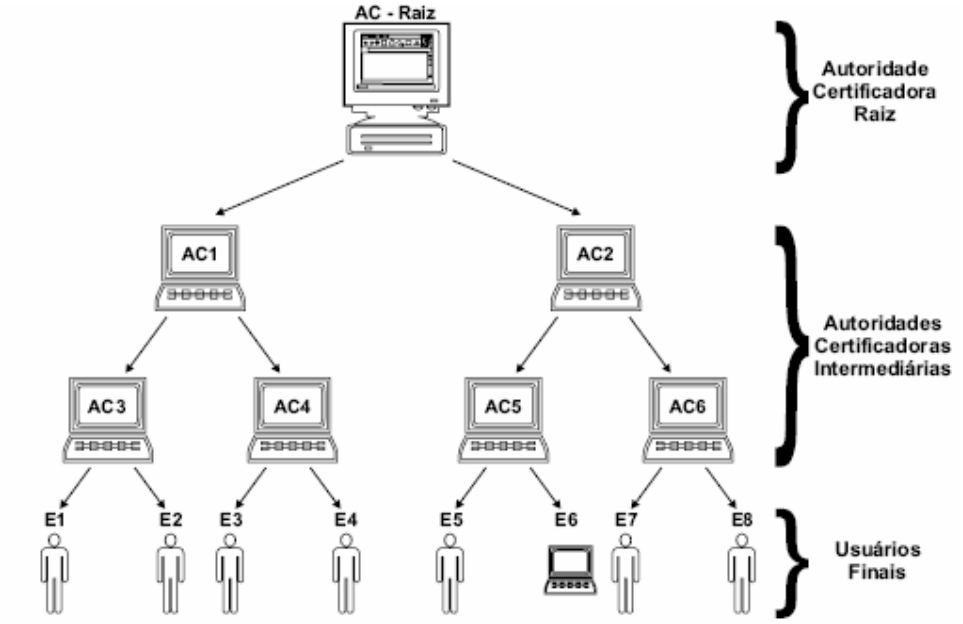

Ilustração 7. Fonte: MIGNONI, Maria Eloísa. Dissertação de Mestrado. **Políticas e Declaração de Práticas de Certificação Digital**.

A AC que fica localizada no topo é denominada AC-Raiz. Esta AC é auto-assinada, ou seja, seu certificado é assinado usando sua própria chave privada.

Abaixo da AC-Raiz pode haver vários níveis de ACs intermediárias. O número máximo de níveis abaixo é definido pela AC do nível atual.

Neste modelo a confiança é centralizada na AC-Raiz, sendo transmitida para os usuários finais através das ACs intermediárias. Todos os usuários que desejarem validar um certificado devem ter conhecimento da AC-Raiz e de sua chave pública.

Uma AC-Raiz não emite certificados para usuários finais. A emissão de certificados é tarefa das ACs intermediárias. Caso seja permitido pela AC-Raiz as ACs Intermediárias poderão emitir certificados para outras ACs abaixo delas.

Em uma estrutura hierárquica denomina-se caminho de certificação à verificação dos certificados de todas as ACs, iniciando pelo certificado da entidade

[36] IGNACZAK, Luciano. Dissertação de Mestrado. **Um Novo Modelo de Infra-estrutura de Chaves Púublicas para Uso no Brasil Utilizando Aplicativos com o Código Fonte Aberto**. Universidade Federal de Santa Catarina, 2002.

final assinou o certificado para o usuário final, passando por todas as ACs intermediárias, até a AC-Raiz.

O caminho de certificação é necessário para determinar a confiança ou não em um certificado. No momento do recebimento de um certificado, cabe a aplicação que irá verificar sua validade descobrir se ele deve ou não ser confiado. Isto é feito através do processamento do caminho de certificação, ou seja, a possibilidade de percorrer todo o caminho da certificação e validação do certificado, através de uma corrente de ligação entre ACs. Antes de o sistema interpretar o certificado recebido como um certificado válido, ele monta todo o caminho de certificação e descobre se este possui algum certificado considerado ”confiável” por ele. Além disso, o sistema também procurará uma brecha no caminho de certificação, ou seja, algum certificado que possua restrições ou que não poderá mais ser considerado válido[37].

Caso a AC emissora do certificado não seja confiada pelo sistema e nenhuma outra AC do caminho de certificação possuir esta confiança, o certificado será assumido como não confiável pelo sistema e a conexão só continuará se o usuário assumir a responsabilidade da confiança.

4.5. Autoridade de Registro

A Autoridade de Registro (AR) é a entidade responsável pela verificação das informações de identificação fornecidas pelos requisitantes de um certificado digital.

O requisitante do certificado deve comparecer pessoalmente a AR com a documentação necessária para garantir a veracidade das informações de identificação solicitadas. As ARs possuem algumas obrigações específicas, estabelecidas pela AC para garantirem a forma como deverão ser recebidas as informações de um requerente a certificado e como as informações serão conferidas.

Se as informações fornecidas pelos requerentes forem validadas, a AR poderá enviar a AC a solicitação de certificado, para que esta gere, assine digitalmente e emita o certificado, contendo as informações verificadas pela AR.

O nível de confiança atribuído a um certificado depende da qualidade do processo de conferência das informações realizado pela AR, pois a Autoridade

[37] MIGNONI, Maria Eloísa. Dissertação de Mestrado**. Políticas e Declaração de Práticas de Certificação Digital para UFSC**. Universidade de Santa Catarina, 2002.

Certificadora irá assinar as informações envidas, que serão incluídas no certificado, sem qualquer verificação adicional.

Todos os recursos para a emissão e administração dos certificados estão centralizados na AC. Uma AC pode credenciar várias ARs distribuídas geograficamente para efetuar a interface entre o usuário final, recebendo a solicitação do certificado e a documentação de identificação, e a AC, que emitirá o certificado.

4.6. Distribuição e Revogação de Certificados

A distribuição dos certificados digitais é realizada através da publicação em diretórios públicos que são repositórios onde estão armazenados certificados de usuários finais e a lista de certificados revogados (LCR).

O diretório público deve manter os dados dos certificados atualizados e garantir um alto nível de disponibilidade.

O acesso ao diretório é necessário, por exemplo, quando as pessoas ou aplicações necessitam da chave pública contida em um certificado para iniciar uma sessão de comunicação sigilosa.

Os serviços de diretórios, em sua grande maioria, são baseados nos padrões X.500 e LDAP. Esses padrões estabelecem um protocolo de acesso ao diretório e o modelo de informação que define como dados são armazenados e gerenciados.

Todos os certificados emitidos por uma Autoridade Certificadora possuem uma data de validade que define o período de tempo em que esse certificado pode ser utilizado. Alguns motivos podem levar a revogação um certificado antes da sua data de expiração, como por exemplo, quando for necessária a alteração de qualquer informação constante no mesmo. Para tanto a ICP deve implementar um sistema de revogação de certificados. Os certificados, quando revogados, devem ser adicionados a uma lista de certificados revogados – LCR. Esta lista deve ser consultada para se assegurar da validade da certificação digital, pois o certificado pode ter sido cancelado.

Os pares de chaves são atualizados periodicamente, e seu período de validade depende do nível de segurança previsto para o tipo de certificado. Além disso, é necessário que o histórico das chaves de criptografia de sigilo usadas

anteriormente seja preservado para garantir que informações antigas cifradas possam ser decodificadas.

As LCRs devem ser disseminadas para que os usuários possam efetuar uma verificação do estado de um certificado desejado. Esta disseminação deve ser feita de maneira eficiente para que não ocorram problemas envolvendo a validação de certificados já revogados pela AC.

4.7. PC e DPC

Toda organização responsável por uma ICP deve elaborar um conjunto de documentos especificando todas as políticas instituídas para garantir a segurança do processo de emissão e manutenção dos certificados emitidos.

O documento da Política de Certificação (PC) descreve o papel de cada componente dentro da ICP, as responsabilidades assumidas pelos seus usuários para a requisição e uso dos certificados digitais, além da manutenção do par de chaves. As políticas de certificação devem abranger desde a solicitação do certificado, até a sua expiração ou revogação[38].

O documento da Declaração de Práticas de Certificação (DPC) descreve detalhadamente como cada componente de uma ICP implementa a política de certificação. A DPC declara a PC associada e especifica os mecanismos e procedimentos utilizados para alcançar as políticas de segurança. Uma DPC pode informar os aplicativos utilizados e os procedimentos de utilização do aplicativo. Ela deve estar suficientemente detalhada para comprovar que todas as políticas podem ser satisfeitas através de procedimentos e ferramentas[39].

4.8. ICP-Brasil

No Brasil, o pilar da certificação digital foi instituido pela Medida Provisória nº 2.200-2, de 24 de agosto de 2001, sob a nomenclatura de Infra-Estrutura de Chaves Públicas Brasileira (ICP-Brasil). O ente presta-se, de acordo com o art. 1º da Medida Provisória em comento, a “garantir a autenticidade, a integridade e a validade

[38] MONTEIRO, Emiliano S. **Certificados Digitais: conceitos e práticas**. 1. Ed. São Paulo: Brasport, 2007.p. 30.
[39] MONTEIRO, Emiliano S. **Certificados Digitais: conceitos e práticas**. 1. Ed. São Paulo: Brasport, 2007.p. 33.

jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras".

Além de criar a Infra-Estrutura de Chaves Pública, a Medida Provisória 2.200-2 procurou estabelecer os efeitos jurídicos produzidos por uma declaração de vontade assinada com certificado emitido no âmbito da ICP-Brasil bem como sobre os efeitos jurídicos emanados de outros meios de comprovação de autoria.

A configuração básica da ICP-Brasil abarca uma autoridade gestora de políticas e uma cadeia de autoridades certificadoras composta pela Autoridade Certificadora Raiz - AC Raiz, pelas Autoridades Certificadoras - AC e pelas Autoridades de Registro – AR.

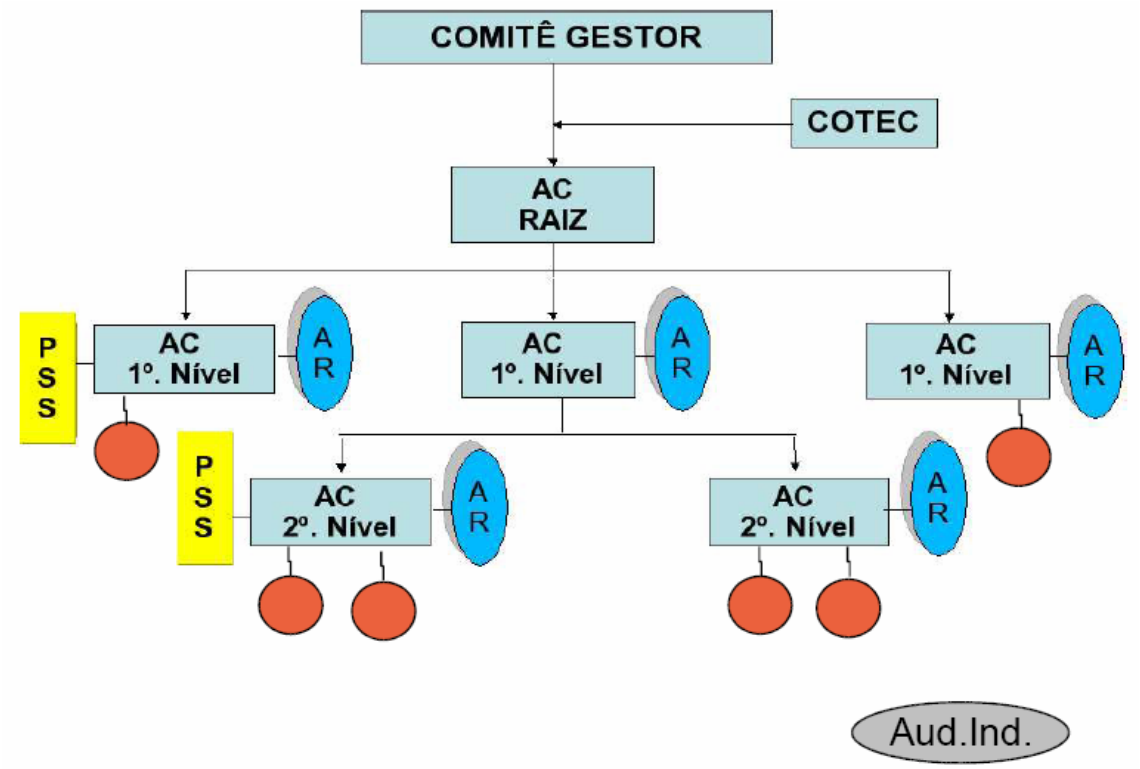

Ilustração 8. Fonte: RIBEIRO, Alexandre Menezes. **A Infra-estrutura de Chaves Públicas Brasileira e suas bases para a Auditoria em Segurança da Informação**.

As funcionalidas das autoridades certificadoras foram descritas nos itens anteriores. Os demais componentes da ICP-Brasil são detalhados a seguir,

conforme definição elaborada pela Diretoria de Auditoria, Fiscalização e Normalização do ITI – Instituto Nacional de Tecnologia da Informação[40].

O Comitê Gestor coordena a implantação e o funcionamento da ICP-Brasil, além de estabelecer a política, os critérios e as normas para credenciamento das ACs, ARs e demais prestadores de serviços de suporte em todos os níveis da cadeia de certificação. O Comitê Gestor estabelece diretrizes e normas técnicas para a formulação de políticas de certificados e regras operacionais das ACs e das ARs e define níveis da cadeia de certificação. Também atualiza, ajusta e revisa os procedimentos e as práticas estabelecidas para a ICP-Brasil, garante sua compatibilidade e promove a atualização tecnológica do sistema e a sua conformidade com as políticas de segurança. Estabelece a política de certificação e as regras operacionais da AC Raiz, bem como homologa, audita e fiscaliza a AC Raiz e os seus prestadores de serviço.

O Comitê Gestor é responsável pela aprovação das políticas de certificados, práticas de certificação e regras operacionais, credenciamento e autorização do funcionamento das ACs e das ARs, bem como autoriza a AC Raiz a emissão do correspondente certificado. Identifica e avalia as políticas de ICP externas, negocia e aprova acordos de certificação bilateral, de certificação cruzada, regras de interoperabilidade e outras formas de cooperação internacional. Certifica, quando for o caso, sua compatibilidade com a ICP-Brasil, observado o disposto em tratados, acordos ou atos internacionais. O Comitê Gestor pode delegar atribuições à AC Raiz.

O Comitê Gestor é auxiliado pelo Comitê Técnico – COTEC que presta suporte e assistência técnica, sendo responsável por manifestar-se previamente sobre as matérias apreciadas e decididas pelo comitê Gestor.

As autoridades de certificadores podem contratar empresas denominadas Prestador de Serviços de Suporte – PSS para prover a de infra-estrutura física e lógica necessária a sua operação, bem como disponibilizar de recursos humanos especializados;

---

[40] RIBEIRO, Alexandre Menezes. **A Infra-estrutura de Chaves Públicas Brasileira e suas bases para a Auditoria em Segurança da Informação**. Disponível em: http://www.arquivar.com.br/espaco_profissional/sala_leitura/teses-dissertacoes-e-monografias/Chaves_Publicas_Brasileira.pdf. Acesso em 19.07.2008 às 18:00.

As autoridades certificadoras devem contratar empresas de Auditoria Independentes, autorizadas pela AC-Raiz para atuar na ICP-Brasil, para realizar auditorias operacionais em entidades a elas subordinadas.

A ICP-Brasil se diferencia das outras cadeias de certificação por ser amplamente aceita e pelas garantias e segurança que oferece aos titulares e usuários dos certificados digitais, sendo as principais[41]:

1. O par de chaves criptográficas deve ser gerado sempre pelo próprio titular e sua chave privada de assinatura é de seu exclusivo controle, uso e conhecimento.
2. Os documentos assinados com processo de certificação da ICP-Brasil possuem presunção de validade jurídica, conforme definido pela MP nº 2.200-2;
3. São utilizados padrões internacionais para os certificados bem como algoritmos criptográficos e tamanhos de chaves que oferecem nível de segurança aceitável internacionalmente;
4. As instalações e procedimentos das entidades credenciadas possuem nível de segurança física, lógica, de pessoal e procedimental em padrões internacionais;
5. As entidades componentes da ICP-Brasil são obrigadas a declarar em repositório público as práticas de segurança utilizadas em todos os seus processos;
6. As entidades estão sujeitas a auditoria prévia ao credenciamento e anualmente, para manter-se credenciadas;
7. Os dados relativos aos certificados são mantidos por no mínimo 30 anos, para permitir comprovação e dirimir dúvidas sobre a assinatura de documentos, atendendo legislações específicas de guarda de documentos;
8. Todas as ACs são obrigadas a contratar seguro para cobertura de responsabilidade civil decorrente das atividades de certificação digital e de registro, com cobertura suficiente e compatível com o risco;

[41] RIBEIRO, Alexandre Menezes. A Infra-estrutura de Chaves Públicas Brasileira e suas bases para a Auditoria em Segurança da Informação. Disponível em: http://www.arquivar.com.br/espaco_profissional/sala_leitura/teses-dissertacoes-e-monografias/Chaves_Publicas_Brasileira.pdf. Acesso em 19.07.2008 às 18:00

9. É obrigatória a validação presencial dos titulares em uma AR para obtenção de certificados.

A Autoridade Certificadora Raiz da ICP-Brasil é a primeira autoridade da cadeia de certificação. É executora das Políticas de Certificados e normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil. Portanto, compete à AC-Raiz emitir, expedir, distribuir, revogar e gerenciar os certificados das autoridades certificadoras de nível imediatamente subseqüente ao seu.

A AC-Raiz também está encarregada de emitir a lista de certificados revogados e de fiscalizar e auditar as autoridades certificadoras, autoridades de registro e demais prestadores de serviço habilitados na ICP-Brasil. Além disso, verifica se as Autoridades Certificadoras estão atuando em conformidade com as diretrizes e normas técnicas estabelecidas pelo Comitê Gestor.

A AC-Raiz está localizada no Instituto Nacional de Tecnologia da Informação - ITI que é uma autarquia federal vinculada à Casa Civil da Presidência da República, cujo objetivo é manter a Infra-Estrutura de Chaves Públicas Brasileira – ICP-Brasil. Compete ainda ao ITI estimular e articular projetos de pesquisa científica e de desenvolvimento tecnológico voltados à ampliação da cidadania digital.

As autoridades certificadores de primeiro e segundo níveis que fazem parte da ICP-Brasil possuem a seguinte estrutura:

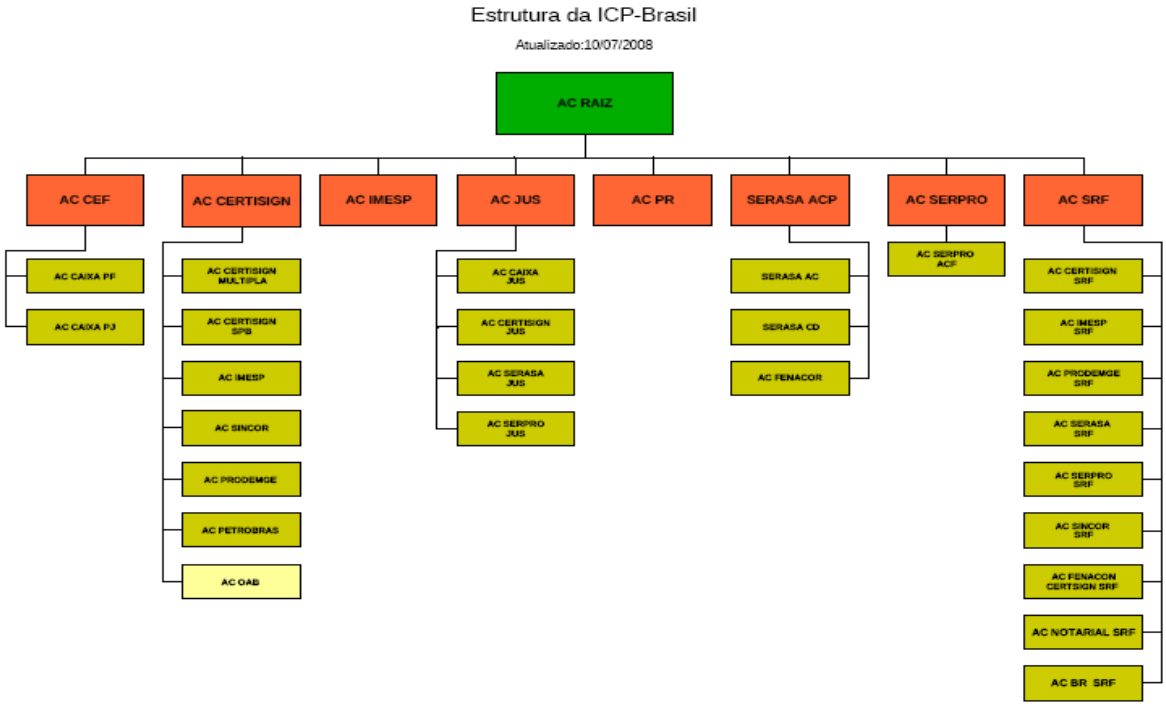

Ilustração 9. Fonte: Instituto Nacional de Tecnologia da Informação.

5. REGULAMENTAÇÃO DA CERTIFICAÇÃO DIGITAL NO PODER JUDICIÁRIO

A implantação da certificação digital no Poder Judiciário do Ceará poderá ser alcançada com a utilização de Certificados Digitais vinculados a Autoridade Certificado da Justiça AC-Jus e o desenvolvimento de aplicações especiíficas, como o Diário da Justiça Eletrônico e o Processo Eletrônico Digital.

Como premissa para início do uso da certificação digital será proposto neste capítulo uma regulamentação do uso dos certificados digitais no âmbito do Poder Judiciário do Estado do Ceará.

5.1. Autoridade Certificadora da Justiça AC-JUS

Autoridade Certificadora da Justiça, AC de primeiro nível da ICP-Brasil é a primeira do Poder Judiciário mundial, criada através de uma decisão conjunta, em 20 de Dezembro de 2004, do Superior Tribunal de Justiça e do Conselho da Justiça Federal que teve inicialmente sua atuação voltada para o STJ, CJF e Justiça Federal.

Em 30 de setembro de 2005 a AC-JUS recebeu a adesão da mais alta cúpula da Justiça, passando a integrar o Comitê Gestor, presidido pelo Presidente do STJ e do CJF e tendo como membro o Coordenador da Justiça Federal, representantes do STF, TST, TSE, STM e dos novos conselhos, criados pela EC. 45, o CNJ e CSJT.

A AC-JUS atua como uma AC normativa, ou seja, não emite certificados diretamente aos titulares, credenciando outras ACs, para que, adotando as regras por ela estabelecidas, os emitam aos requerentes. Estão definidos os tipos de Certificado: Institucional, para órgãos da Justiça, Advogado, Empresarial, Cidadão e para Equipamento Servidor.

A normatização e o credenciamento de outras ACs tiveram como objetivo a massificação do uso de certificados digitais em todo o Poder Judiciário, incluindo os Tribunais de Justiça e outros que, apesar de não fazerem parte do Comitê Gestor da AC-JUS, poderão adotar o padrão de certificados por ela definido.

Os certificados Cert-JUS identificam seus titulares relacionando-os a um determinado órgão público. Cada órgão público que desejar fazer uso de certificados

Cert-JUS deverá responsabilizar-se pelas informações funcionais e institucionais constantes na autorização e no certificado.

Conforme descrito no documento Leiaute dos Certificados Digitais Cert-JUS as seguintes normas devem ser seguidas pelos titulares dos certificados AC-JUS[42]:

- Os certificados Cert-JUS destinam-se aos órgãos da administração pública direta e indireta.
- Órgãos não pertencentes ao Poder Judiciário deverão solicitar CADASTRAMENTO junto à AC-JUS, para a emissão de certificados Cert-JUS.
    - As ACs subseqüentes somente emitirão certificados para órgãos não pertencentes ao Poder Judiciário cujo CADASTRAMENTO tenha sido aprovado pela AC-JUS.
    - Para emissão de certificados Cert-JUS para órgãos do Poder Judiciário não é necessário CADASTRAMENTO prévio na AC-JUS.
- Para a emissão de qualquer certificado Cert-JUS é necessária AUTORIZAÇÃO da autoridade competente da instituição à qual o certificado está relacionado.
    - Para o disposto neste documento, entende-se como autoridade competente:
        - A autoridade máxima do órgão;
        - O representante legal do órgão;
        - Outra pessoa expressamente designada para esta finalidade, por meio de documento oficial.
- O certificado Cert-JUS Institucional deve, obrigatoriamente, ser do tipo A3, isto é, deve ser utilizado dispositivo criptográfico (ex.: token ou smartcard) para a geração do par de chaves criptográficas e armazenamento da chave privada e do certificado.
- Os certificados digitais Cert-JUS Institucional destinam-se exclusivamente aos agentes públicos do Poder Judiciário, autorizados pela autoridade competente do seu órgão de lotação, a recebê-los.

[42] Leiaute dos Certificados Digitais Cert-JUS Versão 2.0. Disponível em http://www.acjus.gov.br/repositorio/Docs_dpc_ps. Acessado em 20.07.2008 às 12:00.

- O certificado Cert-JUS Institucional identifica o titular do certificado não só como indivíduo, mas também como servidor do órgão do Poder Judiciário em que está lotado.
    - Os certificados Cert-JUS Institucional deverão ser utilizados, nos atos praticados pelos agentes públicos no exercício de suas funções, tais como assinatura de documentos e mensagens de correio eletrônico, autenticação para acesso a sistemas e aplicações, login na rede e acesso remoto seguro.
    - Os certificados Cert-JUS Institucional devido a sua natureza especial, que vincula o titular do certificado a uma instituição, podem ser revogados a pedido da instituição ou órgão de lotação do titular do certificado.

5.2. O Diário da Justiça Eletrônico

Uma das aplicações que necessitam da tecnologia de certificação digital para sua implantação é o Diário da Justiça Eletrônico (DJe). O DJe deverá disponibilizar todas as publicações do Tribunal de Justiça com certificação digital reconhecida pela AC-Jus, Autoridade Certificadora criada e mantida pelo Poder Judiciário, vinculada à ICP-Brasil.

O DJe deverá se tornar a única publicação oficial do Tribunal de Justiça. É por meio dele que o Tribunal veiculará seus atos judiciais, administrativos e suas comunicações em geral.

A lei Nº 11.419, de 19 de Dezembro de 2006 estabeleceu em seu artigo 4º que os tribunais poderão criar o Diário da Justiça Eletrônico, disponibilizado em sítio da rede mundial de computadores, para publicação de atos judiciais e administrativos próprios e dos órgãos a eles subordinados, bem como comunicações em geral.

A obrigatoriedade da certificação digital é exigida no parágrafo primeiro do referido artigo quando expõe que o sítio e o conteúdo das publicações de que trata o artigo 4º deverão ser assinados digitalmente com base em certificado emitido por Autoridade Certificadora credenciada na forma da lei específica, ou seja, participante da ICP-Brasil.

A lei Nº 11.419 garante que o Diário da Justiça Eletrônico assinado digitalmente com um certificado da ICP-Brasil substitui qualquer outro meio e publicação oficial, para quaisquer efeitos legais, à exceção dos casos que, por lei, exigem intimação ou vista pessoal.

A publicação do DJe representa uma economia significativa para o Poder Judiciário, pois dispensa a manutenção de um Parque Gráfico destinado a impressão e distribuição do diário em papel.

O sítio do Poder Judiciário do Ceará já possui uma consulta ao Diário da Justiça, porém o arquivo disponibilizado não substitui a versão impressa por não atender ao disposto na lei Nº 11.419, referente à sua assinatura digital.

5.3. Acesso ao Infojud

Uma das demandas dos magistrados do Poder Judiciário Cearense é a utilização do sistema Infojud.

O sistema dá acesso aos juízes, via Internet, a dados cadastrais de pessoas físicas e jurídicas na Receita Federal. O Poder Judiciário já é autorizado a pedir essas informações, com previsão constitucional, autorizadas pelo artigo 198, parágrafo 1º, do Código Tributário Nacional (Lei 5.172/66). O Infojud permite apenas que o processo de solicitação seja feito via Internet, dispensando o uso de ofícios em papel e agilizando a obtenção dos dados pela Justiça.

Os dados disponíveis aos magistrados por meio do sistema englobam as principais informações fiscais coletadas pela Receita junto aos contribuintes: declaração do Imposto de Renda Pessoa Física (IRPF) e do Imposto de Renda Pessoa Jurídica (IRPJ), Imposto Territorial Rural (ITR) e Imposto da Pessoa Jurídica Simples, os dados cadastrais da Pessoa Física e da Pessoa Jurídica e a Declaração sobre Operações Imobiliárias (DOI).

Dessa forma, os juízes terão mais subsídios sobre a movimentação bancária e de transações imobiliárias realizadas por pessoas e empresas investigadas em processos. Segundo o juiz Friedmann Wendpap[43] “Na seara criminal o mapa do patrimônio, da movimentação financeira e até mesmo da existência legal do indivíduo, ficarão nítidos para o julgador, sem a mora dos ofícios e das fotocópias. Penso que na dosimetria da pena haverá uma larga possibilidade de uso das

[43] Publicação disponível em http://www.serpro.gov.br/imprensa/publicacoes/Tema/tema_192/materias/infojud-o-judiciario-na-era-digital. Acesso em 20.07.2008 às 15:00.

informações postas à disposição dos juízes. Na Justiça do Trabalho haverá facilitação dos atos de execução, pois a localização de bens do devedor será imediata e, além disso, combinando-se o uso do Infojud com o BacenJud - Sis- tema de Atendimento das Solicitações do Poder Judiciário do Banco Central do Brasil, os bloqueios de dinheiro em bancos poderão ser mais certeiros".

A utilização do Infojud nas diversas instâncias do Judiciário foi disponibilizada através da assinatura do convênio entre a Receita e o CNJ. O convênio permitiu o acesso dos tribunais estaduais ao sistema. De acordo com Andréa Fernandes[44] "Além do óbvio ganho interno, através da possibilidade de realocação de um grande quantitativo de servidores hoje dedicados exclusivamente ao atendimento dos ofícios judiciais de pedidos de informações à RFB, o Infojud poderá auxiliar bastante na agilização do andamento dos procedimentos de investigação e tramitação dos processos na esfera judicial, representando, dessa forma, uma contribuição, não somente limitada ao Poder Judiciário ou à Administração Pública, mas a toda sociedade brasileira".

O Convênio celebrado pelo CNJ tem como objeto do o fornecimento de informações cadastrais e econômico-fiscais das bases de dados da RFB, em atendimento às requisições judiciais oriundas de órgãos do Poder Judiciário, por meio do sistema Infojudi - Informações ao Poder Judiciário no Centro Virtual de Atendimento ao Contribuinte - e-CAC da RFB.

Dentre as exigências impostas pelo Convênio para utilização do sistema podemos destacar que as informações a serem fornecidas pela RFB dependem do encaminhamento de requisição à RFB por meio eletrônico, com a utilização de certificação digital e que somente poderão ser recebidas e acessadas diretamente pelo magistrado responsável pela requisição, devidamente certificado por Autoridade Certificadora Integrante do ICP - Brasil.

Para utilização do Infojud, portanto, torna-se necessária a aquisição de certificados digitais para todos os membros do Poder Judiciário que pretendem acessá-lo.

5.4. Processo Judicial Digital

[44] Publicação disponível em http://www.serpro.gov.br/imprensa/publicacoes/Tema/tema_192/materias/infojud-o-judiciario-na-era-digital. Acesso em 20.07.2008 às 15:00.

A emenda constitucional 45 instituiu o princípio da razoável duração do processo dentro das garantias fundamentais asseguradas a cada indivíduo, através do inciso LXXVIII do art. 5º da Constituição Federal de 1988.

A temática do tempo do processo tratada ao nível de garantia fundamental advem da insatisfação da sociedade com a prestação da tutela jurisdicional e do entendimento que a jurisdição não deve ser apenas ser prestada pelo Estado como decorrência do direito de ação, mas que a tutela jurisdicional deve ser efetiva, tempestiva e adequada, sendo atribuição do Estado alcançar este objetivo.

Mais do que reformar a legislação em vigor, é necessário dotar o Poder Judiciário de uma estrutura apta a receber e processar, com celeridade, as demandas judiciais. Para tanto, é imprescindível a informatização completa do Judiciário.

De acordo com Carreira Alvim[45]:

> O problema do acesso à Justiça não é uma questão de "entrada", pois, pela porta gigantesca desse templo chamado Justiça, entra quem quer, seja através de advogado pago, seja de advogado mantido pelo Poder Público, seja de advogado escolhido pela própria parte, sob os auspícios da assistência judiciária, não havendo, sob esse prisma, nenhuma dificuldade de acesso.
> O problema é de "saída", pois todos entram, mas poucos conseguem sair num prazo razoável, e os que saem, fazem-no pelas "portas de emergência", representadas pelas tutelas antecipatórias, pois a grande maioria fica lá dentro, rezando, para conseguir sair com vida.
> Este é o grande problema e o grande obstáculo que enfrentamos, cabendo à doutrina, através de concepções voltadas para a realidade brasileira, sem copiar modelos estrangeiros, contribuir para a formação de uma onda de "descesso" (saída) da Justiça, para que o sistema judiciário se torne mais racional na entrada, mas, também, mais racional e humano na saída.

Uma das inciativas para acelerar a prestação jurisdicional foi a criação do processo judicial digital, também chamado de processo virtual ou de processo eletrônico, que pode ser definido como um sistema de informática que reproduz todo o procedimento judicial em meio eletrônico, substituindo o registro dos atos realizados no papel por armazenamento e manipulação dos autos em meio digital.

O Poder Judiciário do Estado do Ceará recebeu do Conselho Nacional de Justiça a doação de um sistema informatizado e equipamentos para implantação do processo judicial eletrônico.

---

[45] CARREIRA ALVIM, José Eduardo. **Justiça: acesso e descesso**. Disponível em: <http://jus2.uol.com.br/doutrina/texto.asp?id=4078>. Acesso em: Acesso em 20.07.2008 às 18:00.

O sistema doado pelo CNJ, denominado Projudi, é um programa de computador que pode ser utilizado através da Internet e permite a completa substituição do papel por autos processuais digitais.

Segundo as informações que constam no sítio do Tribunal de Justiça na Internet o funcionamento do Projudi é bastante simples e seguro. Os advogados e os cidadãos que desejem ingressar com alguma reclamação nos Juizados Especiais podem utilizar a Internet ou se dirigir ao setor de atendimento dos juizados. Esses pedidos serão registrados eletronicamente, com distribuição e cadastramento automático do processo. A partir daí todos os atos serão realizados utilizando-se o computador, com a eliminação do papel.

Somente usuários cadastrados previamente terão acesso ao sistema. A consulta e a prática de atos processuais poderão ser realizadas na Internet ou na sede do Juizado Especial. Os advogados que se cadastrarem receberão senha de acesso ao sistema e também certificados digitais que darão a garantia de identificação, segurança, autenticidade e fidedignidade dos documentos.

Os certificados emitidos pelo Projudi são internos à aplicação, portanto são válidos apenas para utilização no sistema.

Para receber o certificado o advogado deverá ser feito em uma unidade dos Juizados Especiais, levando os originais com cópia autenticada do RG, CPF, carteira da OAB, comprovante de Residência e uma foto 3x4.

No momento do cadastro na unidade será realizada a criação do certificado digital, que é um arquivo que será utilizado para assinar os documentos que serão inseridos no sistema. Este deverá ser gravado num pen-drive e/ou no disco rígido do computador pessoal para facilitar o seu transporte.

Os magistrados e servidores também deverão ser cadastrados pelo administrador do sistema e gravar o certificado digital gerado no processo em sua estação de trabalho.

O Projudi, atualmente, não permite o uso de certificados emitidos pela ICP-Brasil. Como vantagens da utilização do certificados vinculados à ICP-Brasil podemos citar a sua validade como uma identidade digital em todas as transações eletrônicas que possuam certificação digital, bem como a dispensa da realização do cadastro prévio no Poder Judiciário, visto que a validação da indentificação do titular do certificado já foi conferida por uma Autoridade de Registro. Para os advogados uma desvantagem seria o custo de aquisição do certificado.

A implantação da certificação digital no Poder Judiciário levaria a todos os magistrados e servidores utilizarem um certificado vinculádo AC-Jus para efetuar a assinatura digital de todos os documentos manuseados do processo eletrônico.

Algumas unidades do Poder Judiciário do Ceará realizam a colheita da prova oral em mídia digital. Segundo o Juiz Ezequias Silva Leite[46], o procedimento é seguro, idôneo e prático, e pode ser utilizado em todas as Varas da Justiça do Estado, seja nas ações cíveis ou penais. "Esse método não cria nem altera o ato processual. Apenas muda a forma do registro da prova, que passa a ser através de arquivo eletrônico de imagem e som, feito por meio de uma micro-câmera de vídeo e dois microfones de lapela", explica o magistrado.

Entre os benefícios, citou a celeridade, a fidelidade e a oralidade como pontos que, na mídia digital, superam o processo escrito. O ganho de tempo nos interrogatórios, o baixo custo do sistema – composto apenas por microfone de lapela e webcam com tripé –, além das reações corporais que podem ser captadas são algumas das vantagens que, segundo ele, podem auxiliar os magistrados em suas decisões.

Os arquivos digitais com os vídeos dos testemunhos colhidos devem ser assinados eletronicamente pelos magistrados com seu certificado vinculado a AC-Jus. Somente com este procedimento haverá garantia da integridade e autenticidade do arquivo.

5.5. Regulamentação da Certificação Digital

Diante das diversas aplicações e uso da certificação digital o Conselho Nacional de Justiça através da Recomendação n.º 12 de 14 de setembro de 2007 resolveu recomendar aos Tribunais Regionais Federais, aos Tribunais Regionais do Trabalho, aos órgãos União e dos Estados e aos Tribunais de Justiça dos Estados e do Distrito Federal e Territórios que regulamentem e efetivem o uso de formas eletrônicas de assinatura, no menor prazo possível, segundo as suas possibilidades e o atual estágio de desenvolvimento técnico.

---

[46] Disponível em http://www.tj.ce.gov.br/corregedoria/correg_noticia.asp?ID=297. Acesso em 21.08.2008 às 14:00.

Após análise das tecnologias disponíveis no mercado e das necessidades do Poder Judiciário do Estado do Ceará o seguinte modelo de regulamentação poderá ser proposto para o uso da certificação digital:

O PRESIDENTE DO TRIBUNAL DE JUSTIÇA DO ESTADO CEARÁ, no uso de suas atribuições legais,

CONSIDERANDO a instituição da Infra-estrutura de Chaves Públicas Brasileira (ICP-Brasil) pela medida provisória nº. 2.200-2, de 24 de agosto de 2001, para garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras;

CONSIDERANDO que, na forma do §1º do art. 10 da Medida Provisória nº. 2.200-2, as declarações constantes dos documentos em forma eletrônica produzidos com a utilização de processo de certificação disponibilizado pela icp-brasil presumem-se verdadeiros em relação aos signatários, na forma originalmente prevista pelo art. 131 da lei nº. 3.071, de 1º de janeiro de 1916 (antigo código civil), atualmente constante do art. 219 da lei 10.406, de 10 de janeiro de 2002;

CONSIDERANDO que na forma do parágrafo único do art. 1º da Lei n.º 11.419 de 19 de dezembro de 2006, todos os atos processuais do processo eletrônico serão assinados eletronicamente;

CONSIDERANDO que na forma do §2º do art. 1º da Lei n.º 11.419 de 19 de dezembro de 2006, a assinatura eletrônica admite como de identificação inequívoca do signatário a assinatura digital baseada em certificado digital emitido por Autoridade Certificadora credenciada;

CONSIDERANDO a Recomendação n. 12, de 14 de setembro de 2007, do Conselho Nacional de Justiça, para que seja regulamentado e efetivado o uso de formas eletrônicas de assinatura;

CONSIDERANDO a necessidade de regulamentar a utilização da tecnologia de certificação digital e assinatura digital de documentos eletrônicos no âmbito do Poder Judiciário do Estado do Ceará, adaptados os serviços às novas tecnologias que possibilitam a facilidade de acesso e a racionalização de procedimentos, com a decorrente agilização da prestação jurisdiciona.

RESOLVE:

Art. 1º Instituir, no âmbito do Poder Judiciário do Estado do Ceará, a utilização das tecnologias de certificação digital e assinatura digital de documentos eletrônicos.

Parágrafo único - a emissão de Certificados Digitais para magistrados, servidores e equipamentos far-se-á segundo a infra-estrutura de chaves públicas brasileira (ICP-Brasil) através de Autoridade Certificadora vinculada a AC-JUS.

Art. 2º Os certificados serão disponibilizados pela Secretaria de Tecnologia da Informação a servidores e magistrados, conforme o planejamento estabelecido pela direção do Tribunal de Justiça do Ceará.

Art. 3º As chaves criptográficas utilizadas deverão ser geradas e armazenadas em dispositivo eletrônico seguro token, protegido por senha de acesso.

Art. 4º O dispositivo eletrônico "token", será entregue ao titular selecionado, que no ato do recebimento assinará Termo de Responsabilidade quanto à guarda e conservação do dispositivo.

§ 1º No caso de danos, extravio, furto ou roubo do dispositivo, o usuário deverá comunicar imediatamente a Secretaria de Tecnologia, que tomará as providências necessárias para evitar o seu uso indevido.

§ 2º Se a ocorrência for de dano, extravio ou furto do equipamento, o usuário será responsável pelo ressarcimento ao Tribunal de Justiça, pelo seu valor de mercado.

§ 3º Por decisão fundamentada do Presidente do Tribunal de Justiça ou por desligamento do Poder Judiciário, o detentor do certificado digital nos sistemas de informática, compatíveis com essa tecnologia, terá seu acesso bloqueado.

§ 4º Em qualquer das hipóteses previstas no parágrafo anterior, o usuário devolverá ao Tribunal o dispositivo eletrônico "token", fazendo-se remissão do fato no termo de entrega.

Art. 5º A assinatura digital, produto da certificação, é de caráter sigiloso e intransferível e constituí atributo de segurança que identifica seu titular conferindo autenticidade aos documentos e comunicações por ele elaboradas.

§ 1º Os documentos eletrônicos emitidos pelos sistemas informatizados do Poder Judiciário e assinados digitalmente possuem a validade daqueles físicos ou firmados manualmente.

§ 3º Será de única responsabilidade do usuário, inclusive suas conseqüências, o mau uso da assinatura digital, entre os quais a utilização por terceiros e o sujeitará às penas funcionais disciplinares, sem prejuízo das ações penais correspondentes.

Art. 6º Os certificados digitais possuem validade de três anos e, após esse período, poderão ser renovados pelo Poder Judiciário do Ceará.

Parágrafo único. O gerenciamento do período de validade e da renovação dos certificados digitais será de responsabilidade da Secretaria de Tecnologia da Informação, que antes de expirar o prazo de que trata o caput deste artigo, no caso de opção do Poder Judiciário pela manutenção dos certificados, deverá entrar em contato com os respectivos servidores e magistrados para que, com o auxílio da Secretaria, realizem o procedimento de renovação.

Art. 7º Os servidores e magistrados designados a receber os certificados digitais deverão fornecer, de modo completo e preciso, todos os documentos e informações necessárias para a sua identificação, incluindo uma foto 3X4 recente.

§ 1º Serão fornecidas cópias dos citados documentos ao agente da autoridade de registro do certificado digital, as quais poderão ser na forma autenticada ou cópias simples com a apresentação dos documentos originais no ato da entrega.

§ 2º Os documentos de que trata o parágrafo anterior são:

I - Cédula de Identidade (RG, carteira profissional, documento funcional, carteira de habilitação).

II - Cadastro de Pessoa Física – CPF.

III - Um comprovante de residência recente (emitido à, no máximo, 3 meses)

A Infra-estrutura de Chaves Públicas ICP-Brasil criou um conjunto de normas, procedimentos e tecnologias que devem ser utilizadas pelo Poder Judiciário do Estado do Ceará para promover a tão esperada celeridade da justiça.

A regulamentação proposta será o primeiro passo para a elaboração de um planejamento e estimulação do uso de certificação digital. O Poder Judiciário conta com uma equipe técnica capaz de prover soluções, além das aqui expostas, criando inúmeras aplicações.

6. CONSIDERAÇÕES FINAIS

Diante da evolução da forma como os documentos são produzidos e armazenados, passando do meio físico em papel para o formato eletrônico, identificamos as premissas essenciais para garantir a eficácia jurídica dos documentos eletrônicos – integridade, autenticidade e tempestividade.

Foi demonstrado que a adoção dos conceitos da criptografia pelos sistemas informatizados permitiu a criação de técnicas que garantem, através de recursos como a assinatura eletrônica e o sigilo das informações armazenadas e trafegadas via internet, a identificação inequívoca das partes envolvidas em uma transação eletrônica, bem como verificar se as mensagens enviadas foram entregues sem alterações e no momento em que foram realizadas. Tais características permitem ao documento eletrônico alcançar as premissas necessárias a obtenção de sua eficácia probante.

O processo de disseminação do uso dos serviços disponibilizados pelas técnicas de criptografia exigiu a criação de uma infra-estrutura de chaves públicas – ICP. A ICP define um conjunto de normas e procedimentos para distribuir e garantir a titularidade das chaves públicas utilizadas para a assinatura digital. Esta estrutura utiliza a certificação digital com o objetivo de prover a identidade eletrônica dos indivíduos e equipamentos no mundo virtual.

Expomos a legislação responsável pelo modelo da infra-estrutura de Chaves Públicas Brasileira através da Medida Provisória 2.200-2 que procurou estabelecer os efeitos jurídicos produzidos por uma declaração de vontade assinada com certificado emitido no âmbito da ICP-Brasil.

Diante disso, foram propostas algumas aplicações que fazem uso da certificação digital e podem ser implantadas no Poder Judiciário do Estado do Ceará. Algumas destas aplicações, como o Diário da Justiça Eletrônico e o acesso ao sistema Infojud, são de fácil implantação, necessitado apenas da aquisição de certificados digitais.

Para que seja iniciado o uso da certificação digital no Poder Judiciário do Ceará faz-se necessária elaboração de uma regulamentação, conforme solicitado pela Recomendação n.º 12 do Conselho Nacional de Justiça. Este trabalho propôs um modelo de regulamento capaz de estabelecer os procedimentos necessários através de um provimento a ser emitido pela Presidência do Tribunal de Justiça.

Em resumo, a adoção das transações eletrônicas seguras e a implantação do processo eletrônico digital transformou-se em uma realidade sem volta, cabendo ao Poder Judiciário adequar sua estrutura para adaptar-se às necessidades impostas pela sociedade.

7. REFERÊNCIAS

Livros:

MONTEIRO, Emiliano S. **Certificados Digitais: conceitos e práticas**. 1. Ed. São Paulo: Brasport, 2007.

SILVA, Lino Sarlo. **Public Key Infrastructure**. 1 Ed. São Paulo: Novatec Editora, 2004.

THEODORO, Humberto Jr. **Curso de Direito Processual Civil**. 44 ed. Rio de Janeiro. Forense. 2006

Trabalho de Grau:

IGNACZAK, Luciano. Dissertação de Mestrado. Um Novo Modelo de Infra-estrutura de Chaves Púublicas para Uso no Brasil Utilizando Aplicativos com o Código Fonte Aberto. Universidade Federal de Santa Catarina, 2002.

MIGNONI, Maria Eloísa. Dissertação de Mestrado. Políticas e Declaração de Práticas de Certificação Digital para UFSC. Universidade de Santa Catarina, 2002.

DIAS, Júlio da Silva. Tese de doutorado. Confiança no Documento Eletrônico. Universidade de Santa Catarina, 2003.

Documentos em meio eletrônico:

GANDINI, João Agnaldo Donizeti; SALOMÃO, Diana Paola da Silva et al. A segurança dos documentos digitais. Jus Navigandi, Disponível em: http://jus2.uol.com.br/doutrina/texto.asp?id=2677. Acesso em: 07.07.2008 às 09:00.

SANTOS, Moacyr Amaral apud MARCACINI, Augusto Tavares Rosa. Documento Eletrônico como Meio de Prova. Disponível em: http://www.infodireito.com.br/info/index.php?option=com_content&task=view&id=44&Itemid=42. Acesso em: 07.07.2008 às 15:00.

GANDINI, João Agnaldo Donizeti; SALOMÃO, Diana Paola da Silva et al. A segurança dos documentos digitais. Jus Navigandi, Disponível em: http://jus2.uol.com.br/doutrina/texto.asp?id=2677. Acesso em: 07.07.2008 às 09:00

MARCACINI, Augusto Tavares Rosa. Documento Eletrônico como Meio de Prova. Disponível em: http://www.infodireito.com.br/info/index.php?option=com_content&task=view&id=44&Itemid=42. Acesso em: 07.07.2008 às 15:00.

GIANNANTONIO, E. Manuale apud TRUJILLO, Elcio. O Mercosul e a documentação eletrônica. Disponível em: www.senado.gov.br/web/cegraf/ril/Pdf/pdf_135/r135-22.pdf. Acesso em 08.07.200às 18:00.

TADANO, Katiucia Yumi. GED: Assinatura Digital e Validade Jurídica de Documentos Eletrônicos. Disponível em: http://www.arquivar.com.br/espaco_profissional/sala_leitura/teses-dissertacoes-e-monografias/GED_Assinatura_Digital.pdf. Acesso em 12.07.2008 às 13:00.

TRAIN, Sheila. Identidade Digital. Disponível em: https://www.certisign.com.br/treinamento/guias-gratuitos/pdf/livro_id_digital_certificado.pdf. Acesso em 15.07.2008 às 21:00.

RIBEIRO, Alexandre Menezes. A Infra-estrutura de Chaves Públicas Brasileira e suas bases para a Auditoria em Segurança da Informação. Disponível em: http://www.arquivar.com.br/espaco_profissional/sala_leitura/teses-dissertacoes-e-monografias/Chaves_Publicas_Brasileira.pdf. Acesso em 19.07.2008 às 18:00.

Leiaute dos Certificados Digitais Cert-JUS Versão 2.0. Disponível em http://www.acjus.gov.br/repositorio/Docs_dpc_ps. Acessado em 20.07.2008 às 12:00

Publicação disponível em http://www.serpro.gov.br/imprensa/publicacoes/Tema/tema_192/materias/infojud-o-judiciario-na-era-digital. Acesso em 20.07.2008 às 15:00.

Publicação disponível em http://www.tj.ce.gov.br/corregedoria/correg_noticia.asp?ID=297. Acesso em 21.08.2008 às 14:00.

TEJADA,Sérgio. Só a Tecnologia Reduz Custos e Agiliza os Processos. Disponível em: http://www.serpro.gov.br/imprensa/publicacoes/Tema/tema_190/materias/entrevista/. Acesso em 08.07.2008 às 13:00.

ANEXOS

ANEXO A

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

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

Art. 1º Fica instituída a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, para garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras.

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

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

I - Ministério da Justiça;

II - Ministério da Fazenda;

III - Ministério do Desenvolvimento, Indústria e Comércio Exterior;

IV - Ministério do Planejamento, Orçamento e Gestão;

V - Ministério da Ciência e Tecnologia;

VI - Casa Civil da Presidência da República; e

VII - Gabinete de Segurança Institucional da Presidência da República.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

§ 1º O Diretor-Presidente do ITI poderá requisitar, para ter exercício exclusivo na Diretoria de Infra-Estrutura de Chaves Públicas, por período não superior a um ano,

servidores, civis ou militares, e empregados de órgãos e entidades integrantes da Administração Pública Federal direta ou indireta, quaisquer que sejam as funções a serem exercidas.

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

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

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

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

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

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

ANEXO B

LEI Nº 11.419, DE 19 DE DEZEMBRO DE 2006.

O PRESIDENTE DA REPÚBLICA Faço saber que o Congresso Nacional decreta e eu sanciono a seguinte Lei:

CAPÍTULO I

DA INFORMATIZAÇÃO DO PROCESSO JUDICIAL

Art. 1º O uso de meio eletrônico na tramitação de processos judiciais, comunicação de atos e transmissão de peças processuais será admitido nos termos desta Lei.

§ 1º Aplica-se o disposto nesta Lei, indistintamente, aos processos civil, penal e trabalhista, bem como aos juizados especiais, em qualquer grau de jurisdição.

§ 2º Para o disposto nesta Lei, considera-se:

I - meio eletrônico qualquer forma de armazenamento ou tráfego de documentos e arquivos digitais;

II - transmissão eletrônica toda forma de comunicação a distância com a utilização de redes de comunicação, preferencialmente a rede mundial de computadores;

III - assinatura eletrônica as seguintes formas de identificação inequívoca do signatário:

a) assinatura digital baseada em certificado digital emitido por Autoridade Certificadora credenciada, na forma de lei específica;

b) mediante cadastro de usuário no Poder Judiciário, conforme disciplinado pelos órgãos respectivos.

Art. 2º O envio de petições, de recursos e a prática de atos processuais em geral por meio eletrônico serão admitidos mediante uso de assinatura eletrônica, na forma do art. 1º desta Lei, sendo obrigatório o credenciamento prévio no Poder Judiciário, conforme disciplinado pelos órgãos respectivos.

§ 1º O credenciamento no Poder Judiciário será realizado mediante procedimento no qual esteja assegurada a adequada identificação presencial do interessado.

§ 2º Ao credenciado será atribuído registro e meio de acesso ao sistema, de modo a preservar o sigilo, a identificação e a autenticidade de suas comunicações.

§ 3º Os órgãos do Poder Judiciário poderão criar um cadastro único para o credenciamento previsto neste artigo.

Art. 3º Consideram-se realizados os atos processuais por meio eletrônico no dia e hora do seu envio ao sistema do Poder Judiciário, do que deverá ser fornecido protocolo eletrônico.

Parágrafo único. Quando a petição eletrônica for enviada para atender prazo processual, serão consideradas tempestivas as transmitidas até as 24 (vinte e quatro) horas do seu último dia.

CAPÍTULO II

DA COMUNICAÇÃO ELETRÔNICA DOS ATOS PROCESSUAIS

Art. 4º Os tribunais poderão criar Diário da Justiça eletrônico, disponibilizado em sítio da rede mundial de computadores, para publicação de atos judiciais e administrativos próprios e dos órgãos a eles subordinados, bem como comunicações em geral.

§ 1º O sítio e o conteúdo das publicações de que trata este artigo deverão ser assinados digitalmente com base em certificado emitido por Autoridade Certificadora credenciada na forma da lei específica.

§ 2º A publicação eletrônica na forma deste artigo substitui qualquer outro meio e publicação oficial, para quaisquer efeitos legais, à exceção dos casos que, por lei, exigem intimação ou vista pessoal.

§ 3º Considera-se como data da publicação o primeiro dia útil seguinte ao da disponibilização da informação no Diário da Justiça eletrônico.

§ 4º Os prazos processuais terão início no primeiro dia útil que seguir ao considerado como data da publicação.

§ 5º A criação do Diário da Justiça eletrônico deverá ser acompanhada de ampla divulgação, e o ato administrativo correspondente será publicado durante 30 (trinta) dias no diário oficial em uso.

Art. 5º As intimações serão feitas por meio eletrônico em portal próprio aos que se cadastrarem na forma do art. 2º desta Lei, dispensando-se a publicação no órgão oficial, inclusive eletrônico.

§ 1º Considerar-se-á realizada a intimação no dia em que o intimando efetivar a consulta eletrônica ao teor da intimação, certificando-se nos autos a sua realização.

§ 2º Na hipótese do § 1º deste artigo, nos casos em que a consulta se dê em dia não útil, a intimação será considerada como realizada no primeiro dia útil seguinte.

§ 3º A consulta referida nos §§ 1º e 2º deste artigo deverá ser feita em até 10 (dez) dias corridos contados da data do envio da intimação, sob pena de considerar-se a intimação automaticamente realizada na data do término desse prazo.

§ 4º Em caráter informativo, poderá ser efetivada remessa de correspondência eletrônica, comunicando o envio da intimação e a abertura automática do prazo processual nos termos do § 3º deste artigo, aos que manifestarem interesse por esse serviço.

§ 5º Nos casos urgentes em que a intimação feita na forma deste artigo possa causar prejuízo a quaisquer das partes ou nos casos em que for evidenciada qualquer tentativa de

burla ao sistema, o ato processual deverá ser realizado por outro meio que atinja a sua finalidade, conforme determinado pelo juiz.

§ 6º As intimações feitas na forma deste artigo, inclusive da Fazenda Pública, serão consideradas pessoais para todos os efeitos legais.

Art. 6º Observadas as formas e as cautelas do art. 5º desta Lei, as citações, inclusive da Fazenda Pública, excetuadas as dos Direitos Processuais Criminal e Infracional, poderão ser feitas por meio eletrônico, desde que a íntegra dos autos seja acessível ao citando.

Art. 7º As cartas precatórias, rogatórias, de ordem e, de um modo geral, todas as comunicações oficiais que transitem entre órgãos do Poder Judiciário, bem como entre os deste e os dos demais Poderes, serão feitas preferentemente por meio eletrônico.

CAPÍTULO III

DO PROCESSO ELETRÔNICO

Art. 8º Os órgãos do Poder Judiciário poderão desenvolver sistemas eletrônicos de processamento de ações judiciais por meio de autos total ou parcialmente digitais, utilizando, preferencialmente, a rede mundial de computadores e acesso por meio de redes internas e externas.

Parágrafo único. Todos os atos processuais do processo eletrônico serão assinados eletronicamente na forma estabelecida nesta Lei.

Art. 9º No processo eletrônico, todas as citações, intimações e notificações, inclusive da Fazenda Pública, serão feitas por meio eletrônico, na forma desta Lei.

§ 1º As citações, intimações, notificações e remessas que viabilizem o acesso à íntegra do processo correspondente serão consideradas vista pessoal do interessado para todos os efeitos legais.

§ 2º Quando, por motivo técnico, for inviável o uso do meio eletrônico para a realização de citação, intimação ou notificação, esses atos processuais poderão ser praticados segundo as regras ordinárias, digitalizando-se o documento físico, que deverá ser posteriormente destruído.

Art. 10. A distribuição da petição inicial e a juntada da contestação, dos recursos e das petições em geral, todos em formato digital, nos autos de processo eletrônico, podem ser feitas diretamente pelos advogados públicos e privados, sem necessidade da intervenção do cartório ou secretaria judicial, situação em que a autuação deverá se dar de forma automática, fornecendo-se recibo eletrônico de protocolo.

§ 1º Quando o ato processual tiver que ser praticado em determinado prazo, por meio de petição eletrônica, serão considerados tempestivos os efetivados até as 24 (vinte e quatro) horas do último dia.

§ 2º No caso do § 1º deste artigo, se o Sistema do Poder Judiciário se tornar indisponível por motivo técnico, o prazo fica automaticamente prorrogado para o primeiro dia útil seguinte à resolução do problema.

§ 3º Os órgãos do Poder Judiciário deverão manter equipamentos de digitalização e de acesso à rede mundial de computadores à disposição dos interessados para distribuição de peças processuais.

Art. 11. Os documentos produzidos eletronicamente e juntados aos processos eletrônicos com garantia da origem e de seu signatário, na forma estabelecida nesta Lei, serão considerados originais para todos os efeitos legais.

§ 1º Os extratos digitais e os documentos digitalizados e juntados aos autos pelos órgãos da Justiça e seus auxiliares, pelo Ministério Público e seus auxiliares, pelas procuradorias, pelas autoridades policiais, pelas repartições públicas em geral e por advogados públicos e privados têm a mesma força probante dos originais, ressalvada a alegação motivada e fundamentada de adulteração antes ou durante o processo de digitalização.

§ 2º A argüição de falsidade do documento original será processada eletronicamente na forma da lei processual em vigor.

§ 3º Os originais dos documentos digitalizados, mencionados no § 2º deste artigo, deverão ser preservados pelo seu detentor até o trânsito em julgado da sentença ou, quando admitida, até o final do prazo para interposição de ação rescisória.

§ 4º (VETADO)

§ 5º Os documentos cuja digitalização seja tecnicamente inviável devido ao grande volume ou por motivo de ilegibilidade deverão ser apresentados ao cartório ou secretaria no prazo de 10 (dez) dias contados do envio de petição eletrônica comunicando o fato, os quais serão devolvidos à parte após o trânsito em julgado.

§ 6º Os documentos digitalizados juntados em processo eletrônico somente estarão disponíveis para acesso por meio da rede externa para suas respectivas partes processuais e para o Ministério Público, respeitado o disposto em lei para as situações de sigilo e de segredo de justiça.

Art. 12. A conservação dos autos do processo poderá ser efetuada total ou parcialmente por meio eletrônico.

§ 1º Os autos dos processos eletrônicos deverão ser protegidos por meio de sistemas de segurança de acesso e armazenados em meio que garanta a preservação e integridade dos dados, sendo dispensada a formação de autos suplementares.

§ 2º Os autos de processos eletrônicos que tiverem de ser remetidos a outro juízo ou instância superior que não disponham de sistema compatível deverão ser impressos em papel, autuados na forma dos arts. 166 a 168 da Lei nº 5.869, de 11 de janeiro de 1973 - Código de Processo Civil, ainda que de natureza criminal ou trabalhista, ou pertinentes a juizado especial.

§ 3º No caso do § 2º deste artigo, o escrivão ou o chefe de secretaria certificará os autores ou a origem dos documentos produzidos nos autos, acrescentando, ressalvada a hipótese de existir segredo de justiça, a forma pela qual o banco de dados poderá ser acessado para aferir a autenticidade das peças e das respectivas assinaturas digitais.

§ 4º Feita a autuação na forma estabelecida no § 2º deste artigo, o processo seguirá a tramitação legalmente estabelecida para os processos físicos.

§ 5º A digitalização de autos em mídia não digital, em tramitação ou já arquivados, será precedida de publicação de editais de intimações ou da intimação pessoal das partes e de seus procuradores, para que, no prazo preclusivo de 30 (trinta) dias, se manifestem sobre o desejo de manterem pessoalmente a guarda de algum dos documentos originais.

Art. 13. O magistrado poderá determinar que sejam realizados por meio eletrônico a exibição e o envio de dados e de documentos necessários à instrução do processo.

§ 1º Consideram-se cadastros públicos, para os efeitos deste artigo, dentre outros existentes ou que venham a ser criados, ainda que mantidos por concessionárias de serviço público ou empresas privadas, os que contenham informações indispensáveis ao exercício da função judicante.

§ 2º O acesso de que trata este artigo dar-se-á por qualquer meio tecnológico disponível, preferentemente o de menor custo, considerada sua eficiência.

§ 3º (VETADO)

CAPÍTULO IV

DISPOSIÇÕES GERAIS E FINAIS

Art. 14. Os sistemas a serem desenvolvidos pelos órgãos do Poder Judiciário deverão usar, preferencialmente, programas com código aberto, acessíveis ininterruptamente por meio da rede mundial de computadores, priorizando-se a sua padronização.

Parágrafo único. Os sistemas devem buscar identificar os casos de ocorrência de prevenção, litispendência e coisa julgada.

Art. 15. Salvo impossibilidade que comprometa o acesso à justiça, a parte deverá informar, ao distribuir a petição inicial de qualquer ação judicial, o número no cadastro de pessoas físicas ou jurídicas, conforme o caso, perante a Secretaria da Receita Federal.

Parágrafo único. Da mesma forma, as peças de acusação criminais deverão ser instruídas pelos membros do Ministério Público ou pelas autoridades policiais com os números de registros dos acusados no Instituto Nacional de Identificação do Ministério da Justiça, se houver.

Art. 16. Os livros cartorários e demais repositórios dos órgãos do Poder Judiciário poderão ser gerados e armazenados em meio totalmente eletrônico.

Art. 17. (VETADO)

Art. 18. Os órgãos do Poder Judiciário regulamentarão esta Lei, no que couber, no âmbito de suas respectivas competências.

Art. 19. Ficam convalidados os atos processuais praticados por meio eletrônico até a data de publicação desta Lei, desde que tenham atingido sua finalidade e não tenha havido prejuízo para as partes.

Art. 20. A Lei nº 5.869, de 11 de janeiro de 1973 - Código de Processo Civil, passa a vigorar com as seguintes alterações:

"Art. 38. .....

Parágrafo único. A procuração pode ser assinada digitalmente com base em certificado emitido por Autoridade Certificadora credenciada, na forma da lei específica." (NR)

"Art. 154. .....

Parágrafo único. (Vetado). (VETADO)

§ 2º Todos os atos e termos do processo podem ser produzidos, transmitidos, armazenados e assinados por meio eletrônico, na forma da lei." (NR)

"Art. 164. .....

Parágrafo único. A assinatura dos juízes, em todos os graus de jurisdição, pode ser feita

eletronicamente, na forma da lei." (NR)

"Art. 169. .....

§ 1º É vedado usar abreviaturas.

§ 2º Quando se tratar de processo total ou parcialmente eletrônico, os atos processuais praticados na presença do juiz poderão ser produzidos e armazenados de modo integralmente digital em arquivo eletrônico inviolável, na forma da lei, mediante registro em termo que será assinado digitalmente pelo juiz e pelo escrivão ou chefe de secretaria, bem como pelos advogados das partes.

§ 3º No caso do § 2º deste artigo, eventuais contradições na transcrição deverão ser suscitadas oralmente no momento da realização do ato, sob pena de preclusão, devendo o juiz decidir de plano, registrando-se a alegação e a decisão no termo." (NR)

"Art. 202. .....

.....

§ 3º A carta de ordem, carta precatória ou carta rogatória pode ser expedida por meio eletrônico, situação em que a assinatura do juiz deverá ser eletrônica, na forma da lei." (NR)

"Art. 221. .....

.....

IV - por meio eletrônico, conforme regulado em lei própria." (NR)

"Art. 237. .....

Parágrafo único. As intimações podem ser feitas de forma eletrônica, conforme regulado em lei própria." (NR)

"Art. 365. .....

.....

V - os extratos digitais de bancos de dados, públicos e privados, desde que atestado pelo seu emitente, sob as penas da lei, que as informações conferem com o que consta na origem;

VI - as reproduções digitalizadas de qualquer documento, público ou particular, quando juntados aos autos pelos órgãos da Justiça e seus auxiliares, pelo Ministério Público e seus auxiliares, pelas procuradorias, pelas repartições públicas em geral e por advogados públicos ou privados, ressalvada a alegação motivada e fundamentada de adulteração antes ou durante o processo de digitalização.

§ 1º Os originais dos documentos digitalizados, mencionados no inciso VI do **caput** deste artigo, deverão ser preservados pelo seu detentor até o final do prazo para interposição de ação rescisória.

§ 2º Tratando-se de cópia digital de título executivo extrajudicial ou outro documento relevante à instrução do processo, o juiz poderá determinar o seu depósito em cartório ou secretaria." (NR)

"Art. 399. .....

§ 1º Recebidos os autos, o juiz mandará extrair, no prazo máximo e improrrogável de 30 (trinta) dias, certidões ou reproduções fotográficas das peças indicadas pelas partes ou de ofício; findo o prazo, devolverá os autos à repartição de origem.

§ 2º As repartições públicas poderão fornecer todos os documentos em meio eletrônico conforme disposto em lei, certificando, pelo mesmo meio, que se trata de extrato fiel do que consta em seu banco de dados ou do documento digitalizado." (NR)

"Art. 417. .....

§ 1º O depoimento será passado para a versão datilográfica quando houver recurso da sentença ou noutros casos, quando o juiz o determinar, de ofício ou a requerimento da parte.

§ 2º Tratando-se de processo eletrônico, observar-se-á o disposto nos §§ 2º e 3º do art. 169 desta Lei." (NR)

"Art. 457. .....

.....

§ 4º Tratando-se de processo eletrônico, observar-se-á o disposto nos §§ 2º e 3º do art. 169 desta Lei." (NR)

"Art. 556. .....

Parágrafo único. Os votos, acórdãos e demais atos processuais podem ser registrados em arquivo eletrônico inviolável e assinados eletronicamente, na forma da lei, devendo ser impressos para juntada aos autos do processo quando este não for eletrônico." (NR)

Art. 21. (VETADO)

Art. 22. Esta Lei entra em vigor 90 (noventa) dias depois de sua publicação.