Universidade Gama Filho

Mirian Nashiro

Certificação Digital nos Processos da Justiça Brasileira

São Paulo

2009

Universidade Gama Filho

Mirian Nashiro

Certificação Digital nos Processos da Justiça Brasileira

Monografia apresentada à Universidade Gama Filho como requisito parcial para obtenção do título de especialista em Engenharia de Software.

Orientador: Prof. Júlio Celso Noguchi

São Paulo

2009

RESUMO

Este trabalho teve como meta expor a Certificação Digital como uma ferramenta detentora das melhores técnicas e métodos de segurança, e o seu uso no controle dos processos da Justiça Federal. A pesquisa sobre esse tema revelou sua grande eficácia, sobretudo a segurança necessária nos trâmites processuais. Apesar disso, verificou-se a dificuldade enfrentada pela resistência ao seu uso, pela mudança de conceito e legislação que ela exige. As pessoas tornam-se contrárias às mudanças criando assim uma animosidade capaz de prejudicar o julgamento racional e correto sobre ela.

Foram analisadas as perspectivas da conscientização dos usuários sobre a vantagem em seu uso, as ações que estão sendo tomadas para minimizar a exclusão digital e a importância de criar leis específicas que garantam a sua utilização. Assim, com o uso efetivo, em breve, a Justiça poderá estar trabalhando com uma ferramenta eficiente, com servidores satisfeitos, que agilizará o andamento dos processos de forma segura e à prova de fraudes, quebrando de vez o paradigma tão próprio dela.

Palavras-chave: Criptografia, Assinatura Digital, Certificação Digital, Processo Eletrônico, Justiça Federal.

ABSTRACT

The goal of this work was to exhibit Digital Certification as a tool that includes the best security techniques and methods, and its use in the control of legal processes of the Federal Justice system. The research about this issue revealed its great efficacy, above all the security required in the procedural progress of legal processes. Despite this, the study verified the difficulty faced by resistance to its use, by the change of concept and legislation that it requires. People become opposed to the changes, thereby creating an animosity capable of negatively affecting rational and proper judgment about it.

The prospects of raising the users' awareness about the advantages of its use, the actions that are being taken to minimize digital exclusion and the importance of creating specific laws that guarantee its use were analyzed. Thus, with its effective use, the Justice system could soon be working with an efficient tool, with satisfied users, that will speed up the progress of the legal processes in a secure manner that is fraud-proof, finally breaking the paradigm so particular to it.

Key-Words: Cryptography, Digital Signature, Digital Certification, Electronic Process, Federal Justice.

SUMÁRIO

Lista de Figuras vii

Lista de Tabelas viii

1. Introdução 1

1.1. Tema 1

1.2. Delimitação do tema 1

1.3. Apresentação/Formulação do Problema 1

1.4. Referencial Teórico 1

1.5. Justificativa (importância do trabalho) 2

1.6. Objetivos 2

1.6.1. Objetivo Geral 2

1.6.2. Objetivo Específico 2

1.7. Metodologia de Trabalho 3

1.8. Descrição dos capítulos 3

2. Referencial Teórico 3

3. Certificação Digital 4

3.1. Criptografia 5

3.1.1. O que é uma chave? 6

3.1.2. Criptografia Assimétrica 7

3.1.3. Criptográfica Simétrica 9

3.1.4. Criptografia Assimétrica X Criptografia Simétrica 11

3.1.5. Decreto nº 4.533 13

3.2. Assinatura Digital 14

3.2.1. Valor *HASH* 15

3.3. Certificação Digital 20

3.3.1. ICP- Brasil 22

3.3.2. Certificados Digitais 26

3.3.3. Revogação de certificados 30

3.3.4. Linha de tempo da Certificação Digital 32

4. Barreira Cultural e mudanças de paradigmas 34

4.1. Realidade atual 34

4.2. Resistências 35

4.3. Mudando conceitos, adquirindo vantagens e adequando legislação 36

5. Política de Inclusão Digital 38

5.1. Analfabetismo Digital: os Excluídos Digitalmente 40

5.2. Processos Eletrônicos 42

6. Justiça Brasileira 43

6.1. Justiça Federal 43

6.2. Processos da Execução Fiscal 45

6.3. Procedimentos da Execução Fiscal 47

6.4. EFV – Execução Fiscal Virtual 48

7. Conclusão 50

8. Referências Bibliográficas 52

LISTA DE FIGURAS

Figura 1 – Criptografia assimétrica – codificação 6

Figura 2 - Criptografia Assimétrica - decodificação 7

Figura 3 – Criptografia simétrica - codificação 9

Figura 4 – Criptografia simétrica – decodificação 9

Figura 5 - Troca de chaves simétricas protegidas por uma chave assimétrica 12

Figura 6 – *Hashing* 16

Figura 7 – Assinatura Digital 18

Figura 8 – Estrutura de certificado 24

Figura 9 – Solicitação de Certificados Digitais 29

LISTA DE TABELAS

Tabela 1 - Algoritmos assimétricos 8

Tabela 2 – Algoritmos simétricos 10

Tabela 3 – Algoritmos da Assinatura Digital 15

Tabela 4 – Funções *Hashing* 16

Tabela 5 – Protocolos Criptográficos 20

Tabela 6 - Tipos de Certificados, mídias armazenadoras e as validades 28

1 INTRODUÇÃO

1.1. Tema

Certificação Digital

1.2. Delimitação do tema

Certificação Digital nos processos da Justiça Brasileira

1.3. Apresentação/Formulação do Problema

Situação da Implantação da Certificação Digital na Justiça Brasileira: Barreiras culturais e Legislação**.**

1.4. Referencial Teórico

MEDIDA PROVISÓRIA No 2.200-2, DE 24 DE AGOSTO DE 2001.
Institui a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências.

Lei nº. 11.419, de 19 de dezembro de 2006.
Dispõe sobre a informatização do processo judicial, alterando a Lei no Código de Processo Civil e dá outras providências.

CORRÊA, Gustavo Testa. Aspectos Jurídicos na Internet.
Descreve a preocupação e os cuidados que a tecnologia necessita, transformando a internet em um meio poderoso para os aspectos jurídicos.

BENUCCI, Renato Luis. A Certificação Digital a serviço da agilidade na Prestação Jurisdicional

A inclusão digital como meio necessário para diminuir a distância entre os cidadãos e o Poder Judiciário.

1.5. Justificativa (importância do trabalho)

Devido à crescente utilização dos documentos eletrônicos, inclusive para a prática de atos jurídicos, é necessário um conjunto de tecnologias que permita atribuir-lhes as garantias fundamentais antes referidas e que não dependa de um substrato físico. Esse conjunto tem de aderir a padrões para ser portável entre os diferentes sistemas computacionais que tratem documentos eletrônicos e ao mesmo tempo precisa ser reconhecido pela legislação para que os documentos eletrônicos constituam provas legais.

1.6. Objetivos

1.6.1. Objetivo Geral

Apresentar aspectos da legislação brasileira vigente para certificação digital na Justiça do país, conhecer as características e vantagens em sua implementação, bem como entender as dificuldades enfrentadas para a sua aceitação.

1.6.2 - Objetivo Específico

- Apresentar aspectos tecnológicos da assinatura e certificação digital que dêem segurança e confiabilidade aos documentos eletrônicos
- Apresentar o valor jurídico do documento eletrônico, relatando as vantagens em sua implementação.

- Apresentar a infra-estrutura de chaves públicas brasileira (ICP-Brasil)
- Apresentar a economia resultante do uso efetivo dessa tecnologia
- Identificar as principais resistências e barreiras para a implantação do Certificado Digital na Justiça Brasileira
- Apresentar as vantagens da política de inclusão digital para atualizar o nível tecnológico de quem não tem acesso à informação
- Apresentar um modelo de implantação definitiva da Certificação Digital na Justiça Brasileira.

1.7. Metodologia de Trabalho

O método a ser utilizado será a pesquisa bibliográfica, que abrangerá a leitura, análise e interpretação de livros, periódicos, textos, documentos, material da internet e apostilas, com o objetivo de pesquisar e conhecer diferentes contribuições científicas disponíveis sobre o uso da certificação digital dentro da Justiça Federal, a definição dos problemas resultantes desta tecnologia para chegar ao objetivo e a fundamentação da justificativa da escolha deste tema.

1.8. Descrição dos capítulos

Capítulo 1 – Introdução
Capítulo 2 – Referencial Teórico
Capítulo 3 – Certificação Digital
Capítulo 4 – Barreira Cultural e mudanças de paradigmas
Capítulo 5 – Política de Inclusão Digital
Capítulo 6 – Justiça Brasileira
Capítulo 7 – Conclusão
Capítulo 8 – Referência Bibliográfica

2. Referencial Teórico

De acordo com a medida provisória nº. 2.200-2, DE 24 DE AGOSTO DE 2001, ficou instituído a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, que transforma o Instituto Nacional de Tecnologia da Informação em autarquia,

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.

A Lei nº. 11.419, de 19 de dezembro de 2006, dispõe sobre a informatização do processo judicial e altera a Lei no 5.869, de 11 de janeiro de 1973 – Código de Processo Civil.

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 os dispostos 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 à distância com a utilização de redes de comunicação, preferencialmente a rede mundial de computadores;
III - assinatura eletrônica as seguintes formas de identificação inequívocas do signatário:
a) assinatura digital baseado 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.

Para CORRÊA (2002 apud BEHRENS, 2005, p.56):

- Tornar original uma mensagem enviada por correio eletrônico, mediante a utilização de assinaturas digitais;
- Tornar documentos pessoais inacessíveis e, assim privados;

- Verificar a identidade de outra pessoa on-line, que esteja acessando a rede;
- Verificar a fonte provedora de um arquivo que está sendo copiado; em outras palavras, tornar o download mais seguro;
- Proteger transações financeiras;
- Habilitar o fluxo de caixa digital na internet;
- Proteger a propriedade intelectual;
- Proteger a identidade e a privacidade de todos.

De acordo com BENUCCI, os “desconectados” do processo eletrônico, caso não sejam previstos mecanismos de inserção virtual, potencializarão suas dificuldades de acesso à justiça, pois terão dificuldades para o ajuizamento de ações, para obter informações jurídicas, etc., podendo resultar em um quadro de agravamento da distância já existente entre os cidadãos e o Poder Judiciário.

3. Certificação Digital

É a atividade de reconhecimento em meio eletrônico que se caracteriza pelo estabelecimento de uma relação única, exclusiva e intransferível entre uma chave de criptografia e uma pessoa física, jurídica, máquina ou aplicação. Esse reconhecimento é inserido em um Certificado Digital, por uma Autoridade Certificadora. (Certisign, 2009).

3.1. Criptografia

> *Do grego kryptós, "escondido", e gráphein, "escrita", é o estudo dos princípios e técnicas pelas quais a informação pode ser transformada da sua forma original para outra ilegível, de forma que possa ser conhecida apenas por seu destinatário, detentor da chave privada, o que a torna difícil de ser lida por alguém não autorizado. Assim sendo, só o receptor da mensagem pode ler a informação com facilidade. (WIKIPÉDIA, 2009)*

Definição, segundo Glossário - Brasil (2007, p. 11-12), é a área da criptologia que estuda os princípios, meios e métodos de modificar documentos com o objetivo de mascarar seu conteúdo, impedir modificações, uso não autorizado e dar segurança à confidência e autenticação de dados. É a ciência que estuda os princípios, meios e métodos para tornar ininteligíveis as informações, através de um processo de cifragem, e para restaurar informações cifradas para sua forma original, inteligível, através de um processo de decifragem. A criptografia também se preocupa com as técnicas de criptoanálise, que dizem respeito a formas de recuperar aquela informação sem se ter os parâmetros completos para a decifragem.

Gustavo Testa Corrêa descreve a criptografia como "uma "máscara" colocada sob determinado arquivo, tornando-o irreconhecível para aqueles que lhe "olhassem na rua", ou seja, enquanto estivesse trafegando na Rede.". (CORRÊA, 2008, p.81).

Esta técnica transforma informações da sua forma original para outra incompreensível, onde só o seu destinatário é conhecedor da chave que irá decifrá-la, sendo a sua principal finalidade, estabelecer um padrão entre o emissor e o receptor da informação em forma codificada, evitando a leitura por terceiros.

Para SILVA et al. (2008, p.13):

> *[...] criptografia é a "ciência" de fazer com que o custo de adquirir uma informação de maneira imprópria seja maior do que o custo obtido com a informação. O valor da informação usualmente decresce com o tempo, e a criptografia faz com que o tempo requerido para obter a informação de forma não autorizada seja longo o suficiente para decrescer seu valor a valores inferiores ao dos recursos usados para obtê-la.*

Nesta afirmação, o autor explica que a complexidade para decifrar um código criptografado é tão grande que o torna praticamente à prova de violação, pois supondo que alguém finalmente consiga decifrá-lo, a informação não terá mais importância, ou seja, o propósito da criptografia foi atingido.

Mesmo assim, só a criptografia não pode provar a identidade de um usuário ou a identidade do emissor dos dados criptografados. Se um site que criptografa dados é acessado, as informações que são enviadas através de páginas da rede, ainda que exija o nome do usuário e a senha, podem ser facilmente interceptados e não servem como prova de sua identidade. Já os Certificados Digitais resolveria esse problema, fornecendo um meio eletrônico de verificar a identidade. A Certificação fornece uma solução de segurança mais completa, assegurando a identidade de todas as partes envolvidas na transação.

3.1.1. O que é uma chave?

O conceito de “chave” é o mesmo que da chave convencional, aquela que abre e fecha uma porta, dando segurança de acesso.

Ela contém mecanismos de seguranças que impedem a abertura e o acesso indevido de informações e contém informações que controlam a operação de um algoritmo de criptografia.

Na codificação, uma chave especifica a transformação do texto puro em texto codificado ou vice-versa, numa decodificação.

Em um bom algoritmo, o mesmo texto cifrado com chaves diferentes deverá produzir textos cifrados totalmente diferentes. Da mesma forma, decifrar um texto cifrado com a chave errada deverá produzir um texto aleatório ininteligível. Se a chave de decriptação for perdida, o dado cifrado praticamente não pode ser recuperado pelo mesmo algoritmo de criptografia. (WIKIPÉDIA, 2009).

Fazendo uma analogia, chaves criptográficas são similares às senhas do banco. Se usar a senha correta, o acesso aos serviços bancários é liberado, caso contrário, seu acesso é negado. Na criptografia, o uso das chaves se relaciona com o acesso ou não às informações criptografadas. Usando a chave correta, a mensagem poderá ser decriptografada.

Existem basicamente dois tipos de criptografia relacionados ao uso de chaves. A mesma chave é utilizada para cifrar e decifrar uma mensagem indica ser um sistema de criptografia por chave simétrica ou chave secreta ou privada.

Se as chaves são diferentes, é um sistema de chaves assimétricas ou chave pública.

3.1.2. Criptografia Assimétrica

As chaves públicas e privadas formam o par de chaves criptográficas em um sistema de criptografia assimétrica ou criptografia de chaves públicas.

A criptografia assimétrica usa esse par de chaves criptográficas que são matematicamente relacionadas.

A chave pública está disponível para todos que queiram cifrar informações para o dono da chave privada ou para verificação de uma assinatura digital criada com a chave privada correspondente e a chave privada é mantida em segredo pelo seu dono e pode decifrar informações ou gerar assinaturas digitais.

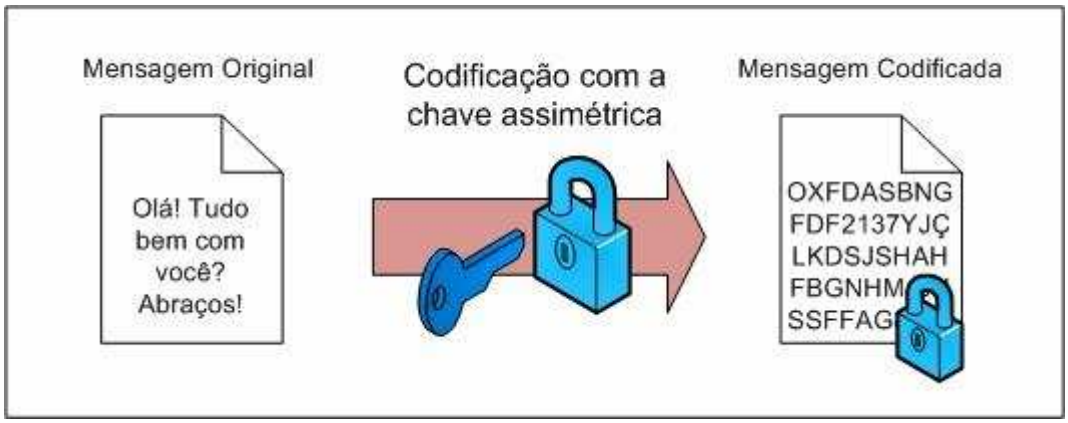

Figura 1 – Criptografia assimétrica - codificação

Figura 2 - Criptografia Assimétrica - decodificação

Num algoritmo de criptografia assimétrica, uma mensagem cifrada com a chave pública pode somente ser decifrada pela sua chave privada correspondente.

Seguem as descrições de alguns algoritmos assimétricos mais utilizados:

Algoritmo	Descrição
RSA	O RSA é um algoritmo assimétrico que possui este nome devido a seus inventores: Ron Rivest, Adi Shamir e Len Adleman, que o criaram em 1977 no MIT. – é um dos algoritmos mais utilizados e o seu funcionamento consiste na multiplicação de dois números primos muito grandes para a geração de um terceiro número. Para quebrar essa criptografia, seria necessária a fatoração desse número para encontrar os dois números primos que o geraram, mas seria necessário um poder muito alto de processamento, inviabilizando a tarefa. A chave privada são os dois números e a pública é o terceiro número. Uma chave RSA de 512 *bits* foi quebrada em 1999 pelo Instituto Nacional de Pesquisa da Holanda, com o apoio de cientistas de mais 6 países. Levou cerca de 7 meses e foram utilizadas 300 estações de trabalho para a quebra. Um fato preocupante: cerca de 95% dos sites de comércio eletrônico utilizam chaves RSA de 512 *bits*.
ElGamal	Desenvolvido por Taher ElGamal, faz uso de um algoritmo conhecido como "logaritmo discreto" para se tornar seguro. É frequente seu uso em assinaturas digitais. É um algoritmo de chave pública utilizado para gerenciamento de chaves. Sua matemática difere da utilizada no RSA, mas também é um sistema comutativo. O algoritmo envolve a manipulação matemática de grandes quantidades numéricas. Sua segurança advém de algo denominado problema do logaritmo discreto. Assim, o ElGamal obtém sua segurança da dificuldade de se calcular logaritmos discretos em um corpo finito, o que lembra bastante o problema da fatoração.
Diffie-Hellman	Também baseado no problema do logaritmo discreto, e o criptosistema de chave pública mais antiga ainda em uso. O conceito de chave pública aliás foi introduzido pelos autores deste criptosistema em 1976. Contudo, ele não permite nem ciframento nem assinatura digital. O sistema foi projetado para permitir a dois indivíduos entrarem em um acordo ao compartilharem um segredo tal como uma chave, muito embora eles somente troquem mensagens em público.
Curvas Elípticas	Em 1985, Neal Koblitz e V. S. Miller propuseram de forma independente a utilização de curvas elípticas para sistemas criptográficos de chave pública. Eles não chegaram a inventar um novo algoritmo criptográfico com curvas elípticas sobre corpos finitos, mas implementaram algoritmos de chave pública já existentes, como o algoritmo de Diffie e Hellman, usando curvas elípticas. Assim, os sistemas criptográficos de curvas elípticas consistem em modificações de outros sistemas (o ElGamal, por exemplo), que passam a trabalhar no domínio das curvas elípticas, em vez de trabalharem no domínio dos corpos finitos. Eles possuem o potencial de proverem sistemas criptográficos de chave pública mais segura, com chaves de menor tamanho. Muitos algoritmos de chave pública, como o Diffie - Hellman, o ElGamal e o Schnorr podem ser implementados em curvas elípticas sobre corpos finitos. Assim, fica resolvido um dos maiores problemas dos algoritmos de chave pública: o grande tamanho de suas chaves. Porém, os algoritmos de curvas elípticas atuais, embora possuam o potencial de serem rápidos, são em geral mais demorados do que o RSA.

Tabela 1 - Algoritmos assimétricos.

3.1.3. Criptografia Simétrica

Criptografia Simétrica utiliza a mesma e única chave privada. É partilhada pelo emissor e pelo receptor da mensagem, assim a chave que cifra é a mesma que decifra.

É necessário que a chave privada só seja do conhecimento do emissor e do receptor. A sua única vantagem é a rapidez no cálculo das operações de cifra/decifra, mas tem a desvantagem da chave ser compartilhada com todos os que precisam ler a mensagem, ficando assim vulnerável a roubos e sendo possível a alteração do documento por qualquer das partes. (Assinaturas Digitais, 2009).

Figura 3 – Criptografia simétrica – codificação

Figura 4 – Criptografia simétrica - decodificação

Os algoritmos da chave simétrica usam chaves criptográficas relacionadas para a cifragem e decifragem. As chaves possuem o mesmo segredo compartilhado entre dois ou mais pessoas que devem manter uma ligação confidencial da informação. A mesma chave é

usada por ambos (emissor e receptor), com a premissa de que esta é conhecida apenas por eles.

Alguns algoritmos simétricos mais comuns:

Algoritmo Simétrico	***Bits***	**Descrição**
DES	56	O *Data Encryption Standard* (DES) é o algoritmo simétrico mais disseminado no mundo. Foi criado pela IBM em 1977 e, apesar de permitir cerca de 72 quadrilhões de combinações (2^{56}), seu tamanho de chave (56 *bits*) é considerado pequeno, tendo sido quebrado por "força bruta" em 1997 em um desafio lançado na Internet. O NIST (*National Institute of Standards and Technology*), que lançou o desafio mencionado, recertificou o DES pela última vez em 1993 e desde então está recomendando o 3DES. O NIST está também propondo um substituto ao DES que deve aceitar chaves de 128, 192 e 256 *bits*, operar com blocos de 128 *bits*, ser eficiente, flexível e estar livre de "*royalties*". O novo padrão, denominado AES (*Advanced Encryption Standard*), está sendo estudado desde 1997 a partir de vários algoritmos apresentados pela comunidade. Os finalistas são: *Serpent, Mars*, RC6, Twofish e Rinjdael, e o resultado deverá ser divulgado no final de 2000.
Triple DES	112 ou 168	O 3DES é uma simples variação do DES, utilizando-o em três ciframentos sucessivos, podendo empregar um versão com duas ou com três chaves diferentes. É seguro, porém muito lento para ser um algoritmo padrão.
IDEA	128	O *Internacional Data Encryption Algorithm* foi criado em 1991 por James Massey e Xuejia Lai e possui patente da suíça ASCOM Systec. O algoritmo é estruturado seguindo as mesmas linhas gerais do DES. Mas na maioria dos microprocessadores, uma implementação por *software* do IDEA é mais rápida do que uma implementação por *software* do DES. O IDEA é utilizado principalmente no mercado financeiro e no PGP, o programa para criptografia de e-mail pessoal mais disseminado no mundo.
Blowfish	32 a 448	Algoritmo desenvolvido por Bruce Schneier, que oferece a escolhe entre maior segurança ou desempenho através de chaves de tamanho variável. O autor aperfeiçoou-o no *Twofish*, concorrente ao AES.
RC2	8 a 1024	Projetado por Ron Rivest (o R da empresa RSA Data Security Inc.) e utilizado no protocolo S/MIME, voltado para criptografia de e-mail corporativo. Também possui chave de tamanho variável. Rivest também é o autor do RC4, RC5 e RC6, este último concorrente ao AES.

Tabela 2 – Algoritmos simétricos

3.1.4. Criptografia Assimétrica X Criptografia Simétrica

Os algoritmos de chave pública podem ser utilizados para confidencialidade e autenticidade. Para confidencialidade, a chave pública é usada para cifrar mensagens, com isso apenas o dono da chave privada pode decifrá-la. Para autenticidade, a chave privada é usada para cifrar mensagens, com isso garante-se que apenas o dono da chave privada poderia ter cifrado a mensagem que foi decifrada com a "chave pública". (WIKIPÉDIA, 2009)

Conclui-se que o conceito de Criptografia Simétrica não atende aos propósitos de validação de documentos jurídicos, visto que somente uma chave é compartilhada entre o receptor e o emissor da informação. Diferentemente da Criptografia Assimétrica que mostrou ser um método mais seguro e adequado para o trâmite processual, pois é composta por duas chaves, uma pública e uma privada de uso restrito do seu proprietário, ou seja, num algoritmo de criptografia assimétrica, uma mensagem cifrada com a chave pública só pode ser decifrada pela chave privada correspondente, garantindo a segurança dos dados.

Entretanto, mesmo que a Criptografia Assimétrica use técnicas seguras, por se tratar de um processo matemático não é inviolável. Torna-se imprescindível o uso correto e responsável para assegurar a unicidade da chave privada.

Tendo em vista as diferenças de velocidade e poder computacional necessário entre a criptografia simétrica e assimétrica, considerando ainda o problema da segurança de transmissão de chaves simétricas, são empreendidas técnicas que combinam os dois métodos criptográficos, como explica CARVALHO (2008).

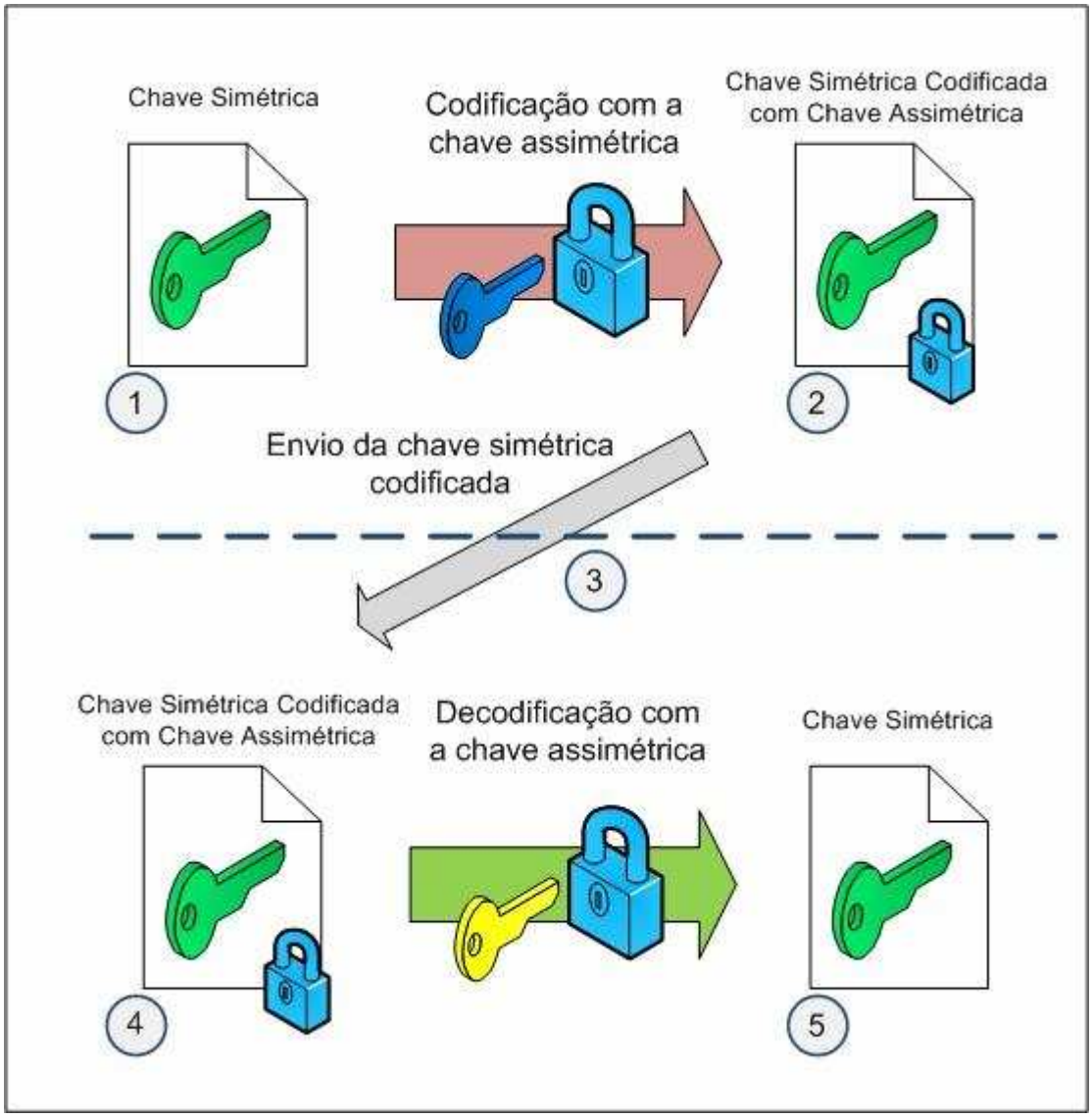

Figura 5 - Troca de chaves simétricas protegidas por uma chave assimétrica

Um algoritmo de chave pública é utilizado para cifrar uma chave criptográfica, gerada aleatoriamente, para ser então utilizada para cifrar a mensagem através de um algoritmo simétrico. O destinatário então primeiro decifra a chave simétrica utilizando sua chave privada no sistema de chave pública, e após decifra a mensagem utilizando a chave recuperada no algoritmo simétrico. Desta forma não há o problema de “compartilhar o segredo da chave” com ninguém. A cada nova mensagem pode-se sempre repetir todo o processo.

3.1.4. DECRETO Nº. 4.553

Tratando-se de informações processuais, a segurança em relação à confidencialidade em sua tramitação é primordial e necessária, conforme DECRETO Nº. 4.553, de 27 de Dezembro de 2002.

O decreto considera sigilosos dois tipos de dados ou informações: os que o conhecimento irrestrito ou divulgação pode acarretar qualquer risco à segurança da sociedade e do Estado e os que precisam ser resguardados para garantir a inviolabilidade da intimidade da vida privada, da honra e da imagem das pessoas:

> *O PRESIDENTE DA REPÚBLICA, no uso da atribuição que lhe confere o art. 84, incisos IV e VI, alínea "a", da Constituição, e tendo em vista o disposto no art. 23 da Lei n o 8.159, de 8 de janeiro de 1991.*
> *CAPÍTULO I*
> *DAS DISPOSIÇÕES PRELIMINARES*
> *Art. 1º Este Decreto disciplina a salvaguarda de dados, informações, documentos e materiais sigilosos, bem como das áreas e instalações onde tramitam.*
> *Art. 2º São considerados originariamente sigilosos, e serão como tal classificados, dados ou informações cujo conhecimento irrestrito ou divulgação possa acarretar qualquer risco à segurança da sociedade e do Estado, bem como aqueles necessários ao resguardo da inviolabilidade da intimidade da vida privada, da honra e da imagem das pessoas.*
> *Parágrafo único. O acesso a dados ou informações sigilosos é restrito e condicionado à necessidade de conhecer.*
> *[...]*
> *CAPÍTULO V*
> *DOS SISTEMAS DE INFORMAÇÃO*
> *[...]*
> *Art. 42 Ressalvado o disposto no parágrafo único do art. 44, os programas, aplicativos, sistemas e equipamentos de criptografia para uso oficial no âmbito da União são considerados sigilosos e deverão, antecipadamente, ser submetidos à certificação de conformidade da Secretaria Executiva do Conselho de Defesa Nacional.*
> *Art. 43 Entende-se como oficial o uso de código, cifra ou sistema de criptografia no âmbito de órgãos e entidades públicos e instituições de caráter público.*
> *[...] (DECRETO Nº. 4.553, 2002)*

Renato L. Benucci descreve que a criptografia ganhou importância com o advento da sociedade da informação, já que solucionou o problema da validade jurídica dos atos realizados em meio eletrônico, comprovando a integridade das informações. (BENUCCI, 2006, p.90)

3.2. Assinatura Digital

A assinatura digital é um método de autenticação de informação digital tipicamente tratada (criptografia), fazendo analogia com a assinatura manual. Entretanto, pode ser confundida com o termo “assinatura eletrônica” que se refere a qualquer mecanismo, não necessariamente criptográfico, para confirmar o remetente de uma mensagem eletrônica.

Para identificar as diferenças, é necessário que sejam verificados as seguintes propriedades:

- autenticidade - há a confirmação de que a assinatura foi feita pelo emissor;
- integridade - se houver qualquer alteração na mensagem, a assinatura não corresponde mais ao documento;
- não repúdio ou irretratabilidade - o emissor não pode negar a autenticidade da mensagem.

Essas características fazem a assinatura digital ser fundamentalmente diferente da assinatura manuscrita. (WIKIPÉDIA, 2009)

A assinatura digital representa o código anexado ou associado logicamente a uma mensagem eletrônica e atesta a autoria de uma determinada informação, podendo esta ser um arquivo, um *e-mail* ou uma transação. Ela comprova quem é autor do documento e a validade dela equivale à assinatura de próprio punho em um documento escrito. A verificação da origem do dado é feita com a chave pública do remetente. (Glossário - ICP, 2007, p.4)

Com o seu uso, é possível garantir a autoria de um documento eletrônico ou transação, garantindo a integridade dos dados, evitando que os mesmos sejam alterados, proporcionando assim, a prova incontestável de que uma mensagem veio do emissor.

O emissor da mensagem usa a chave de assinatura para enviar ao destinatário. Através de algoritmos específicos, a mensagem é cifrada de acordo com esta chave pública. O receptor usará a chave de verificação para decifrar a mensagem. Se houver qualquer alteração, a assinatura será invalidada. (SILVA et al., 2008, p.20).

Seguem alguns algoritmos utilizados na assinatura digital:

Algoritmo	Descrição
RSA	Como já mencionado, o RSA também é comutativo e pode ser utilizado para a geração de assinatura digital. A matemática é a mesma: há uma chave pública e uma chave privada, e a segurança do sistema baseiam-se na dificuldade da fatoração de números grandes.
ElGamal	Como o RSA, o ElGamal também é comutativo, podendo ser utilizado tanto para assinatura digital quanto para gerenciamento de chaves; assim, ele obtém sua segurança da dificuldade do cálculo de logaritmos discretos em um corpo finito.
DSA	O Digital Signature Algorithm, unicamente destinado a assinaturas digitais, foi proposto pelo NIST em agosto de 1991, para utilização no seu padrão DSS (*Digital Signature Standard*). Adotado como padrão final em dezembro de 1994, trata-se de uma variação dos algoritmos de assinatura ElGamal e Schnorr. Foi inventado pela NSA e patenteado pelo governo americano.

Tabela 3 – Algoritmos da Assinatura Digital

3.2.1. Valor HASH

A assinatura digital de documentos eletrônicos utiliza a função *hashing*[1]. O algoritmo percorre todo o documento onde é feita uma análise para ser assinado e um valor de tamanho fixo é gerado. Trata-se do valor *hash*[2] ou resumo criptográfico.

Nos termos criptográficos, segundo BURNETT e PAINE (2002 apud MORENO, PEREIRA e CHIARAMONTE, p.41), a função *hashing* deve ser:

- Simples (eficiente, rápido) se computar o *hash* de dada mensagem;
- Impraticável se determinar a entrada a partir de seu *hash*;
- Impraticável se determinar uma outra entrada que resulte no mesmo *hash* de uma dada entrada;

Os valores de *hash* possíveis são estatisticamente equiprováveis.

O emissor utiliza sua chave privada e a chave pública do receptor para assinar digitalmente o documento. Se houve qualquer adulteração, o valor *hash* será diferente e o resultado será um documento inválido para o receptor.

[1] Função *hashing* - é uma função criptográfica que gera uma saída de tamanho fixo (geralmente 128 a 256 *bits*) independentemente do tamanho da entrada,

[2] *Hash*: É o resultado da ação de algoritmos que fazem o mapeamento de uma sequência de *bits* de tamanho arbitrário para uma sequência de *bits* de tamanho fixo menor conhecido como resultado *hash*, de forma que seja muito difícil encontrar duas mensagens produzindo o mesmo resultado *hash* (resistência à colisão). Faz com que o processo reverso também não seja realizável (dado um *hash*, não é possível recuperar a mensagem que o gerou). (Glossário-ICP, 2009).

Isso garante que os dados estão corretos com a certeza que não houve alteração e evitando assim, a ocorrência de fraudes.

Seguem algumas *funções Hashing* utilizadas nos produtos e protocolos criptográficos:

Funções	Descrição
MD5	É uma função de espalhamento unidirecional inventada por Ron Rivest, do MIT, que também trabalha para a RSA Data Security. A sigla MD significa *Message Digest*. Este algoritmo produz um valor *hash* de 128 *bits*, para uma mensagem de entrada de tamanho arbitrário. Foi inicialmente proposto em 1991, após alguns ataques de criptoanálise terem sidos descobertos contra a função *Hashing* prévia de *Rivest*: a MD4. O algoritmo foi projetado para ser rápido, simples e seguro. Seus detalhes são públicos, e têm sido analisados pela comunidade de criptografia. Foi descoberta uma fraqueza em parte do MD5, mas até agora ela não afetou a segurança global do algoritmo. Entretanto, o fato dele produzir uma valor *hash* de somente 128 *bits* é o que causa maior preocupação; é preferível uma função *Hashing* que produza um valor maior.
SHA-1	O *Secure Hash Algorithm*, uma função de espalhamento unidirecional inventada pela NSA, gera um valor *hash* de 160 *bits*, a partir de um tamanho arbitrário de mensagem. O funcionamento interno do SHA-1 é muito parecido com o observado no MD4, indicando que os estudiosos da NSA basearam-se no MD4 e fizeram melhorias em sua segurança. De fato, a fraqueza existente em parte do MD5, citada anteriormente, descoberta após o SHA-1 ter sido proposto, não ocorre no SHA-1. Atualmente, não há nenhum ataque de criptoanálise conhecido contra o SHA-1. Mesmo o ataque da força bruta torna-se impraticável, devido ao seu valor hash de 160 *bits*. Porém, não há provas de que, no futuro, alguém não possa descobrir como quebrar o SHA-1.
MD2 e MD4	O MD4 é o precursor do MD5, tendo sido inventado por Ron Rivest. Após terem sido descobertas algumas fraquezas no MD4, Rivest escreveu o MD5. O MD4 não é mais utilizado. O MD2 é uma função de espalhamento unidirecional simplificada, e produz um *hash* de 128 *bits*. A segurança do MD2 é dependente de uma permutação aleatória de *bytes*. Não é recomendável sua utilização, pois, em geral, é mais lento do que as outras funções *hash* citadas e acredita-se que seja menos seguro.

Tabela 4 – Funções Hashing

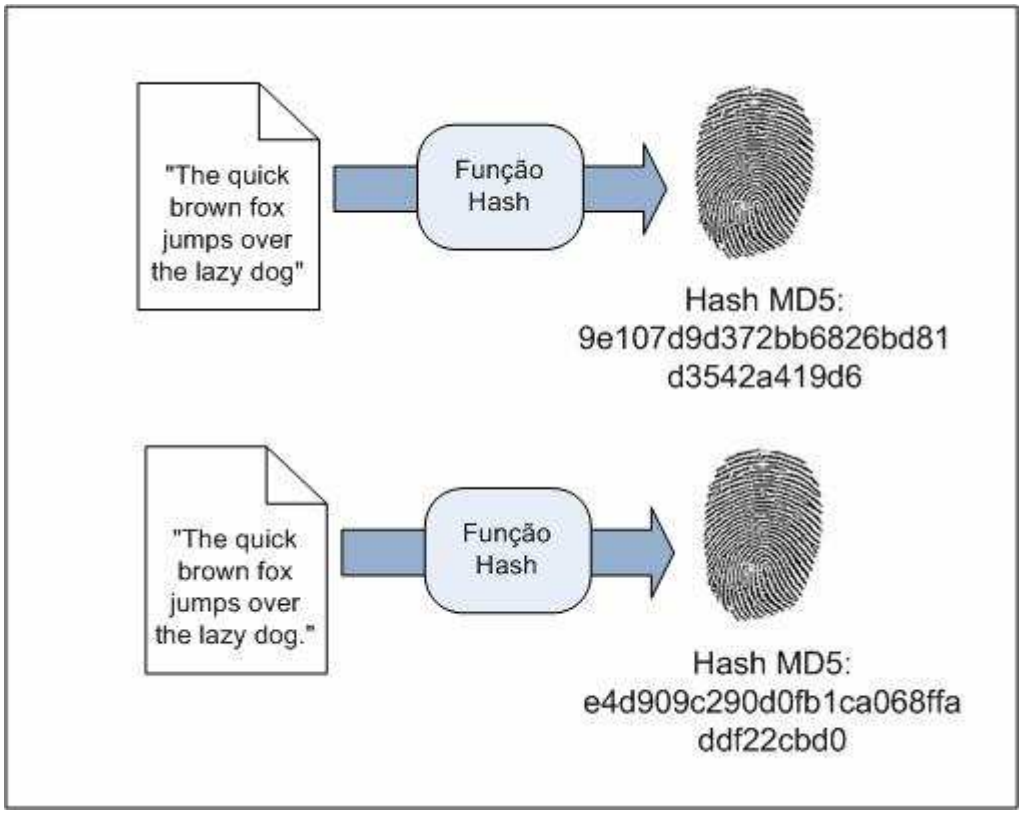

Figura 6 – Hashing

Segundo SILVA et al. (2008, p.20), embora seja possível assinar uma mensagem inteira, não é recomendável por vários motivos. Assinar uma mensagem inteira duplica a quantidade de informação a ser enviada e as operações de criptografia de chave pública ficam mais lentas, fazendo o custo da criptografia pela mensagem inteira tragam problemas de desempenho. Um criptoanalista pode usar a grande quantidade de texto cifrado com a mensagem original para tentar um ataque de análise de mensagens criptografadas.

Dessa maneira pode-se afirmar que a criptografia é feita no resumo gerado pelo algoritmo *hash* - *message digest* (resumo da mensagem), com tamanho em torno de 128 *bits*. A chave privada do usuário é aplicada ao *message digest*, obtendo-se um *message digest* criptografado ou codificado. A seguir, a chave pública do autor é anexada ao documento, presente no certificado digital.

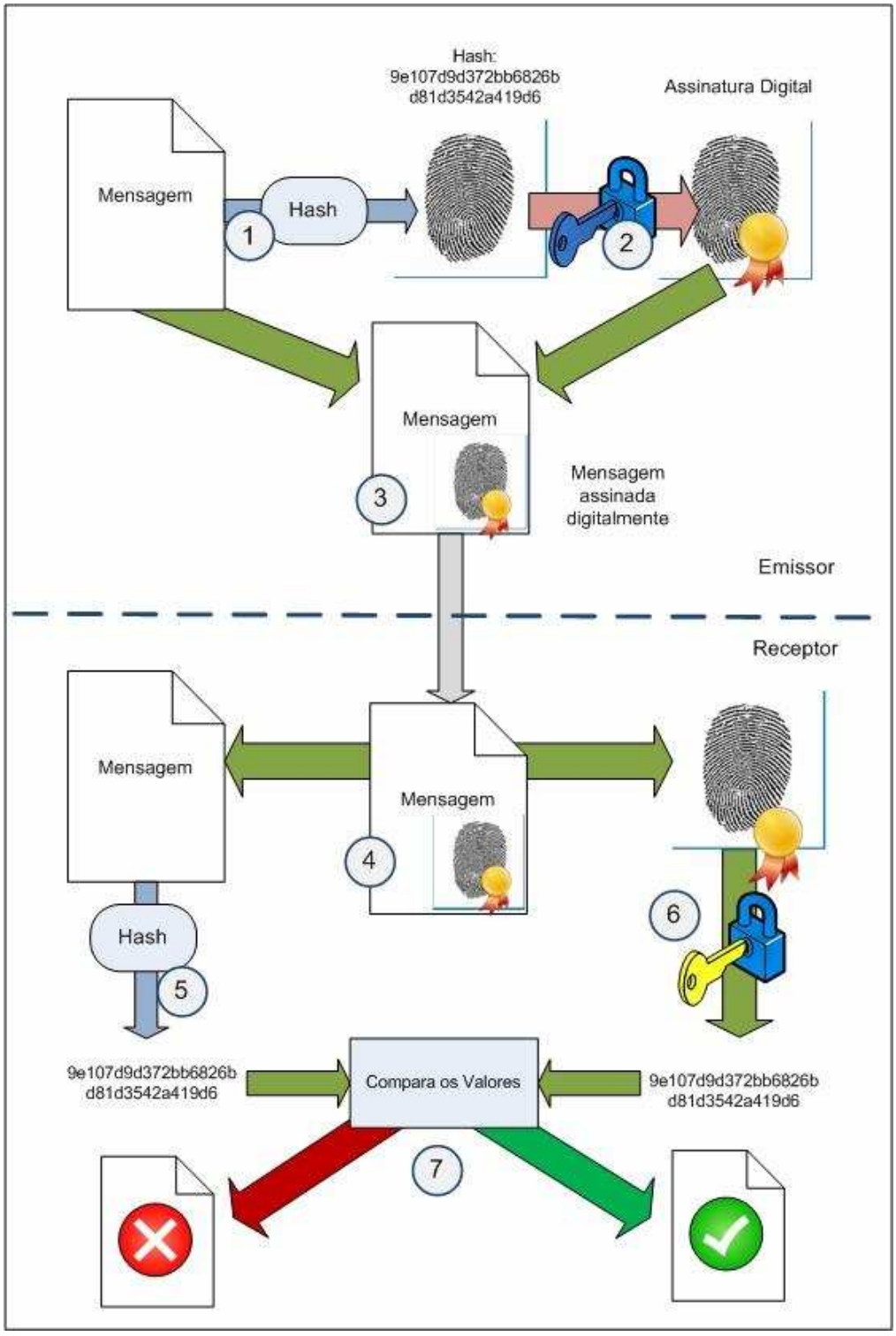

Figura 7 – Assinatura Digital

De acordo com Renato L. BENUCCI (2006, p.95), a assinatura digital de um documento eletrônico consiste na execução de três passos:

1) geração do *message digest* pelo algoritmo *hash*;

2) aplicação da chave privada ao *message digest*;

3) anexação do certificado digital do autor (contendo sua chave pública).

As assinaturas digitais geradas pela mesma chave privada de um usuário em documentos distintos serão diferentes, pois o código *hash* gerado varia em função do conteúdo de cada documento.

Nas palavras de CORRÊA (2008, p.86): “Do ponto de vista jurídico, a identificação do signatário através da assinatura digital realizada sob as condições operacionais das chaves públicas é totalmente relevante, em virtude da confirmação da autenticidade.”.

Esta tecnologia apresenta maior segurança na tramitação de processos judiciais, visando à autenticidade e a integridade de seus dados.

Além disso, permite associar qualquer tipo de documento eletrônico com maior facilidade e velocidade de transmissão. As transações tornam-se praticamente 100% eletrônicas, eliminando o uso de papel.

Resumindo, os algoritmos criptográficos podem ser combinados para a implementação dos três mecanismos criptográficos básicos: a criptografia, a assinatura e o *hashing*. Estes mecanismos são componentes dos protocolos criptográficos, embutidos na arquitetura de segurança. Estes protocolos provêm os serviços associados à criptografia: disponibilidade, sigilo, controle de acesso, autenticidade, integridade e não-repúdio. (MAIA e PAGLIUSI, 2009).

Seguem exemplos de protocolos que empregam sistemas criptográficos híbridos:

Protocolo	Descrição
IPSec	Padrão de protocolos criptográficos desenvolvidos para o IPv6. Realiza também o tunelamento de IP sobre IP. É composto de três mecanismos criptográficos: *Authentication Header* (define a função*Hashing* para assinatura digital), *Encapsulation Security Payload* (define o algoritmo simétrico para ciframento) e ISAKMP (define o algoritmo assimétrico para Gerência e troca de chaves de criptografia). Criptografia e tunelamento são independentes. Permite *Virtual Private Network* fim-a-fim. Futuro padrão para todas as formas de VPN.
SSL e TLS	Oferecem suporte de segurança criptográfica para os protocolos NTTP, HTTP, SMTP e Telnet. Permitem utilizar diferentes algoritmos simétricos, *message digest (hashing)* e métodos de autenticação e gerência de chaves (assimétricos).
PGP	Inventado por Phil Zimmermman em 1991, é um programa criptográfico famoso e bastante difundido na Internet, destinado a criptografia de *e-mail* pessoal. Algoritmos suportados: *hashing*: MD5, SHA-1, simétricos: CAST-128, IDEA e 3DES, assimétricos: RSA, Diffie-Hellman/DSS. Versão mais recente: 6.5.3.
S/MIME	O S/MIME (*Secure Multipurpose Internet Mail Extensions*) consiste em um esforço de um consórcio de empresas, liderado pela RSADSI e pela Microsoft, para adicionar segurança a mensagens eletrônicas no formato MIME. Apesar do S/MIME e PGP serem ambos padrões Internet, o S/MIME deverá se estabelecer no mercado corporativo, enquanto o PGP no mundo do mail pessoal.
SET	O SET é um conjunto de padrões e protocolos, para realizar transações financeira seguras, como as realizadas com cartão de crédito na Internet. Oferece um canal de comunicação seguro entre todos os envolvidos na transação. Garante autenticidade X.509v3 e privacidade entre as partes.
X.509	Recomendação ITU-T, a especificação X.509 define o relacionamento entre as autoridades de certificação. Faz parte das séries X.500 de recomendações para uma estrutura de diretório global, baseada em nomes distintos para localização. Utilizado pelo S/MIME, IPSec, SSL/TLS e SET. Baseado em criptografia com chave pública (RSA) e assinatura digital (com *hashing*).

Tabela 5 – Protocolos Criptográficos

3.3. Certificação Digital

> *É a atividade de reconhecimento em meio eletrônico que se caracteriza pelo estabelecimento de uma relação única, exclusiva e intransferível entre uma chave de criptografia e uma pessoa física, jurídica, máquina ou aplicação. Esse reconhecimento é inserido em um Certificado Digital, por uma Autoridade Certificadora. (GLOSSÁRIO ICP-BRASIL, 2007).*

A Certificação Digital baseia-se em certificados digitais, que são documentos eletrônicos assinados digitalmente por uma terceira parte confiável, que associa o nome e atributos de uma pessoa a um par de chaves (pública e privada). Essa entidade é conhecida como Autoridade Certificadora (AC).

É um mecanismo de segurança capaz de garantir autenticidade, confidencialidade e

integridade às informações eletrônicas. Este processo garante que a assinatura emitida é da entidade ou pessoa indicada na mesma, registrando as assinaturas e fornecendo informações para outra entidade conferir sua autenticidade.

Proporciona maior segurança nas transações e é atualmente é um meio aceito para garantir a segurança requerida na comunicação, envolvendo não só aspectos tecnológicos, mas uma metodologia com controles e autorizações que variam de acordo com as necessidades e organização das autoridades certificadoras, segundo SILVA et al., 2008.

Esse procedimento possibilita a assinatura e autenticação de documentos via internet de qualquer lugar do mundo com maior segurança.

De acordo com Regis Magalhães S. de QUEIROZ, as ACs podem ser públicas ou privadas. Podem ser abertas, prestando serviço ao público interessado ou fechadas, certificando apenas as assinaturas de um determinado grupo. (QUEIROZ, 2001, p.403).

Da mesma forma, Gustavo Testa Corrêa descreve “[...] Autoridade Certificadora, emissora, órgão público ou privado, prestador de serviços de certificação, tem como finalidade destinar a emissão de certificados digitais sobre circunstâncias ou fatos relacionados a um indivíduo, vinculando um par de chaves ao receptor da mensagem de forma segura.”. (CORRÊA, 2008, p.86).

A AC é uma entidade confiável pelas partes envolvidas numa comunicação e/ou negociação, atesta e emite certificados. Ela garante o sigilo e privacidade de *sites* e *e-mails*, controle de acesso a aplicativos, assinaturas de documentos, identificação do remetente, assinatura de mensagens e o não-repúdio de informações.

Deve atender aos requisitos técnicos e é obrigado a oferecer transparência em suas atividades, garantindo a segurança na medida em que o usuário tem conhecimento dos certificados revogados, e para consulta a operações já realizadas.

Para Fabiele BEHRENS (2007, p.54): “[...] Autoridade Certificadora trabalha na comprovação, por meio de emissão de certificado de que o assinante daquele documento digital é realmente e seguramente a pessoa com quem a outra parte está se relacionando.”.

3.3.1. ICP-Brasil

A Infra-estrutura de Chaves Públicas (*PKI - Public Key Infrastructure*) – ICP, é um órgão ou iniciativa pública ou privada com o objetivo de proporcionar a emissão de chaves públicas e oferecer um serviço de credibilidade e confiança nas transações entre as partes que utilizam os certificados digitais, como descreveu SILVA et al. (2008).

KOORN, WALSEN e LUDIN, citados por SILVA et al. (2008, p.70), definem ICP como:

> *[...] uma combinação de tecnologia (hardware e software), processo (políticas, práticas e procedimentos) e de componentes legais (acordos) que vincula a identidade do titular de chaves privadas às respectivas chaves públicas, utilizando a tecnologia assimétrica de criptografia. ICP pode ser utilizada para proporcionar comunicações codificadas e armazenamento de dados (confidencialidade), autenticação da identidade digital de uma pessoa ou uma organização, integridade em mensagens e dados, e agregar a condição de não-repúdio (confirmação de envio e confirmação de recepção) para transações ou mensagens.*

A definição, segundo Glossário ICP-Brasil (2007, p.21): Representa um conjunto de técnicas, arquitetura, organização, práticas e procedimentos, implementados pelas organizações governamentais e privadas brasileiras, a operação de um sistema de certificação. Seu objetivo é instituir as bases de métodos e técnicas do sistema de certificação digital baseado em criptografia de chave pública, garantindo 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.

Para Luiz Gustavo C. da Silva et al. (2008):

> *ICP-Brasil é composta por um conjunto de entidades, padrões técnicos e regulamentos, elaborados para suportar um sistema criptográfico com base em certificados digitais. Foi criado pelo governo federal brasileiro devido à percepção da importância de regulamentação das atividades de certificação digital no país, com vistas a inserir maior segurança nas transações eletrônicas e incentivar a utilização da internet como meio para realização de negócios. (SILVA et al., 2008, p.79)*

A Medida Provisória nº. 2.200-2, de 24 de Agosto de 2001, instituiu a Infra-estrutura de Chaves Públicas Brasileira, a ICP-Brasil, que é composta por uma cadeia de autoridades certificadoras, formada por uma autoridade certificadora-raiz (AC-Raiz), autoridades certificadoras (AC) e autoridades de registro (AR). Sendo a AC-Raiz, o Comitê Gestor da ICP-Brasil, que define as demais entidades que compõem sua estrutura.

Para Alexandre Menezes RIBEIRO et al., as ACs são entidades credenciadas que emitem certificados digitais vinculando par de chaves criptográficas ao respectivo titular. Tem como principais funções: emitir, expedir, distribuir, revogar e gerenciar os certificados, e tem à disposição dos seus usuários, as Listas de Certificados Revogados (LCR[3]) com outras informações pertinentes, mantendo o registro de suas operações. E as ARs são entidades vinculadas operacionalmente à determinada AC. Tem como competência identificar e cadastrar usuários pessoalmente, encaminhar solicitações de certificados às respectivas ACs e manter registros de suas operações. Podem ser credenciadas como AR tanto entidades privadas como órgãos públicos. (RIBEIRO et al., 2004, p.7)

Essa Medida Provisória elaborou as Resoluções do Comitê Gestor da ICP-Brasil, as Instruções Normativas e outros documentos.

O Comitê Gestor deve estabelecer normas para a elaboração de políticas de certificados e regras operacionais das ACs e das ARs, definindo os níveis da cadeia de certificação. Tem ainda como função, atualizar, ajustar e revisar os procedimentos e as práticas estabelecidas para a ICP-Brasil, garantindo sua compatibilidade e promovendo 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 Certificado com Raiz única foi o modelo adotado pela ICP-Brasil e o Instituto Nacional de Tecnologia da Informação – ITI[4], como AC-Raiz.

A AC-Raiz é o ponto inicial e primeira autoridade da cadeia de certificação dessa estrutura e recebeu poderes para validar certificados digitais emitidos, seguindo as políticas

---

[3] Lista de Certificados Revogados (LCR): é uma lista assinada pela Autoridade Certificadora dos certificados revogados. As aplicações que aceitam certificados desta AC devem consultar essa lista para verificar se o certificado está válido. http://www.ccuec.unicamp.br/icp/conceitos.html#a13

[4] O Instituto Nacional de Tecnologia da Informação - ITI é uma autarquia federal vinculada à Casa Civil da Presidência da República do Brasil.
O ITI é a AC Raiz da ICP-Brasil. É a primeira autoridade da cadeia de certificação, executora das Políticas de Certificados e normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil. O ITI integra o Comitê Executivo do Governo Eletrônico, no qual coordena o Comitê Técnico de Implementação do Software Livre no Governo Federal.
Compete ainda ao ITI estimular e articular projetos de pesquisa científica e de desenvolvimento tecnológico voltados à ampliação da cidadania digital. Neste vetor, o ITI tem como sua principal linha de ação a popularização da certificação digital e a inclusão digital, atuando sobre questões como sistemas criptográficos, *software* livre, *hardware* compatíveis com padrões abertos e universais, convergência digital de mídias, entre outras.
Wikipédia - http://pt.wikipedia.org/wiki/Instituto_Nacional_de_Tecnologia_da_Informação

rígidas de certificados e normas técnicas e operacionais aprovadas pelo Comitê Gestor, com validade jurídica. (RIBEIRO et al., 2004, p.7)

As competências da AC-Raiz são emitir, expedir, distribuir, revogar e gerenciar os certificados para as ACs, gerenciar a lista de certificados emitidos, revogados e vencidos, além de executar atividades de fiscalização e auditoria das ACs, das ARs e dos prestadores de serviço habilitados na ICP-Brasil conforme diretrizes e normas técnicas estabelecidas pelo Comitê Gestor da ICP-Brasil.

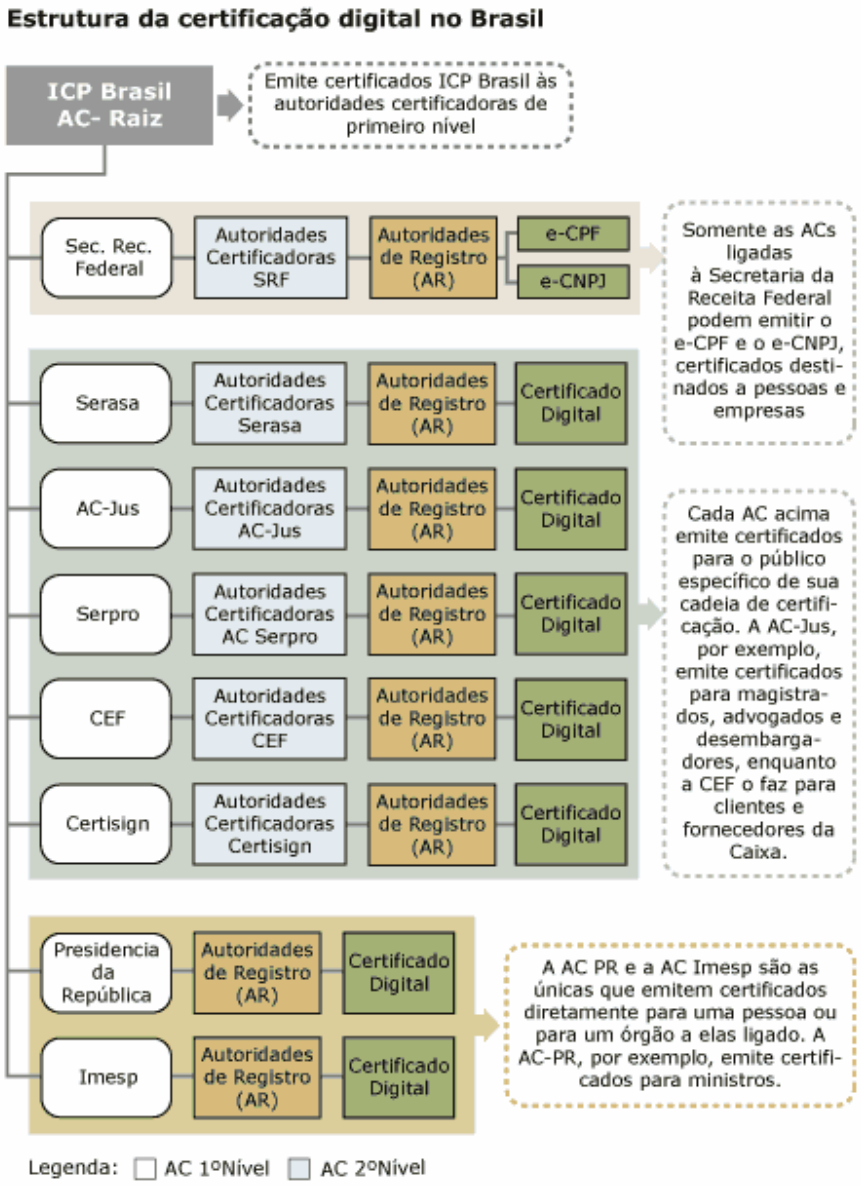

Figura 8 – Estrutura de certificado

A principal função do ICP-Brasil é definir um conjunto de técnicas, práticas e procedimentos a serem seguidas pelas entidades, estabelecendo um sistema de certificação digital baseado em chaves públicas. Cabe a ela credenciar os demais participantes da cadeia, supervisionar e fazer auditoria dos processos.

As entidades participantes devem ser verificadas previamente ao credenciamento, comprovando que tem condições de executar as atividades dentro dos regulamentos. Deve ainda haver um controle anual, constatando que os procedimentos previstos foram executados. (Certisign, 2009)

Propriedades da ICP-Brasil para Alexandre Menezes RIBEIRO et al., (2004, p.11):

- O titular deve estar presente na geração do par de chaves criptográficas, sendo sua chave privada de assinatura de seu exclusivo controle, uso e conhecimento. É obrigatória a validação presencial dos titulares para obtenção de certificados.
- Os documentos assinados com a certificação da ICP-Brasil possuem validade jurídica.
- Os certificados gerados se utilizam de padrões internacionais, como algoritmos criptográficos e tamanhos de chaves que oferecem nível de segurança aceitável internacionalmente.
- As entidades credenciadas possuem instalações e procedimentos com nível de segurança física, lógica, de pessoal e procedimental em padrões internacionais.
- As entidades componentes da ICP-Brasil são obrigadas a declarar em repositório público as práticas de segurança utilizadas em todos os seus processos.
- As entidades ao credenciar-se, passam por uma auditoria prévia e anualmente, para manter-se credenciadas.
- As informações dos certificados são mantidas por no mínimo 30 anos, permitindo a comprovação e suprimir dúvidas sobre a assinatura de documentos, atendendo legislações específicas de guarda de documentos.
- 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.
- Isso significa que um arquivo assinado com uma chave privada certificada pelo ICP-Brasil torna-se um documento, e esta assinatura digital tem o mesmo valor que a assinatura manual, mas com um nível de segurança superior, pois ao contrário dela é virtualmente impossível de imitar, a não ser no caso de divulgação do código que lhe deu origem.

3.3.2. Certificado Digital

O Certificado Digital, definido pelo Glossário ICP-Brasil (2007, p.9) é um conjunto de dados de computador, gerados por uma Autoridade Certificadora, de acordo com a Recomendação Internacional ITU-T X.509, cujo objetivo é registrar de forma única, exclusiva e intransferível, a relação existente entre uma chave de criptografia e uma pessoa física, jurídica, máquina ou aplicação.

Para SILVA et al. (2008, p.72):

> *Antes que um certificado seja emitido, um vínculo precisa ser criado entre a identidade da pessoa ou organização requisitante e a chave pública. Este processo de identificação e autenticação é realizado por uma autoridade de registro (AR). Em alguns casos, a função AR é exercida pela própria AC, enquanto que em outros (por exemplo, quando há uma extensa base de distribuição de usuários), a AC deve delegar a função de AR para terceiros situados em locais apropriados.*

Fabiano MENKE (2005) descreve que os certificados digitais são emitidos com base em padrões estabelecidos em normas internacionais, onde se destaca os padrões ITU[5] X.509 ou ISO 9594-8.

O X.509 é um padrão que especifica o formato dos certificados digitais, de tal maneira que se possa amarrar firmemente um nome a uma chave pública, permitindo autenticação forte. Foi adaptado para a Internet pelo grupo da Internet *Engineering Task Force* (IETF) PKIX. Faz parte das séries X.500 de recomendações para uma estrutura de diretório global, baseada em nomes distintos para localização. Na ICP-Brasil utiliza-se certificados no padrão X.509 V3. (WIKIPÉDIA, 2009)

Em sistemas ICP X.509, a hierarquia de certificados é sempre baseada em uma árvore de cima à baixo, estando a AC-Raiz no topo que não precisa ser assinado por um terceiro confiável. O certificado raiz é auto assinado.

Os certificados digitais X.509 incluem não apenas o nome e a chave pública de um usuário, mas também outras informações sobre o usuário. Esses certificados são mais que um ponto de partida em uma hierarquia digital de confiança. Eles permitem que a autoridade de certificação ofereça ao receptor de um certificado um meio de confiar não apenas na chave pública do indivíduo do certificado, mas também em outras informações sobre o indivíduo do

[5] *Institute of Telecomunication Union*, organização internacional, que possui como um de seus objetivos centrais a padronização no campo das telecomunicações.

certificado. Essas outras informações podem incluir, entre outras coisas, um endereço de e-mail, uma autorização para assinar documentos de um determinado valor ou a autorização para se tornar uma autoridade de certificação e assinar outros certificados.

Os certificados X.509 e muitos outros certificados têm um prazo de validade. Um certificado pode expirar e não ser mais válido. Uma autoridade de certificação pode revogar um certificado por vários motivos. Para processar as revogações, uma autoridade de certificação mantém e distribui uma lista de certificados revogados chamada CRL (lista de certificados revogados). Os usuários da rede acessam a CRL para determinar a validade de um certificado. (HOWSTUFFWORKS, 2009).

Existem oito tipos de certificados. A série A são certificados utilizados na confirmação de identidade na *Web*, em *e-mails*, em redes privadas virtuais (VPN[6]) e em documentos eletrônicos com verificação da integridade de suas informações. São eles, A1, A2, A3 e A4.

A série S com os certificados de sigilo é utilizada na codificação de documentos, de banco de dados, de mensagens e de outras informações eletrônicas sigilosas. São elas, S1, S2, S3 e S4. Esses tipos são diferenciados pelo uso, pelo nível de segurança e pela sua validade.

Segundo Gisele Ribeiro (2009), nos certificados do tipo A1 e S1, as chaves privadas ficam armazenadas no próprio computador do usuário. Já nos tipos A2, A3, A4, S2, S3 e S4, as chaves privadas e as informações referentes ao seu certificado ficam armazenadas em um *hardware* criptográfico - cartão inteligente (*smartcard*) ou cartão de memória (*token* USB ou *pen drive*). Para acessar essas informações você usará uma senha pessoal determinada no momento da aquisição. (RIBEIRO, 2009)

Os certificados mais utilizados são os do tipo A1 e A3. O certificado tipo A1 tem validade de um ano e fica armazenado no próprio computador do usuário. Já o certificado do tipo A3 tem validade de três anos e é armazenado em um *smart card* ou em um *token*.

[6]VPN (*Virtual Private Network*) - Rede Privada Virtual : é uma rede de comunicações privada normalmente utilizada por uma empresa ou um conjunto de empresas e/ou instituições, construída em cima de uma rede de comunicações pública (como por exemplo, a internet). O tráfego de dados é levado pela rede pública utilizando protocolos padrão, não necessariamente seguros. VPNs seguras usam protocolos de criptografia por tunelamento que fornecem a confidencialidade, autenticação e integridade necessárias para garantir a privacidade das comunicações requeridas. Quando adequadamente implementados, estes protocolos podem assegurar comunicações seguras através de redes inseguras. http://pt.wikipedia.org/wiki/Virtual_Private_Network

Tipo de certificado	Chave criptográfica			Validade máxima (anos)
	Tamanho (*bits*)	Processo de geração	Mídia armazenadora	
A1 e S2	1024	*Software*	Arquivo	1
A2 e S2	1024	*Software*	*Smart card* ou *token*, sem capacidade de geração de chave.	2
A3 e S3	1024	*Hardware*	*Smart card* ou *token*, com capacidade de geração de chave.	3
A4 e S4	2048	*Hardware*	*Smart card* ou *token*, com capacidade de geração de chave.	3

Tabela 6 - Tipos de Certificados, mídias armazenadoras e as validades.

Quando um site certificado é acessado, o navegador exibe uma mensagem de identificação e com opções de uso daquele certificado. Se o site não é identificado, a mensagem vem com um aviso de erro e com uma lista de possíveis razões desse erro.

As mais comuns são:

- O navegador não reconhece a AC que emitiu o certificado.
- O certificado do site está incompleto devido a uma configuração incorreta do servidor.
- O usuário está conectado a um site que finge ser o pretendido, com o objetivo de obter informações confidenciais. Neste caso, é possível examinar o certificado antes de marcar uma das três opções (aceitar o certificado permanente ou temporariamente ou não aceitá-lo) e continuar ou não a navegar pelo site.

Regis Magalhães S. Queiroz afirma que, a certificação digital surgiu para evitar fraudes, “[...] onde a identidade do proprietário das chaves é previamente verificada por uma terceira entidade de confiança das partes, que certificará a ligação entre a chave pública e a pessoa que a emitiu, bem como sua validade.” (QUEIROZ, 2001, p. 401).

Dessa maneira, Fabiano Menke em concordância com as afirmações de Queiroz descreve: “quando uma mensagem assinada digitalmente, ela geralmente estará acompanhada do certificado digital do remetente, onde constará, entre outros dados, a sua chave pública". (MENKE, 2005, p.50).

Dando continuidade às palavras de Fabiano MENKE, o autor define:

> *O certificado digital é uma estrutura de dados sob a forma eletrônica, assinada digitalmente por uma terceira parte confiável que associa o nome e atributos de uma pessoa a uma chave pública. O fornecimento de um certificado digital é um serviço semelhante ao de identificação para a*

> *expedição de carteiras de identidade, só que um certificado é emitido com prazo de validade determinado. (MENKE, 2005, p. 49).*

Para a emissão de um certificado digital para pessoa física, são necessárias as seguintes informações: chave pública do titular, nome e endereço de e-mail, validade do certificado, nome da AC emissora do certificado, número de série do certificado digital e assinatura digital da AC. A emissão de certificado para pessoa jurídica requer a apresentação de documentos específicos.

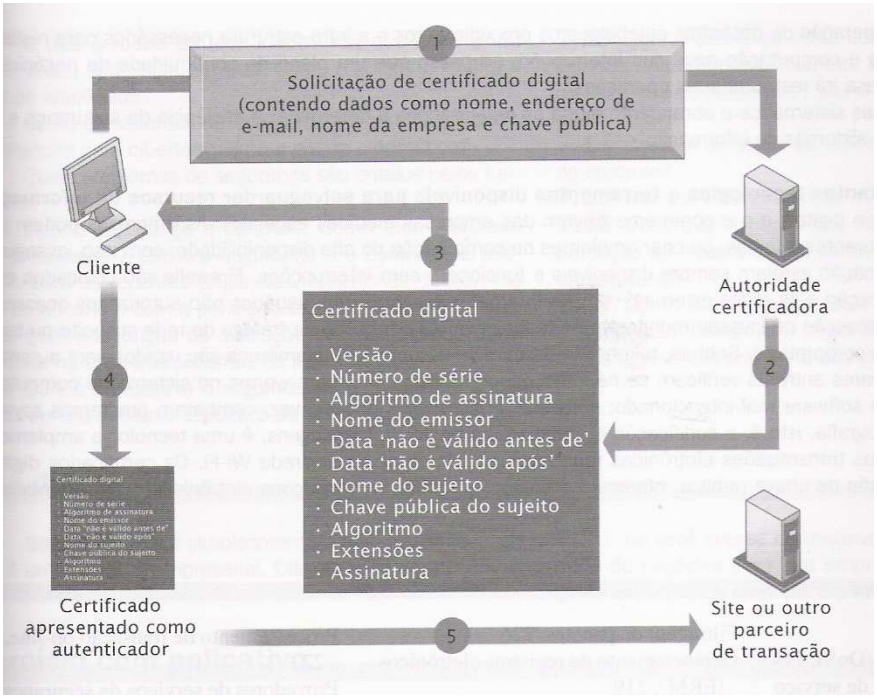

Figura 9 – Solicitação de Certificados Digitais

A AC cria um código *hash* com a informação da identidade do titular e a sua chave pública, faz a assinatura com esta informação utilizando a sua chave privada, criando assim um código *hash* cifrado. Esta informação é incluída no certificado que pode ser armazenado em um *smartcard* ou um *token* protegido por uma senha de acesso, também conhecida como PIN[7] (*Personal identification number*), atribuída pelo próprio titular do certificado.

O receptor do certificado digital faz a verificação da confirmação da integridade, recriando o código *hash* usando o mesmo algoritmo e informação que a AC utilizou na

[7] *Personal Identification Number* ou Número de Identificação Pessoal. É um código numérico usado para restringir o acesso de um serviço somente para pessoas autorizadas a usá-lo. Na telefonia sem fio, o PIN é um código usado em conjunto com um cartão SIM (é uma sigla inglesa para *Subscriber Identity Module* ("módulo de identificação do assinante")) para completar uma chamada recebida ou uma transmissão. *Dicionário Telecomunicações e Informática – Babylon* http://www.babylon.com/definition/pin/Portuguese

criação do *hash* original para o certificado em questão (valor A). Depois decifra o *hash* existente no certificado digital com a chave pública da AC (valor B).

Enfim, compara os dois valores obtidos (A e B) e se estes forem iguais o certificado digital apresenta-se como íntegro. Caso contrário, o certificado digital é detectado como inválido e poderá ser revogado.

3.3.3. Revogação de certificados

Segundo Marcelo Ferreira de Lima (2005, p, 3), a AC além de autenticar aplicações, verifica e mantém atualizadas as informações sobre os estados dos certificados, isto é, tem a responsabilidade de revogá-lo caso este não esteja válido.

Uma revogação não é comum, mas a possibilidade da ocorrência significa que quando um certificado não é confiável, o usuário deverá sempre checar a sua validade. Isto pode ser feito comparando o certificado com uma lista de certificados revogados (LCR).

Um certificado pode ser revogado se for descoberto que a sua chave privada relacionada foi comprometida, ou se o seu relacionamento (entre a AC e a sua chave pública) embutido no certificado estiver incorreto ou foi alterado. Isto poderá ocorrer, por exemplo, se uma pessoa muda de nome ou CPF.

Marcelo F. Lima e Luiz Gustavo C. Silva (2006) descrevem que a ICP-Brasil, apoiada na Medida Provisória n°2.200-2, não exige que um mecanismo diferente da LCR básica completa seja utilizado. Dessa forma, as ACs adotam as LCRs básicas. A freqüência de emissão das LCRs varia para cada AC, podendo ser de uma hora ou de 24 horas.

O objetivo da LCR é mostrar todos os certificados revogados ou cancelados no âmbito daquela AC, garantir que a lista esteja correta e atualizada é a parte mais importante em uma ICP, o que às vezes não é feito corretamente.

Para a LCR ser efetiva, precisa estar disponível sempre e para todos que necessitem e deve ser atualizada frequentemente. A outra maneira de conferir a validade de um certificado é fazer uma consulta a AC usando o *Online Certificate Status Protocol* (OCSP[8]) para saber o

[8] *Online Certificate Status Protocol (*OCSP): lista on-line dos certificados revogados. Deve ser utilizada em casos críticos onde o status do certificado seja importante na transação eletrônica. Ela prova o estado corrente do certificado. http://www.ccuec.unicamp.br/icp/conceitos.html#a9

estado de um certificado específico.

Após a revogação ou expiração do certificado, todas as assinaturas realizadas com este certificado tornam-se inválidas, mas as assinaturas realizadas antes da revogação do certificado continuam válidas se esta operação foi realizada durante o período de validade do certificado.

Quando um certificado é emitido, os principais campos obrigatórios a serem verificado são a identificação e a assinatura da AC, sendo assim, possível a comprovação da autenticidade e a integridade do certificado.

A credibilidade da certificação digital depende da política adotada pela AC, ou seja, o usuário de um certificado digital precisa confiar na AC.

Ao contrário dos documentos de identificação pessoal tradicional como o RG ou CPF, o certificado digital possui um período de validade e só é possível utilizá-lo enquanto ainda não houver expirado. Após esse período, o certificado é automaticamente revogado.

As ACs possuem deveres e obrigações que são descritos em um documento chamado de Declaração de Práticas de Certificação – DPC. Ela é pública para permitir que as pessoas tenham ciência de como foi emitido o certificado digital.

DPC - Declaração de Práticas de Certificação, segundo definição do Centro de Computação da UNICAMP, é um documento definido por RFC (Request For Comments), com força contratual/legal criado pela AC que define:

- Uso dos Certificados
- Processos de identificação e autenticação
- Aspectos operacionais
- Aspectos de segurança (física, lógica e pessoal)
- Procedimentos para continuidade da operação
- Divisão de responsabilidades
- Seguro
- Aceitação por usuários e termos de garantias quando um certificado é aceito
- Responsabilidade dos usuários ao aceitar certificados de outras pessoas
- Perfil dos certificados e lista de certificados revogados. (CCUEC, 2009).

O uso da certificação não torna as transações realizadas isentas de responsabilidades. O uso da chave privada confere ao certificado o não-repúdio à operação, ou seja, o usuário não pode negar posteriormente a realização daquela transação.

A Certificação Digital proporciona essa autenticidade aos documentos eletrônicos e o Poder Judiciário vem reconhecendo que esta é uma ferramenta ideal para ser utilizada com

transparência, respeitando prazos da tutela jurisdicional e da instrumentalidade do processo, tornando mais célere a prestação jurisdicional e o acesso à justiça.

3.3.4. Linha de tempo da Certificação Digital

Existem técnicas para atribuir a indicação de tempo seguro aplicado a uma assinatura digital, chamadas carimbo de tempo (*timestamping*). Estes carimbos adicionam uma data e hora à assinatura, evidenciando que a assinatura de um documento eletrônico era válida naquela data e hora. (ITI, 2009).

A vantagem de um carimbo de tempo é a prorrogação de vida da assinatura de um documento eletrônico, uma vez que é possível verificá-la com base na data em que a assinatura foi produzida. Uma assinatura sem um carimbo só permanece válida enquanto o certificado do signatário é válido. No entanto, com a aposição de um carimbo à assinatura, mesmo que o certificado do assinante deixe de ser válido após a assinatura do documento, seja por revogação ou expiração, a verificação da assinatura é feita com base na data e hora em que foi produzida. Com o carimbo, a assinatura mantém-se válida enquanto o carimbo é válido. Neste sentido, devem ser periodicamente adicionados novos carimbos à assinatura se forem necessário preservá-la por longo prazo. (SOFTPLAN, 2009)

O prazo final para as instituições adotarem o padrão brasileiro de assinatura através da certificação digital é 12 de janeiro de 2010. O padrão brasileiro de carimbo do tempo já é válido, mas ainda falta a implantação da infra-estrutura que proverá o serviço de sincronização de relógios para as Autoridades de Carimbo do Tempo (ACT[9]). A instalação dessa infra-estrutura pelo ITI está prevista para acontecer no último trimestre de 2009.

Um carimbo de tempo é um documento eletrônico assinado que contém o *hash* de sua respectiva assinatura e a data e hora de sua geração. Os carimbos de tempo são gerados por um sistema computacional confiável, o Sistema de Carimbo do Tempo (SCT[10]). O relógio do

---

[9] Autoridade de Carimbo de Tempo (ACT)- A autoridade na qual os usuários de serviços de carimbo do tempo (isto é, os subscritores e as terceiras partes) confiam para emitir carimbos do tempo. http://www.iti.gov.br/twiki/pub/Certificacao/Legislacao/Glossario_ICP-Brasil_-_Versao_1.2.pdf (Glossário ICP-Brasil, p.6).

[10] Sistema de Carimbo de Tempo (SCT) - Dispositivo único constituído por *hardware* e *software* que emite os carimbos de tempo, sob o gerenciamento da ACT. Deve possuir um HSM contendo um relógio a partir do qual

SCT garante a data e hora correta, pois é sincronizado pelo Sistema de Auditoria e Sincronismo (SAS[11]) da AC-Raiz.

Uma assinatura sem um carimbo deixa de ser válida se o certificado do signatário deixar de ser válido. Isso acontece se o certificado expirar ou se qualquer certificado da cadeia de certificação, incluindo o do signatário, for revogado. As assinaturas digitais sem um carimbo de tempo são conhecidas como assinaturas de curto prazo ou de uso restrito, mas seu uso não é obrigatório. (SOFTPLAN, 2009).

Assim, o carimbo de tempo assegura o registro da data e hora em que o documento foi alterado ou ocorreu alguma transação.

A certificação digital já foi regulamentada e um documento assinado digitalmente tem validade jurídica. Ainda assim, percebeu-se a necessidade de registrar o momento em que uma assinatura digital era realizada, garantindo melhor sua eficácia.

O carimbo de tempo detém a hora legal brasileira, com os documentos assinados com validade jurídica e com a comprovação de que as transações ocorreram em um determinado momento. Essas informações ficam a disposição para consulta pelas partes interessadas.

É uma forma segura de agregar e registrar a hora em que determinado certificado concluiu uma operação eletrônica.

4. Barreira Cultural e mudanças de paradigmas

"Quem não muda com o tempo, é punido pela vida". (Gorbatchev *apud* Rocha Neto, 2008).

Dentro da realidade da Justiça, muitos operadores do direito ainda não fazem uso de ferramentas tecnológicas como um básico computador e impressora, por mera resistência ou falta de capacidade pessoal. Mas existem aqueles sem condições de acesso por problemas de ordem financeira. São realidades que assustam, mas são até compreensíveis quando se sabe

---

são emitidos os carimbos do tempo. Nesse HSM devem ser também realizadas as funções criptográficas de geração de chaves e assinaturas digitais.

[11] Sistema de Autenticação e Sincronismo (SAS) - Dispositivo constituído por *hardware* e *software* que audita e sincroniza SAS ou SCT. Deve possuir um HSM com relógio para sincronização e capacidade de processamento criptográfico para geração de chaves criptográficas e realização de assinaturas digitais.

http://www.iti.gov.br/twiki/pub/Certificacao/Legislacao/Glossario_ICP-Brasil_-_Versao_1.2.pdf (Glossário ICP-Brasil, p.34).

que algumas unidades judiciárias ainda funcionam sem qualquer informatização e cidades não têm sequer acesso a internet.

4.1. Realidade atual

O mundo moderno está exigindo cada vez mais, novos conhecimentos e requerendo maior elaboração na quantidade de informações que são transmitidas de maneira tão rápida que as tomadas de decisões tornam-se necessárias de forma igualmente dinâmicas.

A tecnologia reflete um novo paradigma, gerando inovações técnicas, organizacionais e administrativas.

O Judiciário, diante dessa trajetória natural e irreversível, foi compelido a se modernizar em seus procedimentos e operacionalidades pela tecnologia. Os métodos tradicionais e conservadores estão cedendo espaço à informatização dos processos.

O barateamento dos equipamentos de informática tem contribuído para a disseminação do seu uso, onde a princípio era basicamente para armazenamento de informações acerca das partes e processos para posterior consulta.

Atualmente, o Judiciário tem investido em sistemas informatizados e tem feito migrações da parte gerencial administrativa e financeira, tendendo para os serviços em sítios na internet, buscando iniciativas para a virtualização da Justiça Brasileira, de acordo com a Lei nº. 11.419[12] de 19 de Dezembro de 2006.

4.2. Resistências

A definição de mudança, segundo o dicionário Babylon é:

> *Uma alteração de um estado, modelo ou situação anterior, para um estado, modelo ou situação futuros, [...] por razões planejadas e premeditadas.*

---

[12] [...] 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. [...]

> *Mudar envolve necessariamente a capacidade de compreensão e adoção de práticas que concretizem o desejo de transformação. Isto é, para que a mudança aconteça, as pessoas precisam estar sensibilizadas por ela. Perceber a dinâmica das mudanças é uma necessidade. Viver atualizado é uma questão de sobrevivência e uma maneira de visualizar melhor o futuro, já que os novos tempos exigem uma nova postura de pensamento. Existe um mundo que está acabando e outro que está começando e as pessoas, naturalmente, costumam lidar com isso de maneira defensiva, com temor ou rejeição, na maioria das vezes. (BABYLON DICTIONARY, 2009).*

De acordo com essa definição, é necessário sempre estar atento e pronto para quaisquer mudanças que ocorram, aprendendo a lidar com essas novas situações, mesmo que a primeira reação seja a da insegurança.

O processo de mudança tem causado transtornos e resistências e isto é perfeitamente compreensível, como foi explicado anteriormente, pois o choque da desvinculação dos processos manuais onde a assinatura é física, implicando na ruptura com a forma rotineira de trabalhar para os procedimentos eletrônicos onde são empregados chaves, criptografias e certificações digitais são grandes e complexos.

Luiz Gomes da Rocha Neto destaca que as resistências são mais que naturais às inovações, sendo de certa forma a estas inerentes, que terminam por cair ante a constatação de que o novo modelo atingiu a condição de melhor solução de alcance a finalidade a que se destina. (ROCHA NETO, 2008).

A resistência ao uso do computador como ferramenta avançada de trabalho, dificuldade no manuseio do computador e o preconceito, na afirmativa que os procedimentos eletrônicos são acessíveis apenas a minorias, são itens que explicam a resistência ao uso de meios eletrônicos.

4.3. Mudando conceitos, adquirindo vantagens e adequando legislação

É importante diante de tudo isso, que o uso de recursos tecnológicos reflita no Direito, criando maior proximidade entre a Justiça e os cidadãos, agilizando o trâmite processual. Dessa forma, é necessário que os conceitos jurídicos e modelos de atuação do Judiciário sejam adequados às novas modalidades de delitos que são aplicados com o uso dessas novas

ferramentas. Como por exemplo, *spam*, vírus, fraudes eletrônicas, roubo de senhas entre outros ataques que aumentam em proporções gigantescas.

A necessidade de legislação específica nesses casos é fundamental, pois são conflitos civis e comerciais oriundos do *cibermundo*[13].

O grande desafio do Judiciário é vencer o conservadorismo das mentes que operam a Justiça Brasileira para modernizá-la. É uma mudança na cultura e no foco dos operadores de Direito, baseando-se no preparo técnico e manuseio das ferramentas tecnológicas, além de capacitá-los, inclusive na *Web* para criar novas forças eficientes para a interpretação de fatos no combate à crescente criminalidade virtual.

Essa nova realidade provoca incertezas e em conseqüência, torna-se quase natural a resistência a ela. Esse tipo de resistência enfrentada pela modificação nas atividades rotineiras desempenhadas pelos seres humanos provoca geralmente a princípio, uma rejeição à mudança que na maioria das vezes reflete riscos que podem gerar desconforto e medo.

Para Renato L. BENUCCI (2006, p.62):

> *É notório que o emprego da tecnologia informação causa no ambiente social em que se instala uma natural resistência psicológica à novidade, pois exige mudanças na estrutura tradicional do trabalho, a gerar receio e desconfiança. Esse receio do mundo tecnológico apenas pode ser vencido pela educação, que possibilita compreender e assimilar essa nova realidade pelos usuários dos novos sistemas.*

No âmbito da Justiça, o receio pelo desconhecido cria um obstáculo entre o serviço jurisdicional e a informática, muitas vezes causando prejuízos a própria Justiça pelas decisões retrógradas e conservadoras.

Segundo Renato L. BENUCCI (2008, p.63), o profissional do direito possui informação insuficiente sobre as potencialidades da informática aplicada ao direito.

Uma das soluções seria efetuar treinamentos para a capacitação no manejo das novas ferramentas para despertar o interesse pela novidade, comprovados pela eficiência e segurança dessa nova tecnologia.

É natural do ser humano, a capacidade de desenvolver barreiras aos processos de mudanças. Porém, com o advento da evolução tecnológica, é inerente o aprendizado progressivo para a adaptação maior rápida aos novos conceitos, evoluindo para tirar melhor proveito dela.

---

[13] Relativo à cibernética, mundo cibernético, visionário e futurista.
s.f. Ciência que estuda os mecanismos de comunicação e de controle nas máquinas e nos seres vivos. Adj. Aplica-se a uma arte (também dita cinética) que tende a representar, utilizando os recursos da técnica moderna, coisas em movimento. Dicionário online de português - http://www.dicio.com.br/cibernetica/

"Nós, que habitamos os tempos modernos do século XXI, temos que nos adaptar à tecnologia digital que se move à velocidade da Luz. Mais e mais tecnologia está sendo impingida sobre nós a passos cada vez mais rápidos" (VICENTE, 2005, p. 23-24).

Da mesma forma, Dagomir Marquezi afirma o pensamento de Kim Vicente:

> *Hábitos velhos resistem. Mas a tecnologia online existe para humanizar o homem. Para ajudar as pessoas a ter mais tempo livre para se dedicar de verdade as suas famílias e amigos. Para que as empresas possam ser mias enxutas e consigam cortar despesas (e assim pagar melhor seus funcionários). Para que diminua drasticamente o número de pessoas e veículos nas ruas e estradas. Tudo isso parece uma utopia de dez anos atrás – e é. Nós é que estamos atrasados.* (MARQUEZI, 2008, p. 34).

As vantagens resultantes da adoção de tecnologias novas são inúmeras e não pode ser desprezada. A redução de espaços físicos, a economia de gastos com pessoal, papel, tintas de impressão e outros materiais, além da maior segurança nas informações, agilidade, garantia de não repúdio são alguns exemplos dos benefícios que a tecnologia oferece.

Para tanto, é importante e imprescindível que o jurisdicionado some esforços para aproveitar essas vantagens para alcançar a todos indiscriminadamente e proceder a adaptações necessárias para criação de legislações específicas.

Nas palavras de Renato L. Benucci:

> *Essa interação entre direito e tecnologia, em nossa visão ocorre sob duas perspectivas principais. Em uma primeira perspectiva, cabe ao direito regulamentar todo um novo conjunto de situações e relações jurídicas, derivadas da utilização das novas tecnologias, encontrando parâmetros para a sua normatização. (BENUCCI, 2006, p.52).*

Segundo o autor, há a necessidade de empregar meios legais e eficazes para a solução dos conflitos que envolvam aspectos tecnológicos, bem como a competência jurisdicional e as legislações aplicadas no Direito de Informática, considerando suas peculiaridades técnicas deve ser a solução dos antagonismos vinculados à Tecnologia da Informação.

O Conselho Nacional da Justiça – CNJ está implantando um sistema que permite a tramitação informatizada dos processos e a tendência é estender-se para todos os Tribunais.

Entretanto, é necessário levar em consideração as condições físicas de cada Tribunal e as dificuldades regionais, onde existe a escassez de computadores e sistemas que dificultam essa modernização.

É uma questão cultural onde Juízes, procuradores e as partes se assustam com um processo que não esteja em papel e sentem-se receosos de que os processos sejam alterados ou sumam no espaço virtual.

O processo digital pode proporcionar economia de tempo, dinheiro e contribuiu para a preservação do meio ambiente, na medida em que evita o uso de papel.

Do tempo gasto na tramitação de um processo, 70% são despendidos em atos gerados pela burocracia do papel, como a expedição de certidões, protocolos, registros e a tramitação de processos propriamente dita. *(*Agência CNJ de Notícias, 2008)

A era digital chegou para inovar os procedimentos burocráticos e otimizando-os e enquanto a legislação que regularizará a informatização dos processos judiciais não sai, experiências adotadas por várias instâncias do Judiciário mostram que a utilização da informática já é uma realidade e que o avanço tecnológico pode ser um importante instrumento na aplicação da Justiça. (CARDOSO, 2009).

5. Política de Inclusão digital

"Não há amanhã sem projeto, sem sonho, sem utopia, sem esperança, sem o trabalho de criação e desenvolvimento de possibilidade que viabilizem a sua concretização." (FREIRE, Paulo, 2001 apud BEHRENS, 2007, p.103). O que significa que é necessário investir nos meios para se chegar ao fim.

Inclusão Digital é um termo usado para explicar um conjunto de atividades que buscam oferecer os mesmos recursos a todos os componentes da sociedade, permitindo assim um adequado desenvolvimento de todos.

O desenvolvimento tecnológico permitiu aumentar a capacidade de armazenamento, o processamento de informações dos computadores e proporcionalmente, a importância e o interesse para acessar e compreender tais recursos tecnológicos também aumentou.

Entretanto, não é possível afirmar seguramente o futuro da revolução tecnológica devido a diversidades, necessidades, comportamentos e paradigmas que essa mudança representa, e acima de tudo o problema da desigualdade social.

A política de inclusão digital surgiu para amenizar esse problema, onde diversos segmentos da sociedade organizam-se e constituem uma nova esfera na luta pela igualdade de oportunidades. O intuito é levar conhecimento de informática, criando estratégias para a disseminação de equipamentos e ensinar a utilizá-los aos menos afortunados.

Edílson Cazeloto (2008), explica sobre o programa de inclusão digital:

> *Acesso coletivo, subsídio para a compra privada, cursos profissionalizantes, softwares de baixo custo e toda uma parafernália institucional e tecnológica são meios utilizados para tentar fechar esse abismo e permitir que o computador avance por todo o tecido social. (CAZELOTO, 2008, p.18)*

A existência de políticas para corrigir as falhas sociais, fornecendo acesso à informação àqueles cidadãos necessitados atualmente é inadequada, sendo necessária uma reavaliação com determinação de suas causas e discussões das alternativas, onde a resposta nem sempre é óbvia.

Dessa maneira, não há dúvidas que é primordial que se faça a promoção da política de inclusão digital que atinja o maior número possível de pessoas, sem deixar de lado a discussão acerca dos *softwares livres*[14].

A utilização desse tipo de *software*, conforme descrito no artigo 14, trata da obrigatoriedade de utilizar o chamado *software livre* ou até mesmo *software proprietário*[15], mas com o código fonte aberto.

Esse requisito pode proporcionar diversos fatores positivos, como a redução de gastos com licenças periódicas, maior estabilidade, resolução de problemas pelos próprios servidores públicos devidamente capacitados para tanto, e o principal: a possibilidade de padronização do sistema entre os tribunais nacionais, bem como os superiores, de forma a facilitar a interoperabilidade entre os órgãos.

> *Com relação à inclusão digital, os softwares livres não só permitem a viabilização e ampliação de políticas públicas, uma vez que ao reduzir os custos de acesso à tecnologia possibilitam aos organismos governamentais atenderem uma base maior de cidadãos excluídos digitalmente, como também garantem o acesso amplo ao conhecimento tecnológico, nessa área, produzido mundialmente. (O.SILVA, 2004).*

Nos termos do artigo acima citado, o Poder Judiciário poderá desenvolver seus próprios sistemas de informação, sem, contudo, arcar com milionárias cifras por licenças de

---

[14] LEI Nº 11.419, DE 19 DE DEZEMBRO DE 2006.
[...]
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. [...]

Software livre, segundo a definição criada pela *Free Software Foundation* é qualquer programa de computador que pode ser usado, copiado, estudado e redistribuído sem nenhuma restrição. A liberdade de tais diretrizes é central ao conceito, o qual se opõe ao conceito de software proprietário, mas não ao software que é vendido almejando lucro (software comercial). A maneira usual de distribuição de software livre é anexar a este uma licença de software livre, e tornar o código fonte do programa disponível. (WIKIPÉDIA, 2009).

[15] *Software* proprietário ou não livre é aquele cuja cópia, redistribuição ou modificação são em alguma medida restritos pelo seu criador ou distribuidor. A expressão foi cunhada em oposição ao conceito de software livre. Normalmente, a fim de que se possa utilizar, copiar, ter acesso ao código-fonte ou redistribuir, deve-se solicitar permissão ao proprietário, ou pagar para poder fazê-lo: será necessário, portanto, adquirir uma licença, tradicionalmente onerosa, para cada uma destas ações. (WIKIPÉDIA, 2009).

uso de *software proprietário*, além de poder disponibilizar *softwares* aos jurisdicionados, a fim de que haja a perfeita comunicação dos atos processuais. (LOPES, 2007).

Um outro aspecto a ser considerado, é a dependência aos países desenvolvidos em relação à adoção de tecnologias importadas. Segundo Antonio B. O. e SILVA, os níveis de complexidade e de usabilidade da tecnologia dos países fabricantes, dificultam a adequação às necessidades locais, e pode ocorrer tanto na implementação de infra-estrutura para melhoria do acesso das populações carentes à informação (como, por exemplo, os telecentros[16]) quanto na utilização de tecnologia em programas de modernização do setor público. (O. SILVA, 2004).

5.1. Analfabetismo Digital: os Excluídos Digitalmente

Com o advento dos computadores pessoais, o processo de evolução foi ampliado e acelerado ainda mais com o surgimento da internet.

Para aqueles com acesso ao computador, o conhecimento às tecnologias são facilmente absorvidas e a habilidade de operar os equipamentos modernos tornam-se corriqueiras. Ao contrário daqueles cujo acesso a essa tecnologia é restrito, manipular tais equipamentos pode ser complexo. Eles são partes de um problema conhecido como analfabetismo digital[17].

Neste contexto, pode-se afirmar que o avanço tecnológico além de trazer benefícios e facilidades, trouxe uma série de outros problemas e uma delas é a produção de indivíduos excluídos digitalmente.

---

[16] É um ambiente voltado para a oferta de cursos e treinamentos presenciais e à distância, informações, serviços e oportunidades de negócios visando o fortalecimento das condições de competitividade da microempresa e da empresa de pequeno porte e o estímulo à criação de novos empreendimentos. Serve como um instrumento para aproximar os empresários, as instituições públicas e privadas, as organizações não governamentais e a sociedade em geral. É composto por vários computadores interligados em rede local e conectados à internet e tem a orientação de monitores capacitados para atender às demandas dos seus usuários. TELECENTROS - http://www.telecentros.desenvolvimento.gov.br/sitio/sobre/apresentacao/

[17] Analfabeto digital denomina aquele que é incapaz de obter informações por meios da informática ligadas à era digital, como a internet ou qualquer outro meio ligado a computadores. Tipo de analfabetismo contemporâneo bastante comum em regiões que não possuem eletricidade e/ou suporte à rede mundial de computadores, porém há o caso opcional de desinteresse pela máquina por algumas pessoas que contam com fontes mais tradicionais de informação. Nas próximas décadas, espera-se uma expansão digital em todos os setores econômicos e culturais do globo, podendo causar exclusão social daqueles que não estão aptos a interagir com a informação digital. http://pt.wikipedia.org/wiki/Alfabetização

Essas pessoas sem qualificação, geralmente são aquelas sem condições e acabam distanciando-se das novidades tecnológicas e consequentemente das informações acerca dele. E isto é uma desvantagem no mercado de trabalho, que está cada vez mais exigente com os conhecimentos e experiências dos candidatos na área tecnológica.

O conhecimento está sendo cada vez mais valorizado, enquanto que a falta dele cada vez mais ignorada. Para Sérgio SILVEIRA (2001), deve-se combater o analfabetismo funcional[18] e a redução do atraso tecnológico das camadas que vivem a margem da informação. SILVEIRA afirma que:

> *Em primeiro lugar, o Brasil deveria criar um ambiente favorável à criação da tecnologia e o Estado deveria ter uma política de inclusão da população dentro da sociedade da informação. Além disso, as pessoas devem ser educadas para o uso das novas tecnologias e o Estado deve entrar como operador das mesmas. Sem a ação do governo e o incentivo à educação a exclusão não poderá ser combatida. (2001, p.25).*

Não há dúvidas que a tecnologia digital, veio para ficar e possui características particulares que podem trazer grandes benefícios para humanidade. Porém, não se deve esquecer daqueles que serão os grandes prejudicados com essas mudanças. É necessário um esforço do governo para implantar um plano de educação social com informações inerentes às novas tecnologias.

5.2. Processos Eletrônicos

A regulamentação e operacionalização da Lei 11.419[19] incitaram a necessidade de adaptação dos operadores de direito, bem como as instituições de classe (ordem dos

---

[18] Analfabeto funcional é a denominação dada à pessoa que, mesmo com a capacidade de decodificar minimamente as letras, geralmente frases, sentenças e textos curtos e os números, não desenvolve a habilidade de interpretação de textos e de fazer as operações matemáticas. Também é definido como analfabeto funcional o indivíduo maior de quinze anos e que possui escolaridade inferior a quatro anos, embora essa definição não seja muito precisa, já que existem analfabetos funcionais com nível superior de escolaridade. http://pt.wikipedia.org/wiki/Alfabetização

[19] [...] 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. [...]

advogados (OAB), associações de magistrados, associações de membros do ministério público, oficiais de justiça, etc.), baseando-se nos fatores como segurança na tecnologia de informação e armazenamento de dados.

Segundo Renato L. Benucci, não é possível cogitar a ampliação do acesso à justiça por meio da tecnologia sem um movimento mais amplo de transformação e de inserção social. (BENUCCI, 2006, p. 177)

Sem a inclusão digital, a dificuldade de acesso à Justiça no caso dos processos eletrônicos será maior e se agravará.

Esta afirmação fundamenta-se na compreensão da inclusão digital como um direito do cidadão, sendo assim, assunto de interesse público, devendo ser encarada como estratégia para concretizar esses direitos com a simplificação ao acesso a eles.

Mas, apesar da importância da realidade virtual para se alcançar a celeridade processual, criam-se obstáculos para essa implementação.

É primordial rever conceitos antigos e adotar novas tecnologias, avançando no conhecimento do Direito da Informática e da informática jurídica para que a virtualização do processo se torne realidade.

É preciso, portanto, que os profissionais da área jurídica tomem consciência da necessidade de priorizar a inserção do aparato tecnológico em suas atividades, já que o elemento humano se constitui o maior empecilho à implementação das mudanças no campo da informática. A renovação da postura dos lidadores do Direito em relação aos sistemas informáticos é fundamental para resolver, de forma satisfatória e definitiva, o problema da morosidade da Justiça. (BRASIL, 2004).

6. Justiça Brasileira

Existem muitas críticas sobre o Poder Público, muitas vezes com um equivocado preconceito. Os comentários são em geral duros, onde a imagem do funcionalismo público é de que trabalha pouco, ganha muito e muitas vezes é corrupto. É uma caricatura agravada pelo fato incontestável de que a Justiça é lenta, cara, pouco transparente e acessível para poucos.

Os escândalos envolvendo abusos de poder por parte de magistrados, os seus envolvimentos em suspeitas de enriquecimentos ilícitos, vendas de hábeas corpus e tráfico de

influência, também contribuem para o descrédito popular do Judiciário. São fatos isolados, mas é o que fica em evidência, generalizando todo o serviço público.

Segundo George Mamersltein Lima, a concordância com a reforma no Judiciário é praticamente unânime, ao contrário do que é divulgado na imprensa. Essa reforma consiste em uma verdadeira revolução, capaz de moralizar, democratizar e fortalecer e aproximar a Justiça do povo. (M. LIMA, 2003).

A Justiça Brasileira precisa mudar a sua imagem e essa necessidade está sendo trabalhada com grandes investimentos com a aplicação de uma tecnologia inovadora, e segura para os processos que tramitam nela.

6.1. Justiça Federal

No âmbito da Justiça Federal, a verdadeira importância do Poder Judiciário, é aprimorar as instituições democráticas, protegendo o povo contra os abusos do poder público e possibilitando a concretização dos direitos fundamentais e dos objetivos traçados na Constituição Federal.

A Justiça Federal é atuante na defesa da Constituição e dos princípios democráticos, porém é necessário que aconteça mudanças para torná-la um verdadeiro poder de estado.

> *Compete à Justiça Federal processar e julgar as ações propostas contra a União, autarquias federais (como o INSS, o Banco Central) e empresas públicas federais (como a Caixa Econômica Federal), ou em que estas figuram como autoras. Exemplos são as ações em que se discutem tributos federais, benefícios previdenciários ou direitos de servidores federais.*
> *Ainda, dentre outras competências, a de julgar ações de cunho internacional, de direitos de comunidade indígenas e das questões relativas à nacionalidade.*
> *No âmbito criminal, cabe à Justiça Federal julgar crimes como contrabando, tráfico internacional de entorpecentes, moeda falsa, sonegação fiscal, crimes políticos e ambientais. (Institucional - JFSP, 2009)*

O objetivo dessa mudança na justiça é dar uma maior celeridade aos processos, diminuir comportamentos antiéticos praticados pelo Judiciário e reduzir os privilégios dos juízes como forma de moralizar esse poder.

O Judiciário tem a preocupação de solucionar esses conflitos e é essa a razão das iniciativas, mecanismos e procedimentos para a mudança de mentalidade ou mesmo cultural, lutando contra as resistências à tecnologia para garantir uma Justiça bem mais rápida e eficiente.

A adaptação à era digital é uma das necessidades que surgiram com o início da sociedade da informação. É necessário inovar as estruturas produtivas, organizacionais e normativas, bem como uma maior utilização, por parte das instituições públicas e privadas, destes avanços proporcionados pela informática e pelas redes avançadas de informação. (COPALO, 2003 apud BENUCCI, 2006, p.122-123).

A integração entre sistemas jurídicos e as novas tecnologias da informação tendem a aumentar de forma inexorável, o que justifica o pensamento nas formas de aplicação dos recursos tecnológicos para alcançar a melhoria da prestação jurisdicional.

Diante deste contexto, a ampliação e disseminação do uso de processos eletrônicos tem sido uma importante realidade, que auxiliará e melhorará muito o trâmite processual em todo o Judiciário.

Além da consulta com acesso ao teor das decisões dos processos, atualmente o grande investimento é para otimizar o sistema com a implementação da certificação digital, visando eliminar do uso de papel e tentando solucionar a morosidade e o acúmulo de litígios que sobrecarregam a Justiça, modernizando e tornando-a mais eficiente.

6.2. Processos da Execução Fiscal

Os processos de execução fiscal federal consistem em cobranças de créditos da Fazenda Pública (União) e constitui um conjunto de atos sucessivos e coordenados destinados à realização do direito. As partes no processo de execução fiscal são os exeqüentes e os executados.

Tomando como base as informações de Vinícius S. Barbosa (2009), o exeqüente dá entrada a uma petição com o intuito de receber o pagamento da dívida ativa e o executado é citado (citação inicial). Se não houver pagamento no prazo, os bens do executado são penhorados. Após 30 (trinta) dias, é realizado um leilão dos bens penhorados do executado a fim de converter estes bens em dinheiro para sanar o débito.

Podem ocorrer três situações:

1. O executado é encontrado e comprova o pagamento da dívida;
2. O executado é encontrado, mas não possui bens para o pagamento da dívida;
3. O executado não é encontrado.

Na primeira situação, o exeqüente é chamado à manifestação. Se tudo estiver de acordo é realizada uma sentença de extinção da dívida e o processo é arquivado.

No segundo caso o exeqüente é informado sobre a não existência de bens do executado. O exeqüente faz o pedido de suspensão temporária do processo e permanece nesta situação até que o valor da dívida seja pago ou que sejam localizados bens para penhora e pagamento da dívida. Diante desta situação, o executado passa a ter o "nome sujo" no CADIN[20] (Cadastro Informativo de Créditos não Quitados do Setor Público Federal).

No último caso, o executado pode estar se ocultando ou ocultando bens penhoráveis. Por isso são realizadas novas tentativas de localização.

Se o executado for encontrado e não possuir bens, será dado o mesmo prosseguimento da situação anterior. Caso o executado não seja encontrado, mas houver a existência de bens móveis ou imóveis em seu nome, será realizado o arresto destes bens. O exeqüente é chamado para manifestação e em seguida é realizada a citação por edital deste arresto. Após o prazo legal é realizada a nomeação do curador destes bens para garantir a resguarda dos mesmos até o leilão. Geralmente o próprio leiloeiro fica encarregado deste papel.

Após o leilão e conversão dos bens em dinheiro, a dívida ativa é paga integralmente ou parcialmente de acordo com o valor arrecadado. Caso o valor obtido com a venda dos bens em leilão não seja suficiente para quitar a dívida, seu valor é corrigido e o processo fica suspenso aguardando quitação nos mesmos moldes do segundo caso apresentado. (BARBOSA, 2009).

[20] É um banco de dados onde se encontram registrados os nomes de pessoas físicas e jurídicas em débito para com órgãos e entidades federais. As informações contidas no CADIN permitem à Administração Pública Federal uniformizar os procedimentos relativos à concessão de crédito, garantias, incentivos fiscais e financeiros, bem como à celebração de convênios, acordos, ajustes ou contratos, de modo a favorecer a gestão seletiva dos recursos existentes. Compete à Secretaria do Tesouro Nacional expedir orientações de natureza normativa a respeito do CADIN, cabendo ao Banco Central do Brasil, por sua vez, administrar e disponibilizar, por meio do SISBACEN, as informações que compõem o banco de dados. http://www.tesouro.fazenda.gov.br/cadin/

6.3. Procedimentos da Execução Fiscal

Através um pedido da PGFN[21] (Procuradoria Geral da Fazenda Nacional), é apresentado uma dívida ativa de uma pessoa física ou jurídica relacionada à União. A Petição Inicial e CDA (Certidão de Dívida Ativa) chegam à Justiça Federal. Essas petições e as respectivas CDAs são protocolizadas documento a documento (duas vias). Em seguida são encaminhados para a criação de capas e etiquetas, gerando os processos que são cadastrados no Sistema Processual e distribuídos eletronicamente. Os processos são separados e organizados e encaminhados para a secretaria que prepara a autuação onde as folhas são numeradas e rubricadas manualmente. É impresso o despacho de citação e esta segue para o conhecimento e assinatura do juiz e posteriormente o processo pode tomar caminhos diversos.

Verificam-se nessa breve explanação, muitos procedimentos burocráticos e manuais e tudo tende a se agravar com a quantidade de processos que são recebidos diariamente.

> *O novel processo eletrônico só pode oferecer bastante vantagem produtiva se puder eliminar várias tarefas atribuídas aos operadores do direito (juízes, promotores, advogados e serventuários da justiça). O importante é que a maior parte do serviço judiciário possa ser substituída por hardware e software, vale ressaltar, pela informatização automatizada, de modo a promover a celeridade dos julgamentos judiciais. (MADALENA, 2007).*

De acordo com as palavras de Pedro Madalena (2007), a Justiça tem investido na implementação de um sistema moderno capaz de trazer benefícios, melhorando a celeridade dos processos judiciais, bem como oferecendo maior segurança e confidencialidade das informações.

---

[21] Visa apurar a liquidez e certeza da dívida ativa da União, tributária ou de qualquer outra natureza, inscrevendo-a para fins de cobrança, amigável ou judicial; representando privativamente a União, na execução de sua dívida ativa de caráter tributário.
Cabe à PGFN examinar previamente a legalidade dos contratos, concessões, acordos, ajustes ou convênios que interessem à Fazenda Nacional; fixar a interpretação da Constituição, das leis, dos tratados e demais atos normativos a ser uniformemente seguida em suas áreas de atuação e coordenação, quando não houver orientação normativa do Advogado-Geral da União; e representar e defender os interesses da Fazenda Nacional em contratos, acordos ou ajustes de natureza fiscal ou financeira, e junto à Câmara Superior de Recursos Fiscais, aos Conselhos de Contribuintes, ao Conselho de Recursos do Sistema Financeiro Nacional, aos Conselhos Superior e Regional do Trabalho Marítimo e em outros órgãos de deliberação coletiva. http://www3.pgfn.gov.br/institucional/competencia

6.4. EFV – Execução Fiscal Virtual

O EFV (Execução Fiscal Virtual) foi concebido utilizando tecnologia GED[22], Workflow[23], armazenamento, segurança utilizando certificação Digital com s*martcard* para assinatura eletrônica de documentos e conectividade, visando a informatização e automação de procedimentos de execução fiscal e seus incidentes assim como permitir a integração das entidades exeqüentes à Justiça Federal. (INNOVARE, 2009).

É um sistema que viabiliza o processamento eletrônico das ações executivas fiscais que tramitam na Justiça Federal de todo o Brasil, onde os autos processuais em breve serão totalmente informatizados assim como a integração das entidades exeqüentes à Justiça Federal.

Para isso foi assinado um convênio entre a Justiça Federal, Ministério da Fazenda e Ministério da Previdência, para que houvesse uma integração entre os sistemas. Além deles, o Serpro prestou serviços no segmento de soluções de tecnologia relativas à segurança global do projeto, orientando as instituições nos parâmetros de segurança e padrões de interoperabilidade do sistema, garantindo a legalidade das transações, comunicação entre os sistemas, assinatura, certificação digital, criptografia, etc. (SERPRO, 2004).

O projeto prevê a substituição dos autos dos processos de papel pela mídia eletrônica e o seu objetivo principal é dar maior celeridade na prestação jurisdicional, decorrente da utilização do meio eletrônico para esse fim. (BENUCCI, 2006, p.162).

O projeto foi implantado inicialmente no Fórum de Execuções Fiscais da 1ª Subseção de São Paulo, como uma fase piloto com 100 processos.

A idéia do sistema é eliminar a tramitação de papel mediante transferência eletrônica de processos, oferecendo maior agilidade nas execuções fiscais com um mecanismo ligando

---

[22] **Gerenciamento eletrônico de documentos** ou **Gestão electrônica de documentos** (**GED**) é uma tecnologia que provê um meio de facilmente gerar, controlar, armazenar, compartilhar e recuperar informações existentes em documentos. Os sistemas GED permitem aos usuários acessar os documentos de forma ágil e segura, normalmente via navegador Web por meio de uma intranet corporativa, a capacidade de gerenciar documentos é uma ferramenta indispensável para a Gestão do Conhecimento. WIKIPÉDIA - http://pt.wikipedia.org/wiki/Gerenciamento_eletr%C3%B4nico_de_documentos.

[23] **Workflow** (Fluxo de Trabalho**)** é a seqüência de passos necessários para que se possa atingir a automação de processos de negócio, de acordo com um conjunto de regras definidas, envolvendo a noção de processos, permitindo que estes possam ser transmitidos de uma pessoa para outra de acordo com algumas regras. WIKIPÉDIA - http://pt.wikipedia.org/wiki/Fluxo_de_Trabalho.

os sistemas da PGFN com os da Justiça Federal. Esse trâmite será por meio digitalizado, desde a citação até o efetivo pagamento da dívida, se for o caso.

Atualmente, a distribuição de processos está sendo feita mensalmente em número reduzido de 100 processos e gradativamente este número será aumentado.

Esta foi a sistemática adotada para precaver problemas, pois se trata de um sistema bastante complexo que envolve diversas tecnologias, sendo a adaptação aos novos procedimentos bastante difícil.

Este sistema tem pretensão de ser estendido para outras Seções Judiciárias do país, pois no âmbito da Justiça Federal é evidente limitação de espaço físico da infra-estrutura.

Além disso, o EFV garante a autenticidade e a segurança dos documentos eletrônicos, pois utiliza tecnologia de certificação digital aliada a biometria. E mais, as vantagens vão desde os gastos com papel e tinta, além do controle facilitado com a utilização de ferramentas GED e *workflow*.

Com o EFV, a Justiça poderá receber, analisar e devolver os documentos de forma muito mais rápida e confiável, aumentando a eficiência nos tribunais. E o uso da certificação digital otimizará o trabalho do advogado, que ganhará em tempo e na redução de custos para o acompanhamento dos processos.

A utilização da certificação digital na tramitação processual é uma adaptação da Justiça Federal a uma tecnologia em franco desenvolvimento. É um instrumento que promove celeridade e transparência ao Judiciário, de forma a beneficiar o cidadão brasileiro.

“O Judiciário está quebrando um paradigma em benefício de toda a sociedade”. (ADAMO, 2005)

7. Conclusão

A Tecnologia surgiu como uma ferramenta essencial no auxílio às resoluções dos problemas, melhorando, facilitando e agilizando procedimentos e a Certificação Digital é uma tecnologia que está revolucionando os processos da Justiça, tornando-os mais ágeis e seguros. É uma concepção nova e diferente de como ela é conhecida.

Pode-se afirmar que o uso da Certificação Digital está transformando a Justiça em um sistema eficiente e confiável.

Ela une diversos dispositivos de segurança e utiliza um par de chaves criptográficas e assinaturas digitais, associada a uma entidade confiável que autentica a assinatura e emite os certificados, conforme exposto no item 3.3, garantindo a autenticidade, confidencialidade e integridade e o não repúdio às informações eletrônicas.

A medida provisória nº. 2.200-2 e a Lei nº. 11.419, trouxeram legitimidade ao processo eletrônico, verificados nos itens 3.3.1 e 4.1. Apesar delas ainda não tratarem as particularidades dessa tecnologia adequadamente, os benefícios advindos dela justificam considerá-los com validade jurídica.

As vantagens de sua implementação vão além da economia de material. Verifica-se redução do tempo gastos em procedimentos manuais anteriores, onde é possível dedicar maior atenção em outras tarefas mais importantes, a introdução de facilidades na integração com diversas bases de dados, otimizando a troca de informações de forma eletrônica, a possibilidade de comprovar a autoria de um documento, verificar sua integridade e garantir que este será recebido pelo destinatário, além de tornar o processo judicial mais seguro.

Conforme comentado no item 3.3.1, a ICP-Brasil é a entidade apoiada pela media provisória nº. 2.200-2, que garante a autenticidade, a integridade e a validade jurídica de documentos eletrônicos. É a responsável pela emissão das chaves públicas a partir de padrões técnicos, métodos e procedimentos de certidões digitais, visando maior segurança nas transações eletrônicas. As Autoridades Certificadoras e de Registro (AC e AR) compõe a ICP-Brasil.

A evidente economia resultante do uso da Certificação Digital, conforme citado no item 4.3, incluem desde a isenção do uso de papel (ato que contribui para a preservação de um meio ambiente sustentável), cartuchos de impressoras, grampos, etiquetas, pastas, capas de

processos, fotocópias, entre outros materiais, até a redução de espaços físicos, serviços de postagens e mão de obra.

Entretanto, existem algumas dificuldades enfrentadas nesse processo. Entre elas está a resistência ao seu uso. É natural o aparecimento da resistência ao novo até que haja adaptação e aceitação a ele.

Porém não há dúvidas que após o período de adaptação, muitos paradigmas serão quebrados e gradualmente a inclusão da tecnologia de certificação digital nos processos judiciais será bem quista e a Justiça finalmente se tornará justa, correta e ao alcance de todos, indistintamente, conforme afirmação do item 4 e subitens.

É necessário ainda que haja um forte movimento no sentido de levar a informação para aqueles sem condições mínimas de acesso à ela. Sem essa informação, essas pessoas não teriam chances no mercado de trabalho e não seriam capazes de conviver atualmente numa sociedade cercada de tecnologia, de acordo com os itens 5 e 5.1.

Foi implantado o EFV na Justiça que é um projeto piloto inovador que utiliza Certificação Digital aliado a biometria, WorkFlow e GED no trâmite de processos judiciais. Já está implantado como descrito no item 6.4, mas ainda está em fase de adaptação com diversos problemas decorrentes das dificuldades inerentes das técnicas novas, praticamente sem referências para comparações por ser único que detém essas tecnologias associadas.

É inegável que os benefícios decorrentes dele, serão evidenciados depois que os problemas forem sanados e os usuários aprenderem a lidar com essas novas ferramentas.

Entretanto o pensamento do Brasileiro de modo geral em relação à Justiça é “*sempre foi assim...*”, referindo-se à lentidão em que os processos tramitam. É um conceito que vem de longa data e tem sido uma como regra.

Portanto, inserir uma nova ferramenta, com conceitos inovadores e cheios de recursos para o dia a dia, mesmo que melhore as condições e resultados do serviço, causa uma antipatia, pois é como se estivesse “quebrando a regra”.

Por isso conforme relatado anteriormente, é necessário um período de reconhecimento, de adaptação para posterior aprovação. E é isso que a Certificação Digital está tentando fazer: mudar paradigmas, melhorar o serviço, oferecendo agilidade, segurança e confiabilidade em um sistema que estava desacreditado por todos.

8. Referências Bibliográficas

ADAMO, Roberval. **JUDICIÁRIO GANHA AGILIDADE COM CERTIFICAÇÃO DIGITAL. Serpro instala e opera a primeira Autoridade Certificadora do Judiciário**, Ano XXVII - Edição 177. janeiro/fevereiro 2005. Disponível em http://www.serpro.gov.br/imprensa/publicacoes/Tema/tema_177/materias/a-agilidade-com-certificacao-digital. Acesso em 28 set. 2009.

AGÊNCIA CNJ DE NOTÍCIAS: Resistência cultural atrapalha informatização nos tribunais, set. 2008. Disponível em < http://monoceros.cnj.gov.br/portalcnj/index.php?option=com_content&view=article&id=5074:resistencia-cultural-atrapalha-informatizacao-nos-tribunais-&catid=1:notas&Itemid=169>. Acesso em 24 set. 2009.

ASSINATURAS DIGITAIS. Disponível em <http://assinaturas-digitais.web.simplesnet.pt/criptografia_simetrica.htm>. Acesso em 18 set. 2009.

BABYLON Dictionary. Definição de Mudança. Disponível em <http://dicionario.babylon.com/mudança>. Acesso em 03 set. 2009.

BARBOSA, Vinícius Souza. **GANHO OBTIDO COM A UTILIZAÇÃO DO GERENCIAMENTO ELETRÔNICO DE DOCUMENTOS EM PROCESSOS JUDICIAIS**. 2009. 55 f. MBA em Gestão da Qualidade de Sistemas de Informação - Centro Universitário UNIFIEO, Osasco, 2009.

BEHRENS, Fabiele. **Assinatura Eletrônica & Negócios Jurídicos**. /Fabiele Behrens./ Curitiba: Juruá, 2007.

BENUCCI, Renato Luís. **A Tecnologia Aplicada ao Processo Judicial** – Campinas, SP: Millennium Editora, 2006.

BRASIL. Decreto nº. 4.553, de 27 de dezembro de 2002. **Decreto define forma de tratamento para informações sigilosas**. Diário Oficial União, Brasília, DF, 27 dez. 2002. Disponível em: < http://www.planalto.gov.br/CCIVIL/decreto/2002/D4553.htm>. Acesso em: 18 set. 2009.

BRASIL**. Oficinas de Planejamento Estratégico - RELATÓRIO CONSOLIDADO - Comitês Técnicos, Comitê Executivo do Governo Eletrônico**, Maio de 2004, pp. 12-14. Disponível em < http://www.computadoresparainclusao.gov.br/anexos/E15_1872diretrizes_inclusao_digital_gov.pdf>. Acesso em 24 set. 2009.

CARDOSO, Maurício: **Judiciário na Era Digital: tecnologia a serviço do cidadão**. Revista Âmbito Jurídico. Disponível em <http://www.ambito-juridico.com.br/pdfsGerados/noticias/11385.pdf >. Acesso em 25 set. 2009.

CARVALHO, Hugo Eiji Tibana: **PKI - Infra-estrutura de Chaves Públicas**. UFRJ - Universidade Federal do Rio de Janeiro, 2008. Disponível em <http://www.gta.ufrj.br/ensino/eel879/trabalhos_vf_2008_2/hugo/Criptografia.html#Topic9>.

Acessado em 24 set. 2009.

CAZELOTO, Edílson. **Inclusão Digital: Uma visão crítica**. São Paulo: Editora Senac. São Paulo, 2008.

CERTISIGN. **Glossário de Certificação Digital.** Disponível em: <http://www.certisign.com.br/certificacao-digital/por-dentro-da-certificacao-digital/glossario> Acesso em: 14 set. 2009.

CERTISIGN. ICP-Brasil -Infra-estrutura de Chaves Públicas Brasileira**.** Disponível em: <http://www.certisign.com.br/certificacao-digital/infra-estrutura-de-chave-publica/icp-brasil> Acesso em: 15 set. 2009.

CORRÊA, Gustavo Testa. **Aspectos Jurídicos da Internet**. /Gustavo Testa Corrêa. – 4ª ed. – São Paulo: Saraiva, 2008.

CCUEC - Centro de Computação UNICAMP. Disponível em: <http://www.ccuec.unicamp.br/icp/conceitos.html#a13>. Acesso em 15 set. 2009.

GLOSSÁRIO ICP-BRASIL: Infra-Estrutura de Chaves Públicas Brasileira. Versão 1.2. Disponível em <http://www.iti.gov.br/twiki/pub/Certificacao/Legislacao/Glossario_ICP-Brasil_-_Versao_1.2.pdf>. Acesso em 17 set. 2009.

HOWSTUFFWORKS.Como tudo funciona: **Como funciona o certificado digital**. Disponível em: <http://informatica.hsw.uol.com.br/certificado-digital9.htm>. Acesso em 24 set. 2009.

INNOVARE, TRF3 EFV - Sexto Prêmio Innovare - Tema: JUSTIÇA RÁPIDA E EFICAZ, 2009. Documento do EFV enviado pelo Tribunal Regional Federal da 3ª Região para concorrer ao prêmio.

INSTITUCIONAL – JFSP. Justiça Federal de Primeiro Grau em São Paulo. Disponível em: <http://www.jfsp.jus.br/competencia/>. Acesso em 26 set. 2009.

ITI. Instituto Nacional de Tecnologia da Informação: **O que é Certificado Digital?**. Disponível em: <http://www.iti.gov.br/twiki/pub/Certificacao/CartilhasCd/brochura01.pdf> Acesso em 19 set. 2009.

LIMA, George Marmelstein. **Devaneios sobre a Justiça Brasileira – a reforma do Judiciário vista do "olho do furacão"**. Dez. 2003. Universidade Federal do Ceará. Disponível em < http://www.georgemlima.xpg.com.br/ref.pdf>. Acesso em 27 set. 2009.

LIMA, Marcelo Ferreira de. **Assinatura Digital**: Solução Delphi & CAPICOM – Florianópolis: Ed. Visual Books, 2005.

LIMA, Marcelo F.; Silva, Luiz Gustavo C.: **Revogação de Certificados na Infra-estrutura de Chaves Públicas Brasileira: Estado Atual e Alternativas.** Disponível em <http://www.marcelolima.eti.br/MarceloLimaICPbrrevogacao.pdf> Acesso em 16 set. 2009.

LOPES, Leopoldo F. da Silva. **Processo e Procedimento Judicial Virtual – Comentários à Lei 11.419/06 e suas importantes inovações**. Revista Jus Vigilantibus. Campo Grande – MS. 21, mar. 2007. Disponível em: < http://jusvi.com/artigos/23883>. Acesso em: 21 set. 2009

MADALENA, P. **Processo Judicial Virtual. Automação Máxima**. Nov. 2007. Disponível em <http://www.amb.com.br/portal/docs/artigos/PROCESSO%20JUDICIAL%20VIRTUAL-automa%C3%A7%C3%A3o%20m%C3%A1xima.doc>. Acesso em 27 set. 2009.

MAIA, Luiz Paulo; Pagliusi ,Sergio. **Criptografia e Certificação Digital**. Disponível em <http://www.training.com.br/lpmaia/pub_seg_cripto.htm> . Acesso em 24 set. 2009.

MARQUEZI, Dagomir. **A era do home office**: Uma conquista para o século 21 é trabalhar a distância em horários livres. Info Exame: Para quem vive de tecnologia, São Paulo, n. 270, p.34, ago. 2008. Mensal.

MENKE, Fabiano. **Assinatura eletrônica:** aspectos jurídicos no direito brasileiro. São Paulo: Revista dos Tribunais, 2005.

MORENO, Edward David; PEREIRA, Fábio Dacêncio; CHIARAMONTE, Rodolfo Barros: **Criptografia em Software e Hardware**. Disponível em http://www.livrariacultura.com.br/imagem/capitulo/3168257.pdf>. Acesso em 02 out. 2009.

QUEIROZ, Regis Magalhães Soares (coordenadores Newton Lucca e Adalberto Simão Filho). **Direito e Internet – Aspectos Jurídicos Relevantes**. São Paulo: Edipro, 2001.

RIBEIRO, Alexandre M., Oliveira, Evandro L. de, Cardoso, Pedro P., Bertol, Viviane R. Lemos. **A Infra-estrutura de Chaves Públicas Brasileira e suas bases para a Auditoria em Segurança da Informação.** In: ___. Diretoria de Auditoria, Fiscalização e Normalização - ITI – Instituto Nacional de Tecnologia da Informação. p.6. Brasília, 2004. Disponível em <http://www.arquivar.com.br/espaco_profissional/sala_leitura/teses-dissertacoes-e-monografias/Chaves_Publicas_Brasileira.pdf >. Acesso em: 13 set. 2009.

RIBEIRO, Gisele. **Como funciona o certificado digital:** Os tipos de certificação digital. Disponível em: <http://informatica.hsw.uol.com.br/certificado-digital4.htm>. Acesso em: 13 set. 2009.

ROCHA NETO, Luiz Gomes da. **Judiciário, Tecnologia e Resistência**. 13, jun. 2008. Disponível em < http://academico.direito-rio.fgv.br/ccmw/LUIZ_GOMES_DA_ROCHA_NETO>. Acesso em 20 set. 2009.

SERPRO**. Sistemas desenvolvidos pelo Serpro para a Fazenda Nacional decretam o fim do papel.** F**IM DAS FICHAS** - Edição 176. novembro/dezembro 2004. Disponível em <http://www.serpro.gov.br/imprensa/publicacoes/Tema/tema_176/materias/fim-das-fichas>. Acesso em 27 set. 2009.

SILVA, Antonio Braz de O. et al. **Inclusão digital, política de *software* e outras políticas de inclusão**. In: CINFORM, 5, 2004, Salvador. Anais. Salvador: UFBA, 2004. Disponível em http://www.netic.com.br/docs/publicacoes/pub0007.pdf . Acesso em: 27 set. 2009.

SILVA, Luiz Gustavo Cordeiro da et al. **Certificação Digital – Conceito e Aplicações**: Modelo Brasileiro e Australiano. Rio de Janeiro: Editora Ciência Moderna Ltda., 2008.

SILVEIRA, Sérgio Amadeu. **Exclusão Digital - A miséria na Era da Informação**, São Paulo: Fundação Perseu Abramo, 2001.

SOFTPLAN. Assinatura Digital de Documentos Eletrônicos no Brasil: Conceitos Básicos e Infra-estrutura. Disponível em <http://www.softplan.com.br/saj/downloads/cartilha_eletronica.pdf>. Acesso em 19 set. 2009.

VICENTE, Kim. **Homens e Máquinas**: Como a tecnologia pode revolucionar a vida cotidiana. Rio de Janeiro: Ediouro, 2005. 383 p.

WIKIPÉDIA. Disponível em: < http://pt.wikipedia.org/wiki/Algoritmo_de_Chave-simétrica > Acesso em: 07 set. 2009.

WIKIPÉDIA. Disponível em: <http://pt.wikipedia.org/wiki/Criptografia> Acesso em: 14 set. 2009.

WIKIPÉDIA. Disponível em: <http://pt.wikipedia.org/wiki/Chave_(criptografia)> Acesso em: 22 set. 2009.

WIKIPÉDIA. Disponível em: <http://pt.wikipedia.org/wiki/Assinatura_digital> Acesso em: 14 set. 2009.

WIKIPÉDIA. Disponível em: <http://pt.wikipedia.org/wiki/X.509> Acesso em: 14 set. 2009.

WIKIPÉDIA. Disponível em: <http://pt.wikipedia.org/wiki/Instituto_Nacional_de_Tecnologia_da_Informação> Acesso em 19 set. 2009.

WIKIPÉDIA. Disponível em: <http://pt.wikipedia.org/wiki/Software_proprietário>. Acesso em 25 set. 2009.

WIKIPÉDIA. Disponível em: <http://pt.wikipedia.org/wiki/Software_livre>. Acesso em 25 set. 2009.

FOLHA DE APROVAÇÃO DA MONOGRAFIA

UNIVERSIDADE GAMA FILHO
CURSO DE PÓS-GRADUAÇÃO LATO SENSU
Tecnologia da Informação
Certificação Digital nos Processos da Justiça Brasileira
Esta monografia será examinada e aprovada para a obtenção do título de Especialização em Engenharia de Software no Programa de Pós-Graduação da Universidade Gama Filho

_____
Prof. Julio Celso Noguchi – Orientador

_____
Examinador

_____
Examinador

SÃO PAULO/SP
2009