UNIP – UNIVERSIDADE PAULISTA

Paulo de Freitas Riquena

A Certificação Digital como Busca de Garantias do Mundo Virtual

São Paulo

2011

PAULO DE FREITAS RIQUENA

A Certificação Digital como Busca de Garantias do Mundo Virtual

Monografia apresentada à UNIP – Universidade Paulista, com objetivo de obtenção de título de especialista, no curso da pós-graduação “lato sensu” em Tecnologia da Informação e Internet sob a orientação do Profº Ronald Stevis Cassiolato.

São Paulo

2011

AGRADECIMENTOS

Agradeço aos colegas entrevistados que serviram tanto como referências técnicas e àqueles que exprimiram suas dúvidas sobre a tecnologia aqui estudada e que me impulsionaram na respostas a diversas outras questões.

RESUMO

Este trabalho tem por objetivo o estudo da Certificação Digital em diversas aplicações, onde a autenticidade dos participantes do mundo virtual se fizer necessária, tanto para o envio de documentos cifrados, ou não, como simples mensagem que exijam autoria e autenticidade e assinatura digital. Demonstrar que a aplicação dessa tecnologia visa a superação de qualquer dúvida quanto aos autores de mensagens e ou clientes de sites comerciais. Quando é realizada uma compra com cartão de crédito ou paga-se contas via internet, por exemplo, são realizadas transações que exigem fortes doses de confiança. Tanto do lado de quem faz o acesso quanto do lado de quem vende o serviço ou o produto. Entre essas duas pontas sempre há que considerar que aquele ambiente onde elas se encontram é uma rede pública de comunicação, e que pode haver um “hacher” em cada cruzamento dessa trama mundial de bits e bytes, esperando uma oportunidade para se apropriar do dinheiro alheio. É justamente por isso que consumidores e empresas que querem ter a garantia da autenticidade de quem está do outro lado, dependem cada vez mais dessa técnica criptográfica. Há também um direcionamento neste estudo quanto a aplicabilidade dessa tecnologia no Judiciário Federal de segunda instância, onde por verificação prática existiu a oportunidade de acompanhar o uso dessa ferramenta contribuindo para a celeridade processual. Existe como auxílio a referência também à legislação aplicada ao tema, sem a ambição de sua interpretação, mas como material de apoio desse trabalho. Convém ressaltar ainda, que o referencial de pesquisa consta de entrevistas, buscas em sites de legislação, assim como sites de Universidades, e na obra –Certificação Digital ICP Brasil. - Os Caminhos do Documento Eletrônico no Brasil de Robson Machado-, -Jornal Folha de São Paulo-, Revista Veja e outras publicações comerciais melhor detalhadas nas referências bibliográficas.

Palavras chave:- Certificação Digital, Autenticidade e Garantia Virtual, Criptografia, Processo Jurídico Eletrônico.

.

ABSTRACT

This paper aims to study the Digital Certification in various applications where the authenticity of the participants of the virtual world is needed, either for sending encrypted documents or not encrypted, as for simple messages which requires authorship and authenticity and digital signature, but always taking regard to overcome any doubt about the authors of posts or clients of commercial sites. When we make a purchase with credit card or pay bills on the Internet, we perform transactions that require heavy doses of confidence. Either for those who make the access as for those who sell the service or product. Between these two edges we always have to imagine that we are in a public web of communication and that there may be a "Hacker" at every intersection of this global network, waiting for an opportunity to steal people's money. That is why consumers and businesses who want the guarantee of the authenticity of those on the other hand, are increasingly dependent on the encryption. My studies are also directed to the applicability of this technology over the second instance of Paulista Federal Court, where from practical examination, i had the opportunity to follow the use of this tool contributing for the procedural celerity. I also refer to the legislation applied over the theme, without the ambition of its interpretation, but as support material for this paper. My reference for research consists on interviews, searches on legislation sites, universities sites, on the work of Robson Machado in Certificação Digital – ICP – Brasil- Os Caminhos do Documento Etronico no Brasil- Journal Folha de São Paulo-, Magazine Veja, and other trade publications more detailed in the references. It is important to include the theoretical reference that supports the work and which authors served as a bibliographic database.

Keywords:- Virtual Digital Certificate Authenticity Virtual Warranty Encryption Eletronic Legal Process

SUMÁRIO

INTRODUÇÃO

A inclusão digital que permeia boa parte da população brasileira, seja ela de cunho filantrópico ou não, e que representa no cenário atual um enorme crescimento do mundo virtual, se deveu em grande parte a um crescimento da bolha da internet no final de 2000, nunca antes visto e nunca mais retomado. Para se ter uma idéia, a expectativa de crescimento da bolsa de valores Nasdaq –que mede os índices das empresas de tecnologia- naquele ano era de 3.500 pontos e verificou-se um pico de 5.132 pontos. Isso significou mais que o dobro do ano anterior.

No decorrer dos cinco anos seguintes a esse evento, empresas de internet que não tinham sequer modelo de negócios já estruturado ganharam relevância e obtiveram patamares muito saudáveis entre consumidores de seus produtos e principalmente, investidores.

Só para exemplificar, empresas que abriram seu capital ao mercado posteriormente, como o Google e a Salesforce –de sistemas de relacionamento corporativo-, foram as primeiras que estufaram durante a bolha de crescimento, com retorno financeiro invejável. Analistas e investidores estavam tomando as primeiras lições de como analisar o potencial dessas empresas que operam no mundo virtual, incluindo nesse meio as redes sociais.

O consumo de micro-computadores em lares brasileiros impulsionado por programas de financiamento atrelado a projetos governamentais de computador para todos, ganhava o vislumbre diferente de ser um utilitário e ou novo eletrodoméstico, mas sim um novo mundo a ser alcançado, o da internet. Muitos nem mesmo sabiam para que servia, mas se o filho pediu o vizinho aconselhou, que na primeira oportunidade, mesmo que em cinqüenta prestações, o computador adentraria o lar e aos poucos envolveria a todos. Ultrapassando barreiras, encurtando distâncias e fazendo mundo menor.

Nessa mesma seara de crescimento, deu-se também o crescimento dos microcomputadores nas empresas existentes e nas que surgiam como pequenas e

médias, já os traziam como ferramentas inerentes ao trabalho, pois as empresas nasciam voltadas para um ambiente de negócios realizados dentro do mundo virtual.

Os antigos métodos de controle de produtos e serviços que eram gerenciados e catalogados em livros, fichas, pastas, enfim, fisicamente em papéis, passaram para os programas de computadores. Desde as pequenas locadoras de produtos de entretenimento, às de máquinas e serviços, aos laboratórios de exames clínicos que imprimiam os resultados para entregar pessoalmente aos clientes.

Assim como as indústrias que forneciam apenas a lojas distribuidoras, passam a colocar seus produtos em uma página na internet e mostrar aos seus clientes a disponibilidade de acesso a eles, através de um computador com acesso à internet, sem precisarem sair de casa ou do local de trabalho.

O comércio eletrônico *e-comerce*, ganha proporções inimagináveis tornando-se uma das principais formas de transação comercial, de tal maneira, que já demandam por legislações específicas e com especializações dos julgadores dentro do poder judiciário.

Em uma pesquisa feita pelo IBOPE em 2008, estimava-se uma cifra de 41,4 milhões de usuários de computadores no Brasil. Nesta contagem, ficou excluído o número de usuários de computadores no ambiente de trabalho.

Na mesma época o DATAFOLHA, devido a essa diferença de metodologia de pesquisa, contabilizou 64,5 milhões de usuários. Vale dizer, que ambos os institutos consideraram apenas os internautas maiores de 16 anos.

São também informações dos institutos de pesquisa, que no ano de 2009 nas regiões urbanas, 44% da população e 97% das empresas brasileiras estavam conectadas na internet.

Em uma publicação de agosto de 2010 o IBOP/Nielsen apontava que somente naquele mês a população brasileira com acesso à internet havia crescido 5,9% sobre o mês anterior e com um ganho de 11% sobre o mesmo período do ano de 2009.

E para se falar apenas em número de usuários economicamente ativos, no mês de agosto de 2010 o tempo desses usuários ligados na internet foi de 67 horas e 26 minutos incluindo os logados no ambiente de trabalho e domicílio com um ganho de 1,2% sobre o mesmo mês do ano anterior.

Se comparados a outros países o Brasil sempre conta com excelentes marcas no que tange ao tempo de uso de computadores, sempre na frente de países como França, Espanha, Alemanha e Austrália, conforme fontes do IBOPE/Nielsen.

E num instante, aquele que acabara por comprar um computador com o intuito de substituir a máquina de escrever e proporcionar uma ferramenta de estudos transforma-se num comprador inveterado de produtos pelos sites dos fabricantes ou canais de vendas e estão realizando negócios jurídicos.

O comércio eletrônico, ou como já está se denominando um jargão, *e-comerce*, mostrou nos estudos no ano de 2005, que movimentou 2,5 bilhões de reais e no ano seguinte subiu para 3,9 bilhões de reais. Em 2010, há uma estimativa de que o comercio eletrônico tenha movimentado 14 bilhões de reais, informa o editorial do *Jornal Folha de São Paulo* em 28 de fevereiro de 2011, apontando um crescimento de quase 40% anual.

Pressionados pela onda digital, os poderes públicos, mesmo que atrasados, corriam para modernizar seus métodos de atendimento que estavam sustentados num intrincado mundo de formulários de requisições e centenas de trâmites burocráticos, exigindo mais mão de obra e espaço físico para acomodar funcionários e armazenar papéis. Quando o mundo virtual pede passagem, o resultado não poderia ser outro se não a insatisfação dos cidadãos e a clara sensação de ineficiência do poder público.

O trabalho manual era de tal monta e tamanha a demanda, que os funcionários se digladiavam no revezamento para o uso dos antigos *terminas burros* -aparelhos compostos de monitor monocromático de fósforo verde e teclado- ou dos isolados micro-computadores, ambos ligados às barulhentas impressoras matriciais.

Felizmente este é um mundo do serviço público que está ficando para trás. Hoje encontramos prefeituras com muitas informações e serviços on-line, assim como repartições estaduais e federais.

A expedição de certidões, por exemplo, tanto as de cunho administrativas assim como as judiciais, estão disponíveis na rede mundial de computadores, e muitas de forma gratuita, sem **o serviço de intermediários**, como ainda é o caso ainda, de certidões expedidas pelos cartórios de registro civil, ou de registro de imóveis, que cobram pela emissão. *www.arisp.com.br*.

Apesar de todas essas facilidades de transformar procedimentos outrora tão complicados e presenciais, em alguns cliques do mouse diretamente do conforto da residência, local de trabalho ou mesmo em lugares distantes, ou seja, transformar o mundo real em bits e bytes do mundo virtual, fica ainda sobrando uma ponta de desconfiança, deixada pelo vazio do papel sem o tradicional carimbo em poder dos usuários.

É justamente nesta transformação do real que se pauta este trabalho, respondendo a questões sobre segurança dos participantes de relações jurídicas virtuais no mundo da internet que navegam. As facilidades que o ambiente virtual oferece, e a evolução da segurança nas transações on-line em relação às tradicionais em constante atualização e, por conseguinte demonstrar as garantias dos documentos assinados digitalmente.

Como não poderia deixar de mencionar, mesmo que de relance, para embasar o título deste estudo, o mecanismo que envolve os métodos da criptografia, que sempre foi, continua hoje sendo e prosseguirá por um bom tempo, a maneira que as pessoas encontraram para que suas mensagens fossem direcionadas e reservadas àqueles que realmente interessam. E mais, a preocupação de que terceiros não conheçam o conteúdo dos seus documentos, e quando estes forem de conhecimento público, que a sua identificação seja de caráter incontestável. Nasce então a certificação digital.

Capítulo 1 – A Popularização da Internet e o Serviço Público

1.1 - O Comércio Eletrônico

No início do novo século, a popularização da internet tomou vultos estratosféricos e trouxe consigo o aparecimento das denominadas lojas virtuais, por intermédio das quais se realiza o comércio eletrônico. Houve também a criação dos *home-bankings*, que trazia um conjunto de práticas bancárias *on-line*, transformando o computador pessoal do correntista, num verdadeiro terminal de cliente que antes até então só era possível o acesso no interior das agências bancárias, e excetuando o saque de dinheiro, todas as outras operações são possíveis.

Uma pesquisa promovida pela câmara-e-net, no primeiro semestre de 2008, as compras *on-line* somaram 3,8 bilhões de reais, com um ganho de 45% sobre o mesmo período do ano anterior.

A empresa de comércio eletrônico Mercado Livre, divulgou em fevereiro de 2011, que seu lucro líquido alcançou de 56 milhões de dólares, só no ano de 2010, representando um avanço de 68% em relação ao resultado de 2009, quando faturou 33 milhões de dólares. A empresa atribui o aumento ao número de produtos comercializados pela plataforma do e-comerce, meio pelo qual foram comercializados 39,2 milhões de produtos, que resultou um volume de transações de 3,4 bilhões de dólares só em 2010. O resultado inclui os 13 países onde a empresa opera: Argentina, Brasil, México, Uruguai, Colômbia, Venezuela, Chile, Equador, Peru, Costa Rica, República Dominicana, Panamá e Portugal. Somando uma receita de 216,7 bilhões de dólares em 2010. *Jornal Valor Econômico de 23/02/2011.*

Tais práticas se tornaram o ponto central de um processo revolucionário de transformações no cotidiano das pessoas conectadas à internet, mudando para sempre o comércio e as finanças de forma muito intensa. Entretanto todas essas facilidades de acesso oferecidas pela internet são alvos fáceis e volúveis, que aguçam a ganância de pessoas mal-intencionadas, exigindo sempre a utilização de mecanismos de segurança na internet.

Em São Paulo, uma vez por semana 37% dos consumidores acessam site de compras coletivas. Quando estão na web, os consumidores buscam com mais intensidade, ofertas relacionadas à alimentação, citada por 27% dos clientes. Os produtos eletrodomésticos aparecem em seguida com 25,6% de acesso, de acordo com uma pesquisa realizada pelo Shopping Jardim Sul, buscam alinhar os serviços dos shoppings à facilidade de descontos dos sites de compras coletivas, para tornar uma estratégia para atrair o público.

Nessa mesma pesquisa, um percentual superior a 90% dos entrevistados disse se sentir mais seguro quando as promoções são oferecidas pelas lojas dos próprios empreendimentos. Desses entrevistados, 53% dos consumidores opinaram que, os shoppings devem direcionar suas promoções na divulgação on-line dos seus produtos relacionados a calçados, roupas e alimentação. Jornal Folha de São Paulo 01/03/2011.

A evolução da segurança é uma constante preocupação que envolve as transações on-line, e os meios utilizados para quebrar os tradicionais mecanismos de segurança evoluem no mesmo tempo, assim como são constantes as tentativas de se quebrarem os novos mecanismos de defesa. Torna-se um círculo vicioso, pois é necessário desenvolvimento de novas tecnologias que correm para atender a garantia que os métodos tradicionais já não oferecem.

1.2 - O Judiciário Federal e a Certificação Digital

A morosidade dos processos judiciais, que vem há muito tempo sendo discutida, é o tema que causa a maior insatisfação com o judiciário brasileiro, situação esta, que está sendo mitigada com a implantação de novas tecnologias aos poucos adotadas nos tribunais.

A morosidade do Judiciário na prestação de seus serviços é o mais significativo arranhão à efetivação da democracia plena, pois como, já se disse, para que a Justiça seja injusta não faz falta que contenha equívoco, basta que não julgue quando devia julgar. É que o estômago do pobre não espera longas digressões, pelos intermináveis arrazoados e deliberações dos teóricos, pelas solenidades e formalidades exageradas sem maiores diligencias com o direito concreto, motivo maior da longa caminhada processual. - Antonio Pessoa Cardoso- Desembargador do Tribunal de Justiça da

Bahia- em: O processo Sem Autos- Editora Juruá, e HTTP: WWW.justicasempapel.com.br

O processo no direito brasileiro é extremamente lento, caro e complexo, exigindo muita paciência do cidadão que tem um direito violado, ademais, imensos gastos e várias solenidades, que contribui para o aumento da distância entre ricos e pobres, com repercussão patrimonial e emocional com a demora da sua finalização.

Podemos apontar vários fatores determinantes que fazem com nossa justiça seja morosa. A começar por uma demanda muito grande de processos e a escassez de operadores de jurídicos (juízes) para julgar tamanho volume de pretensões que todos os dias são distribuídos nos diversos fóruns do país.

Essa sobrecarga de processos recai sobre os juízes e os obriga a enfrentar pautas que chegam a ser desumanas. Situação parecida enfrentam os tribunais superiores, que exigem um esforço desmedido por parte dos ministros destes tribunais, a exemplo dos processos já julgados pelo Supremo Tribunal Federal, com 103.869 processos julgados em 2010 e com 11.803 processos nos dois primeiros meses de 2011. Fonte *http://www.stf.jus.br/portal/cms/verTexto.asp?servico=estatistica&pagina=movimentoProcessual*

A esta causa soma-se, entre outras, a existência de uma legislação processual que a cada dia se torna mais ultrapassada, como por exemplo, o Código de Processo Civil, que é considerado complexo, lento e difícil representando um obstáculo à agilização da tramitação dos processos, por facilitar um sem-número de procrastinação, não se encaixando nos padrões exigidos pela modernização da justiça.

O próprio Banco Mundial já considerou a justiça brasileira como sendo de intensa morosidade, representando um obstáculo ao crescimento do Brasil, e que ocupa a trigésima justiça mais lenta do mundo onde, exemplificando, a cobrança de uma dívida tem duração processual superior a 380, muito acima dos 75 dias que demora um processo semelhante no Haiti. *Revista Veja em 28/01/2004 pg. 78*

O governo brasileiro e seus demais órgãos de administração pretendem implementar novas tecnologias no campo da informatização para proporcionar celeridade e a

eficácia, com a proteção jurídica, e ampliar o alcance dos serviços internos da própria administração e principalmente ao cidadão.

Essa implementação possibilita ao mundo jurídico, a realização de diversos atos processuais por intermédio da internet.

1.3.- Regularização de Atos e Peças Processuais por Meio Eletrônico

A primeira iniciativa no sentido do recebimento de atos e peças processuais por meios eletrônicos foi dada pela lei federal nº 9.800 de 26 de maio de 1999, que dispôs sobre a utilização de fac-símile, e em seus dois primeiros artigos, a seguintes possibilidades:

> Art. 1º - É permitida às partes a utilização de sistema de transmissão de dados e imagens tipo fac-símile ou outro similar, para a prática de atos processuais que dependam de petição escrita.
>
> Art. 2º A utilização de sistemas de transmissão de dados e imagens não prejudica o cumprimento dos prazos, devendo os originais ser entregues em **juízo,** necessariamente, até cinco dias da date de seu término. Conforme matéria publicada pela Revista *Veja em 28/01/2004 pag. 78.*

Num futuro próximo, porém já presentes em alguns estados da federação, a utilização do e-mail para o envio de peças processuais, o que ocasionará uma revolução, na rotina dos advogados, pois os mesmos poderão praticar tais atos diretamente de seus computadores, eliminando uma série de gastos que se fazem necessários atualmente.

Do lado do judiciário, uma das opções é o envio das intimações por via eletrônica, vinculando o advogado ao processo e enviando-lhe todos os despachos e decisões proferidas, além de possibilitar a esse profissional o amplo acompanhamento processual sem o deslocamento até o cartório do fórum.

1.4 - Fases da Regulamentação das Novas Tecnologias

Existem projetos do governo federal desde o ano de 1996, procurando não ficar alheio à modernização, massificação e popularidade dos micro-computadores e tem apresentado projetos visando a modernização burocrática nos mais diversos âmbitos, mas é a partir de 1999 que foram editadas as primeiras disposições jurídicas sobre o tema como se demonstra a seguir.

Como já mencionado, veio a edição da lei 9.800/99, que permitiu às partes a utilização de meios eletrônicos para o envio de peças processuais sem prejuízo dos prazos, conforme determinado em seus artigos 1º e 2º. Em seu artigo 4º, atribui toda e qualquer responsabilidade sobre os dados transmitidos a quem fez a transmissão, bem como a entrega do material original que deverá ser no mesmo teor, sob pena de serem enquadrados como litigantes de má-fé.

É vital importância desse artigo da lei, pois trata da segurança das informações transmitidas, deverá ser confiável, par que no decurso desse processo, não possa haver alteração de dados, pois ocasionará uma dura sanção caso isso ocorra, tanto para a parte como para seu advogado por terem concorrido para a modificação dos dados.

Já o Decreto 3505, de 13 de junho de 2000, institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal, estabelecendo mais uma vez a vontade do governo de automatizar e incorporar as novas tendências tecnológicas.

O que chama bastante a atenção neste decreto, conforme artigo 1º descrito abaixo, que é constituído de importantes noções de como o governo brasileiro está preocupado com o desenvolvimento da tecnologia no país. A ponto de se assemelhar a um projeto de implantação tecnológica, compreendendo desde a segurança e privacidade da informação assim como a capacitação científica do país e até alertar para sua importância as demais instâncias da administração pública federal.

> “Art. 1º Fica instituída a Política de Segurança da Informação nos órgãos e nas entidades da Administração Pública Federal, que tem como pressupostos básicos:
>
> I - assegurar a garantia ao direito individual e coletivo das pessoas, à inviolabilidade da sua intimidade e ao sigilo da correspondência e das comunicações, nos termos previstos na Constituição;
>
> II - proteção de assuntos que mereçam tratamento especial;
>
> III - capacitação dos segmentos das tecnologias sensíveis;
>
> IV - uso soberano de mecanismos de segurança da informação, com o domínio de tecnologias sensíveis e duais;
>
> V - criação, desenvolvimento e manutenção de mentalidade de segurança da informação;
>
> VI - capacitação científico-tecnológica do País para uso da criptografia na segurança e defesa do Estado; e
>
> VII - conscientização dos órgãos e das entidades da Administração Pública Federal sobre a importância das informações processadas e sobre o risco da sua vulnerabilidade.”

Denota-se que há preocupação de se criar uma nova mentalidade sobra a segurança dos dados que trafegam pelo mundo virtual, bem como a preocupação com a capacitação e conscientização dos órgãos da administração sobra a importância da tecnologia a ser implementada.

O artigo 3º chama bastante a atenção e dispõe sobre os objetivos desta política pública.

> “Art. 3º São objetivos da Política da Informação:

I - dotar os órgãos e as entidades da Administração Pública Federal de instrumentos jurídicos, normativos e organizacionais que os capacitem científica, tecnológica e administrativamente a assegurar a confidencialidade, a integridade, a autenticidade, o não-repúdio e a disponibilidade dos dados e das informações tratadas, classificadas e sensíveis;

II - eliminar a dependência externa em relação a sistemas, equipamentos, dispositivos e atividades vinculadas à segurança dos sistemas de informação;

III - promover a capacitação de recursos humanos para o desenvolvimento de competência científico-tecnológica em segurança da informação;

IV - estabelecer normas jurídicas necessárias à efetiva implementação da segurança da informação;

V - promover as ações necessárias à implementação e manutenção da segurança da informação;

VI - promover o intercâmbio científico-tecnológico entre os órgãos e as entidades da Administração Pública Federal e as instituições públicas e privadas, sobre as atividades de segurança da informação;

VII - promover a capacitação industrial do País com vistas à sua autonomia no desenvolvimento e na fabricação de produtos que incorporem recursos criptográficos, assim como estimular o setor produtivo a participar competitivamente do mercado de bens e de serviços relacionados com a segurança da informação

VIII - assegurar a interoperabilidade entre os sistemas de segurança da informação.”

Fica assegurado toda e qualquer implementação de normas garantidoras do funcionamento e expansão da política governamental e principalmente na área jurídica, com a possibilidade do desenvolvimento de tecnologias próprias, para que o país não dependa das tecnologias desenvolvidas em outros países até porque, poderia comprometer as informações de segurança nacional.

Mais propriamente no âmbito jurídico, foi a Lei nº 10.259, de 12 de julho de 2001, que trouxe a mais inovadora transformação no tocante à prática de atos virtuais pelos operadores do direito, ao dispor sobre a instituição dos Juizados Especiais Cíveis e Criminais no âmbito da Justiça Federal.

Essa disposição está incluída no artigo 8º parágrafo segundo da lei, como segue reproduzido abaixo:

> "Art. 8º (...)
>
> § 2º Os tribunais poderão organizar serviço de intimação das partes e de recepção de petições por meio eletrônico."

Finalmente, avançando na ideologia de modernização total do poder público, foi instituída a Medida Provisória 2.200-2 editada em 24 de agosto de 2001, que institui a Política Nacional de **Infra-estrutura de Chaves Públicas**, criando uma autarquia federal –ICP-Brasil- responsável pela gestão dos Certificados Eletrônicos. Assim como para pesquisas e toda regulamentação necessária à formalização e à validação dos documentos que circularão por meios digitais através de delegação às Autoridades Certificadoras (AC) e Autoridades de Registro (AR), assuntos estes que serão tratados detalhadamente no decorrer deste trabalho.

No artigo 1º desta Medida Provisória procura especificar as áreas e o que se pretende instituir com essa política de segurança, como um marco da validade do documento eletrônico no Brasil.

> “Art. 1º Fica instituída a Infra-Estrutura de Chaves Públicas Brasileira - ICPBrasil, 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 ICP-Brasil –Infra-Estrutura de Chaves Públicas Brasileira, foi instituída e 2001 pelo governo federal, através da Medida Provisória mencionada, é constituída por um conjunto de regras e normas mas que fundamentalmente estão baseadas em padrões públicos **internacionais**, mas que são definidas aqui no Brasil, de acordo com nossa realidade jurídico-institucional, por um comitê gestor composto por representantes da sociedade civil e do governo federal.

A intenção é justamente garantir a autenticidade dos documentos eletrônicos, a ICP Brasil, disponibiliza um mecanismo, que concentra padrões técnicos e administrativos, que serão mais bem detalhados adiante, com o intuito de comprovar que a assinatura digital e os dados presentes em determinado documento eletrônico são na realidade, dignos de fé e autênticos.

Conforme comentado acima, dos dispositivos legais, o Judiciário Brasileiro nesse meio tempo, passou a admitir que algumas fases do processo sejam realizadas eletronicamente, como por exemplo, os despachos feitos por meio virtual, e que são assinados eletronicamente, com certificado digital, pelo juiz responsável.

O advento da Lei nº 11.280, de 17 de fevereiro de 2006, desde sua publicação já confirmou a tendência eletrônica dos mandamentos judiciais, incluindo o parágrafo único do artigo 154 do Código de Processo Civil, como segue:

> Parágrafo único. Os Tribunais, no âmbito da respectiva jurisdição, poderão disciplinar a prática e a comunicação oficial dos atos processuais por meios eletrônicos, atendidos os

> requisitos de autenticidade, integridade, validade jurídica e interoperabilidade da Infra-Estrutura de Chaves Públicas Brasileira – ICP – Brasil.

A celeridade no poder judiciário, aclamada todos os dias pela mídia e a população em geral, se aproxima com a adoção da certificação digital fazendo parte do dia-a-dia das ferramentas de trabalho nos gabinetes e secretarias do Poder Judiciário, que também sofre pressão de seu órgão controlador externo, que é o CNJ- Conselho Nacional de Justiça- que busca rapidez cada vez maior na prestação jurisdicional.

O viés legal oferecido e o mecanismo tecnológico à disposição, permitem que os juízes e desembargadores em geral, atendam aos princípios da instrumentalidade do Direito Processual, isto é, melhorar o exercício da prestação jurisdicional, tornando tal prestação mais segura e mais rápida.

A Justiça Federal Especial, assim como a Estadual e a maioria dos tribunais brasileiros, já adotam ou estão em vias de adotar a forma dos processos eletrônicos para peticionamento de todas as peças iniciais do processo e a abertura de vistas do andamento processual. O TST – Tribunal Superior do Trabalho, o TSE – Tribunal Superior Eleitoral e o STF – Supremo Tribunal Federal já permitem o peticionamento por intermédio de sua página disposta na Internet.

A certificação digital já foi utilizada pelo Tribunal Superior Eleitoral, para lacrar dos programas utilizados na votação eletrônica de outubro de 2008 os quais foram compilados, testados e assinados digitalmente pelo presidente do Tribunal e por representantes do Ministério Público, da Ordem dos Advogados do Brasil e por partidos políticos. Assim como foi publicada pelo TSE – a resolução nº 23.205/2010, mais especificamente em fevereiro de 2010, dispondo sobre a cerimônia de assinatura digital e fiscalização do sistema eletrônico que já foi implantado e utilizado nas eleições de 2010. O mais interessante, foi que o TSE, por intermédio de seu presidente submeteu os programas que seriam utilizados a vários profissionais de TI, que ficaram dias tentando quebrar a segurança do sistema das eleições. Vide Matéria da Folha de São Paulo a segir:

Até personagens da ficção, como MacGyver e James Bond, ficariam intrigados diante do esquema de segurança montado pelo Tribunal Superior Eleitoral para proteger os sistemas e as informações utilizadas nas eleições.
São duas salas-cofre, climatizadas, à prova de fogo e terremoto, com 90 computadores considerados o "centro nervoso" do processo eleitoral. Construídas em 2005, custaram R$ 7,5 milhões.

A Folha foi na manhã de ontem ao local, cujo acesso é restrito até mesmo para os ministros da corte. O secretário de Tecnologia da Informação do TSE, Giuseppe Janino, responsável pelo setor, só pode entrar lá acompanhado.
Em uma das salas ficam guardados o cadastro nacional de eleitores, o registro e a prestação de contas dos candidatos. Lá também se centraliza a apuração e totalização dos votos de todo o país. Apenas 30 pessoas têm permissão para entrar e só se informar senha e digitais.

Um sistema de ar-condicionado mantém a temperatura em 18ºC e verifica presença de fumaça. Em caso de incêndio, retira todo o oxigênio do local.
Em outra sala menor -e mais protegida- estão as ***matrizes dos softwares que fazem funcionar as urnas eletrônicas. Esses programas possuem assinaturas e registros digitais do TSE, da OAB, dos partidos e da Procuradoria Geral Eleitoral.*** *Em caso de suspeita de adulteração de urna, os técnicos* ***cruzam as assinaturas*** *presentes no sistema questionado com aquele guardado no tribunal.*

Para entrar nesse ambiente, cujo acesso é permitido a três pessoas, é preciso passar por seis portas codificadas, sendo que a quinta e a sexta só abrem quando a anterior fecha. Ontem, foi a primeira vez que um órgão de imprensa foi ao local, conhecido pelos servidores do TSE como "o cofre do cofre".
"Pode-se dizer que a fraude é inviável", garantiu Janino.
Em 2009, o TSE abriu prazo para que hackers tentassem invadir o sistema. Ninguém teve êxito. Segundo Janino, o TSE registrou em 2008 cerca de 200 tentativas de invasão por hora no dia da eleição municipal. Jornal Folha de São Paulo19/05/2010 – pg. A04

Os procedimentos acima descritos garantem a autoria, a integridade e a autenticidade dos programas desenvolvidos pelo TSE, que garante que os programas desenvolvidos pelo Tribunal não seriam passíveis de modificação e que desde o momento em que foram lacrados com a certificação digital, permaneceriam os mesmos até o dia da eleição.

Vale dizer, que todos o programas utilizados dentro da urna eletrônica são assinados digitalmente. Para assinatura digital, foi utilizado um algoritmo assimétrico proprietário e de conhecimento exclusivo do TSE.

O procedimento consiste no seguinte: ao ser iniciada, a urna eletrônica verifica a assinatura dos programas, e simplesmente não funciona em caso de não conformidade dos mesmos.

Esse processo de verificação automática permite a fiscalização da idoneidade dos softwares utilizados nos processos de votação, apuração e totalização dos votos, e concede total transparência até a última fase do processo de desenvolvimento de programas utilizados nas urnas, visto que, se uma simples alteração ou modificação vier a ser imposta impossibilita o uso do equipamento.

Os chamados **cartões inteligentes** –**smartcards**- são utilizados como mídia para conferir o padrão da Infraestrutura de chaves públicas –ICP – Brasil, do Instituto de Tecnologia da Informação da Casa Civil da Presidência da República. Este sistema será mais bem detalhado no decorrer deste trabalho.

Capítulo 2 – Segurança Tecnológica Necessária

No momento quero ressaltar que a certificação digital chegou para favorecer os órgãos do Poder Judiciário de agilidade no trâmite processual, favorecendo seu andamento, e auxiliando a diminuir a enorme quantidade de processos acumulados, assim como a agilização daqueles que dão entrada diuturnamente em todos os tribunais brasileiros.

2.1. A Questão da Segurança na Transmissão de Dados

Uma vez que já se está devidamente familiarizado com as questões da morosidade da justiça brasileira, bem como a par das legislações que contemplam a modernização das tecnologias da informação, pretende-se adentrar agora nos caminhos da segurança da informação e o envio de informações utilizando-se dos modernos meios tecnológicos disponíveis na atualidade por operadores jurídicos.

Se faz necessário iniciar conceituando algumas expressões que são a base para o entendimento do tema, tais como: Segurança, segurança da informação e por fim os pilares que garantem um processo eletrônico confiável.

Para conceituarmos “segurança” é consultado o dicionário Aurélio, pois além de fonte de consulta em larga escala, é o que melhor define o termo:

> “**segurança**. S. f. 1. Ato ou efeito de segurar(se). 2. Estado, qualidade ou condição de Seguro. 3. Convicção, certeza. 4. Confiança em si mesmo. S2g. 5. Bras. Pessoa encarregada da segurança pessoal de alguém, de empresa, etc.”

A segurança na área de informática se desenvolve desde as primeiras utilizações desta tecnologia e ganharam maior atenção com a implementação das redes e da Internet em virtude da possibilidade de compartilhar quaisquer tipos de dados e informações para qualquer lugar do mundo de uma forma segura.

Nasce então, o conceito de “Segurança da Informação”.

O Decreto nº 3505, de 13 de Junho de 2000, que institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal, conceitua segurança da informação como:

> “Art. 2º ....
>
> II - Segurança da Informação: proteção dos sistemas de informação contra a negação de serviço a usuários autorizados, assim como contra a intrusão, e a modificação desautorizada de dados ou informações, armazenados, em processamento ou em trânsito, abrangendo, inclusive, a segurança dos

> recursos humanos, da documentação e do material, das áreas e instalações das comunicações e computacional, assim como as destinadas a prevenir, detectar, deter e documentar eventuais ameaças a seu desenvolvimento.”

Uma das questões que se suscitou com a implantação de meios eletrônicos para auxiliar o processo é, se há segurança em termos absolutos nesta circulação da informação. A resposta foi, que ainda não havia segurança total, pois nada era seguro contra tudo e contra todos, mesmo com a tecnologia na época existente.

Hoje, a preocupação básica dos profissionais de Tecnologia da Informação é criar métodos que possam formar uma base confiável para os processos via meio eletrônico e sua possível regulamentação pelo Direito. Por este motivo, para se ter uma informação segura, há a presunção de cinco requisitos básicos: 1-Autenticação, 2-Privacidade, 3-Autorização, 4-Integridade dos Dados e 5-Não Repudio.

A questão mais importante de qualquer processo eletrônico é sem dúvida alguma a confiabilidade. Somente quando conseguirmos atender a todos esses requisitos acima numerados é que atingiremos o **processo eletrônico confiável**, que só para ilustrar ficaria como na figura abaixo, nos moldes do livro de Robson Machado. Onde os cinco pilares sustentam o **processo eletrônico confiável**, e que por sua vez são sustentados por uma **infra-estrutura de segurança** que para se manter de pé, necessita de uma **política de segurança**, sem a qual, todos os demais desestruturam.

2.2.Políticas de Segurança

Não há que se falar em segurança, sem antes definir suas políticas, são elas que devem impor as regras em que se baseiam toda a confiança no sistema. São elas também que mostram o que deve ser protegido e o que não precisamos proteger. São também responsáveis por mostrar contra quem é preciso proteger as informações. Tais definições estão contidas em documentos e regras que serão utilizadas em meio ao processo de transação eletrônica.

2.3. Infraestrutura de Segurança

A definição melhor para o termo seria a numeração dos conteúdos básicos para se garantir que as políticas de segurança sejam seguidas e podemos numerá-los e classificá-los da seguinte forma:

Do ponto de vista FÍSICO, são classificados os CPDs, com o antigo, mas ainda usual Centro de Processamento de Dados, com todos os seus controles de acesso, suas salas-cofre, os Servidores, Roteadores, os Hardwares de Firewall, e demais componentes sólidos.

Do ponto de vista LÓGICO, pode-se classificar os componentes em: primeiro e por uma questão prática, todos os sistemas operacionais, como por exemplo: o AIX da IBM, o Windows versão x da Microsoft, o Mac OS-x da Aple, e o sistema livre mais conhecido, que é o Linux, que são os mais comuns. Depois temos os programas antivírus, e anti-spyware, depois os softwares de firewalls.

Essa Infraestrutura explicada, pode ser considerada o mínimo que normalmente é adotado por qualquer empresa que coloque na internet a sua página. Porém, somente eles ainda não são suficientes para garantir o **Processo Eletrônico Confiável** apontado na figura anterior.

Seguindo os ensinamentos de Robson Machado, na descrição de um alicerce sólido e bem estruturado, onde se pode erguer os pilares do Processo Eletrônico Confiável, primeiro tratados de forma mais simples, apenas como apresentação, e em seguida tratados com mais refinamento técnico, como segue:

2.4. Autenticação

Autenticar-se, configura-se no ato de estabelecer ou confirmar algo (ou alguém) como autêntico, ou seja, que está a reivindicar a autoria e veracidade de alguma coisa. A autenticação também remete à confirmação da procedência de um objeto ou pessoa, que no neste caso, frequentemente relacionada com a verificação de sua identidade.

No jargão da segurança de informação, a autenticação é um processo que busca verificar a identidade digital do usuário de um sistema, normalmente, no momento em que ele requisita um acesso (login) em um programa de computador ou em um sistema operacional.

Reforçando, autenticar quer dizer provar a identidade de alguém. Quando se adquire um certificado digital na hierarquia da ICP – Brasil, por exemplo, o e-CPF, é obrigatório

ir pessoalmente a uma AR –autoridade de registro- levando todos os documentos pessoais.

O funcionário responsável na AR vai conferir e arquivar a cópia destes documentos junto com a assinatura de quem está requerendo, e uma declaração afirmando o conhecimento de todas as responsabilidades ligadas ao uso do certificado digital.

Fazendo uma analogia com a solicitação do RG –Carteira de Identidade, que utiliza alguns procedimentos de segurança, tais como: papel moeda, assinaturas, chancela de um órgão emissor etc., o certificado digital, ou e-CPF é semelhante, porém forma eletrônica.

A **pessoa** se autentica e prova que é ela mesma quem está portando o documento da seguinte forma:

Com algo ela possui: - Um RG, um CPF ou um Titulo de Eleitor, a Certidão de Nascimento, que possuem como característica desse meio de prova: 1-) É diretamente vinculado à pessoa para a qual foi emitido. 2-) É difícil de forjar, copiar ou alterar e 3-) É emitido por um terceiro confiável.

Com algo que ela sabe: - São representados pelos segredos que guarda, por exemplo o código PIN – personal identification number – que é uma senha de acesso ao cartão bancário ou ao token, que é o mesmo exemplo do PIN que fazem parte dos aparelhos de celular, que se dá pouca importância a ele, mas que é uma informação pessoal e que só o usuário do chip deve saber, tal qual as senhas de cartões de contas bancárias.

Com algo que ela é: - É o caso, por exemplo, das autenticações feitas com impressões digitais ou por meio de leitura da retina, reconhecimento de voz, assinatura etc., mas sempre guardam esses meios de autenticação, uma forma considerada intrusiva, e que sempre que guardado os bits gerados pela leitura, podem

ser copiados, e no caso da impressão digital, um ferimento nos dedos pode atrapalhar o reconhecimento, ou o desconforto de ter uma luz entrando nos olhos, ou um ruído no ambiente atrapalhar o mecanismo que reconhece o som da voz. Desta maneira, só é segura a autenticação, que é utilizada em um dispositivo no qual se possa garantir a integridade da informação que transita deste a leitora até o processo de identificação.

Com o intermédio da certificação digital: - que guarda as seguintes singularidades: 1- A identificação é inequívoca, o certificado presente no smartcard é associado a uma pessoa física ou jurídica. 2- Sua validade é facilmente verificada por outras pessoas, consultando on-line o órgão emissor, ou por programas que interpretam os certificados contidos no cartão. 3- Alto nível de proteção contra fraude e falsificação. 4- Vincula a uma transação a pessoa física ou jurídica portadora.

2.5. Privacidade

A privacidade é a habilidade de uma pessoa em controlar a exposição e a disponibilidade de informações acerca de si própria.

Está relacionada com a capacidade de existir na sociedade de forma anônima, bem como de garantir que as informações sobre si não sejam expostas de qualquer maneira. Alguns exemplos bastante usuais de informações que precisamos proteger em nosso dia a dia são o número de nosso cartão de crédito, as nossas senhas de banco e nossos dados pessoais.
Também se refere à capacidade que temos em garantir sigilo às informações mais sensíveis, protegendo-as conta acesso não autorizado. Se feita a comparação no mundo físico, a privacidade é almejada mediante o uso de medidas convencionais, como o uso de chaves, trancas, cofres, sistemas de alarme etc.. Essas medidas mostram-se eficazes pois dão a sensação de manter um controle de acesso físico às informações.

Porém quando se trata do ambiente digital, a internet, o problema de acesso físico à informação se torna complicado, tendo em vista, a infraestrutura que a informação trafega e que guardam um sério risco de serem interceptadas. Isso se deve

principalmente às redes baseadas no protocolo IP –todas- na atual versão IPv4, que quando criadas não tiveram lá grandes preocupações com a segurança. Quando a internet foi projetada, não havia a grande preocupação com a segurança da informação que se tem hoje. A utilização da rede de computadores se baseava em tornar mais fácil e ágil a comunicação entre as pessoas, e pelos recursos disponíveis na época, tornar a troca de informação mais amigável.

Neste quadro, se a internet não guarda grandes trancas para prover sigilo, e a privacidade é um dos pilares anteriormente descritos, para o processo eletrônico confiável, se faz necessário criar um mecanismo que possa conferir sigilo às transações eletrônicas, e esse mecanismo é o da criptografia.

2.6. Autorização

A autorização é o mecanismo responsável por garantir que apenas os usuários autorizados utilizam os recursos protegidos de forma controlada. É a autorização que garante que o usuário só vai conseguir fazer aquilo que ele realmente tem permissão para fazer.

No mundo físico, a autorização é concedida a alguém quando se confere a uma pessoa a senha do sistema de alarme, ou a chave das trancas, cadeados, para que ela possa desempenhar um determinado trabalho. Pode-se também conferir autorização por cargo ou função que guardam inerentes as responsabilidades que assumem, nas pessoas de gerentes da empresa, ou o presidente do tribunal e portanto a autorização já lhe está conferida.

Busca-se com a autorização de certificação digital, todas as aplicações que fazem funcionar um determinado processo eletrônico, já reconhecem de pronto o usuário e automaticamente lhe atribui as autorizações necessárias à execução de seus trabalhos, sejam de presidente do tribunal, um ministro dos tribunais superiores, um coordenador, um parceiro de negócios e até mesmo um usuário da internet.

2.7. Integridade dos Dados

A integridade é a garantia de que se possa identificar que um determinado dado ou informação não tenha sofrido alterações não autorizadas.

No mundo físico, se utiliza vários mecanismos para garantir a integridade dos dados, tais como: 1- Autenticação de cópias feitas em cartórios. 2- Assinatura de testemunhas. 3- Papéis especiais, dentre outros. Dentro desse contexto, quando é feito alguma alteração, com o intuito de forjar a informação contida naquele papel, sempre há meios técnicos e científicos utilizados para provar a alteração, seja da informação ou até mesmo da assinatura.

No mundo virtual, as técnicas digitais estão ficando tão aprimoradas com o uso de scanners, photoshop, leitores óticos etc., que a alteração do documento fica muito difícil de ser percebida. Há necessidade de um mecanismo criado para esse fim, que é denominado “resumo” (do inglês hash), com o qual, por processo matemáticos de criptografia, permite gerar um resumo do conteúdo do documento protegido.

Tal técnica garante que se for alterado um bit que seja do documento protegido, a assinatura que lhe confere autenticidade será definitivamente perdida tornando sem efeito a autenticidade anteriormente conferida.

2.8. Não Repúdio -

É a possibilidade de criar uma prova juridicamente aceita da vinculação de uma pessoa a um par de chaves criptográficas.

O Processo Jurídico Confiável é o resultado do êxito na tarefa de erguer os cinco pilares sobre os dois alicerces já citados. Alicerces estes, constituídos por regras, documentos e infraestrutura física e lógica no interior dos CPDs. O desafio que se propõe a seguir é mostrar como levantar os cinco pilares, resultando na

CERTIFICAÇÃO DIGITAL, e para isso adentra este estudo em detalhes mais aprofundados de questões técnicas sobre protocolos e procedimentos de criptografia, que é praticamente impossível não descrever, sob pena de descrédito do tema.

No mundo físico, ao se assinar um determinado documento, mesmo que a assinatura seja posta de forma errada, com características diferentes das usuais, existem técnicas periciais que podem demonstrar sua irregularidade ou ao contrário, afirmar que realmente foi aquela pessoa quem assinou, e determina o não repúdio.

No mundo virtual, para se garantir que o funcionamento de qualquer processo, que dependa da identificação inequívoca das pessoas envolvidas, utiliza-se os certificados digitais, que garantem o mecanismo de identificação sem dúvidas das partes envolvidas.

A emissão de um certificado digital, segue normas e técnicas que permitem a associação inequívoca daquele certificado com a pessoa que o possui. Sempre há um terceiro de confiança, entre o portador de um certificado digital e a outra parte envolvida. Este terceiro de confiança, é o responsável pela identificação do usuário e pela respectiva associação deste com o seu certificado digital.

Para se obter um certificado digital, é necessário apresentar documentos físicos, tais como RG, Foto 3x4 recente, Comprovante de Residência, Título de Eleitor, CPF, PIS etc, ao funcionário autorizado da AR –Autoridade de Registro. Que posteriormente solicita á sua Autoridade Certificadora vinculada, o certificado digital. A autoridade de registro é o terceiro de confiança nesta relação.

Pode-se traçar um paralelo entre o ato de se ir a um cartório de registro assinar um documento e faz o reconhecimento de firma. O oficial de registro neste momento é o terceiro de confiança, que fixa um selo do cartório juntamente com sua assinatura para atestar que a pessoa ali descrita realmente assinou aquele documento.

A Medida Provisória nº 2.200/2001 que institui a Infraestrutura de chaves públicas brasileira foi o marco da validade do documento eletrônico no Brasil. O detalhamento dos cinco pilares que sustentam um processo eletrônico confiável que é atendido pela

certificação digital, será estudado a seguir com explicações sobre a base da criptografia envolvida e todas as fases que dão confiabilidade às autoridades de registro.

Capítulo 3 - Criptografia -

A criptografia é uma ciência que usa a matemática (em forma de algoritmos) para ocultar, dados (embaralhar informações).
A palavra criptografia é originário do idioma grego, Kriptos, quer dizer escondido, oculto e grifo é a escrita. A criptografia consiste na arte de escrever em cifras ou em códigos não decifráveis a olhos nus, chamados de cifragem. Para decifrar a mensagem original, o destinatário aplica o processo inverso, a decifragem, que torna a mensagem legível novamente.

Criptografia é um algoritmo que visa esconder de forma embaralhada as informações sigilosas, tornando-as incompreensíveis às pessoas não autorizadas a lê-las, somente as autorizadas conseguem decifrá-las. A segurança em informática consiste na certeza de que as informações em uso não serão acessadas por qualquer um. O conhecimento destes fundamentos é importante para entender a infraestrutura de chaves públicas e a Certificação Digital.

3.1. História da Criptografia -

Há autores que apontam a criptografia existindo desde que existe comunicação escrita entre os humanos, e que se quis garantir a confidencialidade dessa comunicação, perto de 2.500 anos de história.

3.2. Método Scytale -

Um dos métodos de criptografia chamado “scytale” é atribuído às primeiras civilizações o uso de métodos e técnicas para embaralhar mensagens. Estima-se que surgiu com os gregos antigos em meados do séc. VI A.C.

O método consistia em uma vara que era chamada de scytale, na qual era enrolada uma fita de tecido em espiral até preenchê-la totalmente. Então começava a escrita no sentido longitudinal da fita enrolada. Depois desenrolava-se a fita, onde havia uma série de caracteres soltos e a enrolava em forma de bobina e remetendo-a ao destinatário, informando o comprimento e o diâmetro que deveria ser utilizado para enrolar a fita e ler o conteúdo.

As chaves da mensagem eram o comprimento e o diâmetro que deveria ser utilizado para enrolar a fita novamente e desencriptar a mensagem.

3.3. Substituição Numérica Monoalfabética -

Foi o método utilizado por Julio Cesar, esse método chamado de substituição monoalfabética por correspondente numérica. Onde cada letra do alfabeto é substituída por um número, na escala crescente. Exemplo:

01	02	03	04	05	06	07	08	09	10	11	12	13
A	B	C	D	E	F	G	H	I	J	K	L	M
14	15	16	17	18	19	20	21	22	23	24	25	26
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Dessa maneira, conforme a relação acima, estabelecia-se uma chave para a cifragem enviava ao destinatário. Por exemplo, para transmitir a palavra MENSAGEM mandaria os números: $_{m}13$, $_{e}05$, $_{n}14$, $_{s}19$, $_{a}01$, $_{g}07$, $_{e}05$, $_{m}13$. De posse dessa tabela, sempre que o destinatário recebesse uma mensagem com a chave 3, bastaria adicionar esse número à letra correspondente. Então o M seria 16, o E ficaria 08 e assim por diante. Se converter novamente os valores para letras. então a palavra MENSAGEM na chave 3 ficaria PHQVDJHP. Apesar de mais rebuscado o método é bem simples e o espaço de 26 chaves possíveis já é o suficiente para mostrar a sua fraqueza.

3.4. A Criptografia Para Fins Militares -

De uma cifragem simples, dos tempos antigos e modernos, entrou no século XX de forma muito mais sofisticada. Já nesta época utilizavam-se máquinas como apoio de cifrar e decifrar, que executavam o serviço de forma muito mais rápida e eficiente, que procurava transmitir mensagens ás tropas de maneira que o inimigo, mesmo interceptando a mensagem, ficaria muito confuso par entender. Neta mesma época desenvolveu-se métodos de análise dos métodos para decifrar a mensagem, a criptoanálise, que resume-se em estudar métodos para decifrar mensagens.

3.5. Criptografia Como Segurança de Dados -

A criptografia está intimamente relacionada com a segurança dos dados, assumindo um papel cada vez mais importante devido à grande quantidade de informações que são movimentadas e a utilização crescente da rede de computadores.

Davi Monteiro Diniz, aponta que “criptografia consiste em uma escrita que se baseia em um conjunto de símbolos cujo significado é conhecido por poucos, permitindo com isso que se criem textos que serão incompreensíveis aos que não saibam o padrão da conversão necessário para sua leitura”. Diniz, Davi Monteiro -Documentos Eletrônicos, Assinaturas Digitais:- Da Qualificação Jurídica dos Arquivos Digitais em Documentos. São Paulo LTR 1999.

Desta forma, uma mensagem só será criptográfica se tiver sido gerada a partir de um sistema metaliguístico e, ainda, tiver uma intenção enigmática.

Ângela Bittencourt Brasil esclarece que a técnica de assinatura feita através da criptografia e da criptoanálise "consiste numa mistura de dados ininteligíveis onde é necessário o uso de duas chaves, a pública e a privada, para que ele possa se tornar legível". Compara a criptografia como sendo semelhante ao segredo de um cofre forte. Esclarece, ainda, que essa assinatura é formada por uma série de letras, números e símbolos e é feita em duas etapas, sendo que na primeira o autor, através de um software que contém um algoritmo próprio, realiza uma operação e faz um tipo de resumo dos dados do documento que quer enviar, também chamado de função

hash. Em um segundo momento, ele utiliza a chave privada, a qual irá encriptar esse resumo e o resultado desse processo, que é a Assinatura Digital. *Brasil, Angela Bitencourt Membro do Ministério Público RJ.–Revista Jus Navigand, ano 5 nº 40 mar 2000.*

Em conclusão, aponta a mesma autora que a assinatura eletrônica, diferentemente da assinatura real, se modifica a cada arquivo transformado em documento, fazendo com que seu autor não a repita, como faz com as assinaturas apostas nos documentos reais.

Capítulo 4 -Técnicas Criptográficas

Existem essencialmente duas grandes técnicas de criptografia, denominadas simétrica e assimétrica. A criptografia simétrica, também conhecida como chave secreta ou tradicional, é a mais antiga. Servem de exemplos a Scytale e a numérica monoalfabética. Utiliza-se somente de uma chave, a qual está vinculada ao processo de cifragem e decifragem.

Em se tratando de criptografia assimétrica, também conhecida como chave pública, é utilizado um par de chaves, uma delas a pública, podendo ser amplamente conhecida, e a outra, a chave privada, conhecida apenas por seu proprietário. Aqui as chaves são totalmente independentes entre si; porém, uma chave completa a outra.

Conclui-se desta forma que a mensagem que é cifrada por uma chave privada somente poderá ser decifrada por uma chave pública correspondente.

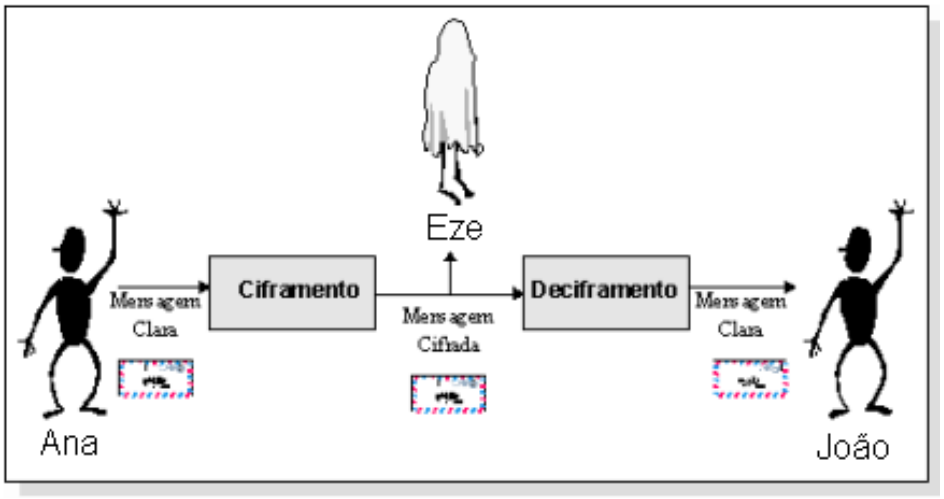
4.1. Criptografia Simétrica -

Nesse modelo de criptografia, também chamado de convencional, a mensagem a ser enviada é sempre decifrada pela mesma chave que a cifrou, ou seja, para que o destinatário consiga entender, terá que ser enviado também a chave a ele.

Por este método, também pode-se combinar uma determinada chave anteriormente, mas segurança sempre vai depender desta combinação ser segura ou não. Esse tipo de criptografia é bastante utilizada desde os anos 70 com os diversos tipos de hardware e software, pois a decifragem é bastante segura e exige pouco processamento.

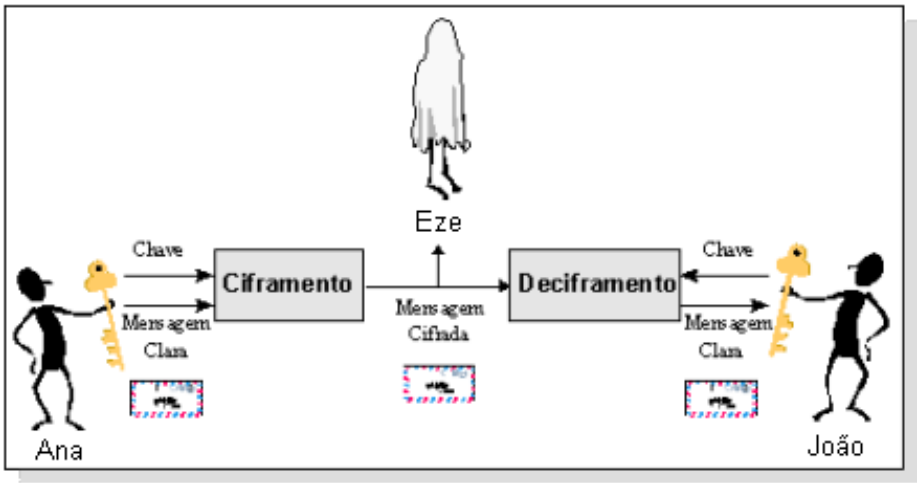
O modelo e as técnicas de criptografia sempre correram na frente da capacidade computacional, pois na medida em que esta última cresce, os sistemas criptográficos ficam mais sensíveis à quebra por um método que se convencionou chamar de força bruta, que não é nada mais do que o de tentativa e erro.

O ciframento de uma mensagem baseia-se em dois componentes: um algoritmo e uma chave. Um algoritmo é uma transformação matemática. Ele converte uma mensagem em claro em uma mensagem cifrada e vice-versa. Conforme nossos personagens, quando Ana (origem) cifra uma mensagem, ela utiliza um algoritmo de ciframento para transformar o conteúdo em claro da mensagem em texto cifrado. Quando João (destinatário) decifra uma mensagem, ele utiliza o algoritmo de deciframento correspondente para converter o texto cifrado de novo em uma mensagem clara (conforme figura)



Antigamente, a segurança do ciframento estava baseada somente no sigilo do algoritmo criptográfico. Se Eze (um intruso) conhecesse o algoritmo sem chave, poderia decifrar uma mensagem cifrada tão facilmente quanto João. Pode-se contornar o problema apresentado utilizando o segundo componente básico da criptografia de mensagens: a chave. Uma chave é uma cadeia aleatória de bits utilizada em conjunto com um algoritmo. Cada chave distinta faz com que o algoritmo trabalhe de forma ligeiramente diferente.

O número de chaves possíveis depende do tamanho (número de bits) da chave. Por exemplo, uma chave de 8 bits permite uma combinação de no máximo 256 chaves (2^8). Quanto maior o tamanho da chave, mais difícil quebrá-la, pois estamos aumentando o número de combinações.



Quando Ana cifra uma mensagem, ela utiliza um algoritmo de ciframento e uma chave secreta para transformar uma mensagem clara em um texto cifrado. João, por sua vez, ao decifrar uma mensagem, utiliza o algoritmo de deciframento correspondente e a mesma chave para transformar o texto cifrado em uma mensagem legível. Eze, por não possuir a chave secreta, mesmo conhecendo o algoritmo, não conseguirá decifrar a mensagem.

A segurança do sistema passa a residir não mais no algoritmo e sim na chave empregada. É ela que agora, no lugar do algoritmo, deverá ser mantida em segredo por Ana e João.

Quando a chave de ciframento é a mesma utilizada para deciframento ou esta última pode facilmente ser obtida a partir do conhecimento da primeira, ambas precisam ser compartilhadas previamente entre origem e destinatário, antes de se estabelecer o canal criptográfico desejado, utilizando-se um canal seguro e independente do destinado à comunicação sigilosa. Este tipo de ciframento emprega a criptografia conhecida como simétrica ou de chave secreta.

4.2. Descrição de Alguns Algoritmos Criptográficos Simétricos -

Dentre os mais conhecidos algoritmos simétricos estão: DES (Data Encyption Standard) com chaves de 40 a 56 bits. O Triple-DES – com chaves de 50, 112 e 168 bits. Estudos mostram que mesmo com três chaves distintas de 56 bits, alcançando 168 bits, o nível de segurança nunca ultrapassou os 112 bits. Depois temos desde o RC2 ao RC6 com chaves variando de 40 a 126.

DES (56 BITS) - 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.

Triple DES (112 E 168 Bits) - O 3DES é uma simples variação do DES, utilizando-o em três ciframentos sucessivos, podendo empregar uma versão com duas ou com três chaves diferentes. É seguro, porém muito lento para ser um algoritmo padrão.

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), começou a ser estudado em 1997 a partir de vários algoritmos apresentados pela comunidade. Os finalistas são: Serpent, Mars, RC6, Twofish e Rinjdael, e o resultado só foi divulgado no final de 2000.

IDEA (128 Bits) - O International 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 Bits) - Algoritmo desenvolvido por Bruce Schneier, que oferece a escolha entre maior segurança ou desempenho através de chaves de tamanho variável. O autor aperfeiçoou-o no Twofish, concorrente ao AES.

RC2 (8 a 1024 Bits) - 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.

4.3. Desvantagens da Criptografia Simétrica -

Apesar de sua simplicidade, existem alguns problemas na criptografia simétrica.

Como cada par necessita de uma chave para se comunicar de forma segura, para uma rede de n usuários precisaríamos de algo da ordem de n^2 chaves, quantidade esta que dificulta a gerência das chaves.

A chave deve ser trocada entre as partes e armazenada de maneira segura, o que nem sempre é fácil de ser garantido.

A criptografia simétrica não garante a identidade de quem enviou ou recebeu a mensagem –(Autenticidade e Não Repúdio).

Vale ressaltar que, de acordo com a lei de “Moore” que é comprovada na prática há mais de 30 anos, a capacidade computacional dobra a cada 18 meses, mas, apesar disso, a tecnologia e os recursos de criptografia também evoluem de forma a estarem sempre “anos luz” à frente da capacidade de quebra de qualquer sistema computacional.

Comprovada a evolução da criptoanálise, e em se tratando de chaves comercialmente utilizadas de 128, 256, e 512 bits, mesmo com tais recursos de capacidade computacionais, a quebra dessas chaves é extremamente improvável.

4.4. Criptografia Assimétrica -

Conforme observamos, sobre os mecanismos de criptografia utilizados atualmente, não se pode levantar dúvidas quanto á sua segurança. Porém, apenas um sistema de

criptografia forte não nos garante os pilares necessários. Dentre os cinco pilares já estudados, a criptografia simétrica nos proporciona apenas a privacidade. Portanto, ainda é preciso uma solução para erguer os polares da autenticação, autorização, integridade e não repúdio.

Como se não bastasse, o problema da criptografia simétrica está na distribuição das chaves, as quais precisam ser combinadas previamente e de forma segura entre emissor e receptor. Isso dificulta o uso dessa modalidade de criptografia para viabilizar um processo eletrônico confiável, pois ainda a combinação de chaves torna-se uma brecha na segurança.

A saída é utilizar outra modalidade de criptografia desenvolvida por chaves assimétricas, isto é, não há que se combinar uma chave para desencriptar a mensagem, pois não existe, nessa modalidade, apenas uma chave, mas sim duas que são utilizadas para cifrar a mensagem.

A modalidade de chaves assimétricas á muito mais fácil de gerenciar e, principalmente, muito mais versáteis, tendo em vista a liberdade existente na divulgação da chave pública.

Há porém, que se levar em conta que, o tempo de processamento para mensagens com criptografia assimétrica é muitas vezes maior do que a criptografia simétrica, e isso pode limitar seu uso em determinadas situações. A força da criptografia assimétrica, ou de chave pública, depende da dificuldade de fatoração de números muito grandes. Devido a essa exigência, os sistemas assimétricos geralmente não são tão eficientes computacionalmente falando, quanto os simétricos. Só para se ter uma idéia, um algoritmo RSA de chave pública (assimétrica) chega a ser 100 vezes mais lento que o DES de chave secreta (simétrica).

E continuando o exemplo, se formos criptografar apenas uma frase, computacionalmente falando, talvez fosse indiferente a utilização de um ou outro

método. Mas quando a necessidade é de criptografar grandes volumes de textos ou mesmo arquivos eletrônicos, a criptografia assimétrica se mostra pouco eficiente. A solução encontrada para o problema foi utilizar a criptografia assimétrica apenas para trocar a chave secreta de forma segura e, uma vez estando os interlocutores de posse da chave secreta, utilizar a criptografia simétrica para cifrar suas mensagens e arquivos.

Essa modalidade de chaves públicas foi criada nos anos de 1970, a criptografia assimétrica surge como solução para o problema de troca de chaves entre os interlocutores. Nesta modalidade, são usadas duas chaves ligadas matematicamente. Uma delas é mantida em segredo e é denominada chave privativa.

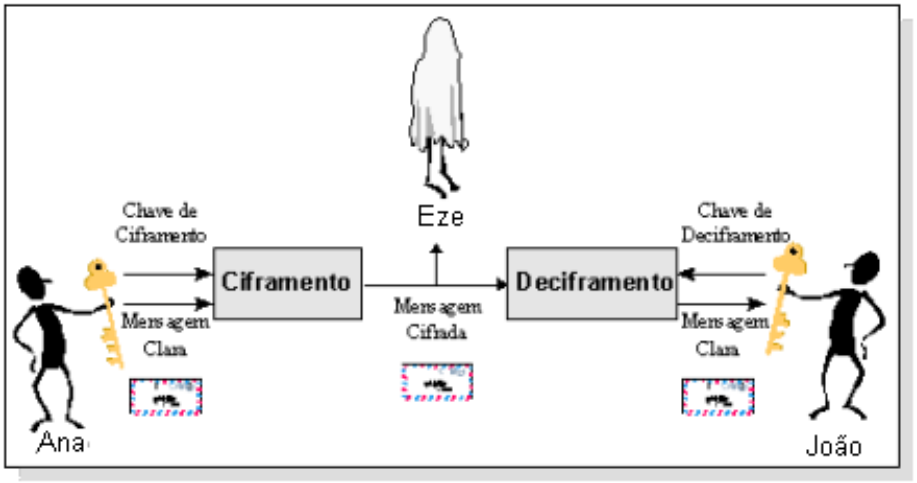
Como o próprio nome diz, essa chave privativa pode ser representada como sendo a identidade do seu proprietário, logo, como novamente o seu nome sugere, sua privacidade é crucial. A outra chave, denominada chave pública, pode estar disponível a todos.

Reforçando ainda mais o conceito, e a Idea é tornar repetitivo o conceito para melhor fixá-lo. A maneira de contornar os problemas da criptografia simétrica é a utilização da criptografia assimétrica ou de chave pública. A criptografia assimétrica está baseada no conceito de par de chaves: uma chave privada e uma chave pública. Qualquer uma das chaves é utilizada para cifrar uma mensagem e a outra para decifrá-la. As mensagens cifradas com uma das chaves do par só podem ser decifradas com a outra chave correspondente. A chave privada deve ser mantida secreta enquanto a chave pública é mantida disponível livremente para qualquer interessado.

De uma forma simplificada, o sistema funciona assim: João e todos os que desejam comunicar-se de modo seguro geram uma chave de ciframento e sua correspondente chave de deciframento (conforme figura seguinte). Ele mantém secreta a chave de deciframento; esta é chamada de sua chave privada. Ele torna pública a chave de ciframento. Chamada de chave pública.

A chave pública realmente condiz com seu nome. Qualquer pessoa pode obter uma cópia dela. João inclusive encoraja isto, enviando-a para seus amigos ou publicando-a em boletins. Assim, Eze não tem nenhuma dificuldade em obtê-la. Quando Ana deseja enviar uma mensagem somente para a João, (sigilo) precisa primeiro encontrar a chave publica dele.

Feito isto, ela cifra sua mensagem utilizando a chave pública de João, despachando-a em seguida. Quando João recebe a mensagem, ele a decifra facilmente com sua chave privada. Eze, que interceptou a mensagem em trânsito, não conhece a chave privada de João, embora conheça sua chave pública. Mas este conhecimento não o ajuda a decifrar a mensagem. Mesmo Ana, que foi quem cifrou a mensagem com a chave pública de João não pode decifrá-la agora.



A grande vantagem deste sistema é permitir que qualquer um possa enviar uma mensagem secreta, apenas utilizando a chave pública de quem irá recebê-la. Como a chave pública está amplamente disponível, não há necessidade do envio de chaves como é feito no modelo simétrico. A confidencialidade da mensagem é garantida, enquanto a chave privada estiver segura. Caso contrário, quem possuir acesso á chave privada terá acesso às mensagens.

Dentro dessa Criptografia de chave pública encontram-se os seus criadores e que na verdade foram os que inspiraram tal modelo de criptografia, que são Diffie e Hellman, que definiram o modelo que usamos até hoje em nosso sistema de certificação digital.

A Idéia do sistema de Whitfield Diffie e Martin Hellman, que no ano de 1976, apresentaram no IEEE –Institute of Eletrical and Eletronic Enginners- que foi fundado nos Estados Unidos em 1884, um artigo chamado New Directions in Cryptography, tansactions on Information Theory. Este nome revolucionou os sistemas criptográficos existentes. Em uma só tacada, este procedimento criou dois tipos de serviços. A Assinatura Digital, que é criada através do uso da Chave Privada e sua verificação é feita utilizando a chave pública, e o Sigilo, que utiliza a chave pública do destinatário, o qual deve utilizar sua chave privada para decifrar uma mensagem.

4.5. Descrição de Alguns Algoritmos Assimétricos -

Muito embora terem sido considerados os precursores da criptografia de chaves públicas, nem Diffie, nem Hellman, conseguiram implementar o sistema. A solução foi encontrada com a criação do **RSA** em 1977 e publicada em 1987 por três professores do MIT: -Massachusetts Institute of Technology- Ron Rivest, Adi Shamir e Leonard Adleman, que a exemplo do método Diffie-Hellman, o RSA também depende de uma função unidirecional. Porém, ao invés de logaritmos discretos e exponenciação, o RSA utiliza a multiplicação e a fatoração de números primos.

O **RSA**, se baseia no fato de que é muito fácil e rápido multiplicar números primos, mas é extremamente difícil fatorar o produto de números primos grandes. Produtos de números primos pequenos são fáceis de fatorar, por exemplo:- 77 = 7x11, mas quando estes números aumentam, a dificuldade aparece, por exemplo: 408.508.091 = 18.313x22.307. Gerar a chave pública envolve multiplicar dois primos grandes; qualquer um pode fazer isto.

Derivar a chave privada a partir da chave pública envolve fatorar um grande número. Se o número for grande o suficiente e bem escolhido, então ninguém pode fazer isto em uma quantidade de tempo razoável. Assim, a segurança do RSA baseia-se na dificuldade de fatoração de números grandes. Deste modo, a fatoração representa um limite muito superior ao tempo necessário para quebrar o algoritmo.

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.

O RSA – Caso não foi ainda percebido, 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, atualmente, o algoritmo de chave pública mais amplamente utilizado, além de ser uma das mais poderosas formas de criptografia de chave pública conhecidas até o momento. O RSA utiliza números primos grandes como descrito acima. 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 baseia-se na dificuldade de fatoração de números primos grandes.

ElGAMAL - O ElGamal é outro 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.

Apenas finalizando falando um pouco mais de RSA, o uso da criptoanálise avançou muito na frente da capacidade computacional de força bruta, que são as tentativas de quebra de chaves por tentativa e erro.

Para se ter uma idéia da força do RSA, em 1977 foi lançado um desafio, que foi fatorar um número de 129 dígitos. Somente em 1994, o número foi fatorado com sucesso por 600 voluntários. Assim temos estimativas de organismos internacionais, tais como o NIST –National Institute of Standards and Technology, prevêem que chaves do tipo RSA, de 2048 bits, ainda durarão por cerca de 10 anos e que chaves RSA de 4096 dígitos terão, no mínimo, mais 20 anos de vida.

Capítulo 5 – Resumo de Mensagens Dentro da Assinatura Digital-

Sem querer estender muito, o resumo –HASH em inglês-, consiste em gerar um valor chamado de –message digest- (MD), termo em inglês para Resumo de Mensagem, partindo-se de um texto qualquer.

Entra então na questão, o algoritmo HASH, que é composto por fórmulas e funções matemáticas unidirecionais complexas, que garantem a irreversibilidade e a unicidade do MD gerado. Isso significa que textos diferentes não produzem o mesmo MD. A alteração de um único bit na mensagem gera um MD completamente diferente.

Encontram-se diversos algoritmos de HASH, mas para que sejam úteis ao propósito é que sejam criptograficamente seguros, deverá atender aos seguintes requisitos:

SEM RETORNO- Deverá ser difícil ou impossível determinar a mensagem que produziu aquele HASH. Isso impedirá que alguém substitua uma mensagem por outra que tenha o mesmo HASH.

ALEATORIEDADE- a mensagem deverá parecer aleatória, também para impedir que alguém determine a mensagem original.

EXCLUSIVIDADE- o HASH deverá ser exclusivo, de modo que a existência de duas mensagens com o mesmo message digest seja praticamente impossível. Vale ressaltar que a identificação de HASHs repetidos, implicam a necessidade de revisão do algoritmo e ensejam a edição de uma nova versão com uma quantidade de chaves maior, permitindo assim maior exclusividade.

5.1 - Função Hashing -

A Assinatura Digital obtida através do uso da criptografia assimétrica ou de chave pública infelizmente não pode ser empregada, na prática, de forma isolada, do modo como foi didaticamente descrito no item anterior. Está faltando, portanto, descrever um mecanismo fundamental para o adequado emprego da Assinatura Digital. Este mecanismo é a função Hashing. Sua utilização como componente de assinaturas digitais se faz necessário devido à lentidão dos algoritmos assimétricos, em geral, cerca de 1.000 vexe mais lentos do que os simétricos.

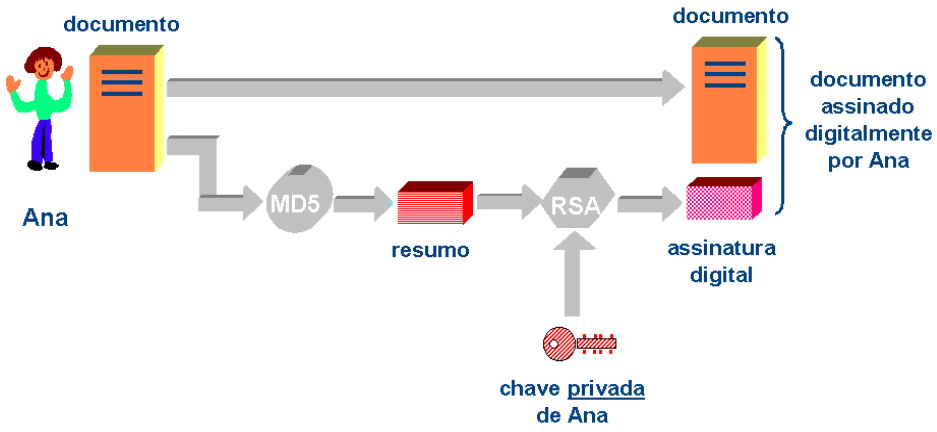
Assim, na prática é inviável e contraproducente utilizar puramente algoritmos de chave pública para assinaturas digitais, principalmente quando se deseja assinar grandes mensagens, que podem levar preciosos minutos ou mesmo horas para serem integralmente "cifradas" com a chave privada de alguém. Ao invés disso, é empregada uma função Hashing, que gera um valor pequeno, de tamanho fixo, derivado da mensagem que se pretende assinar, de qualquer tamanho. Assim, a função Hashing oferece agilidade nas assinaturas digitais, além de integridade confiável como descrito a seguir:

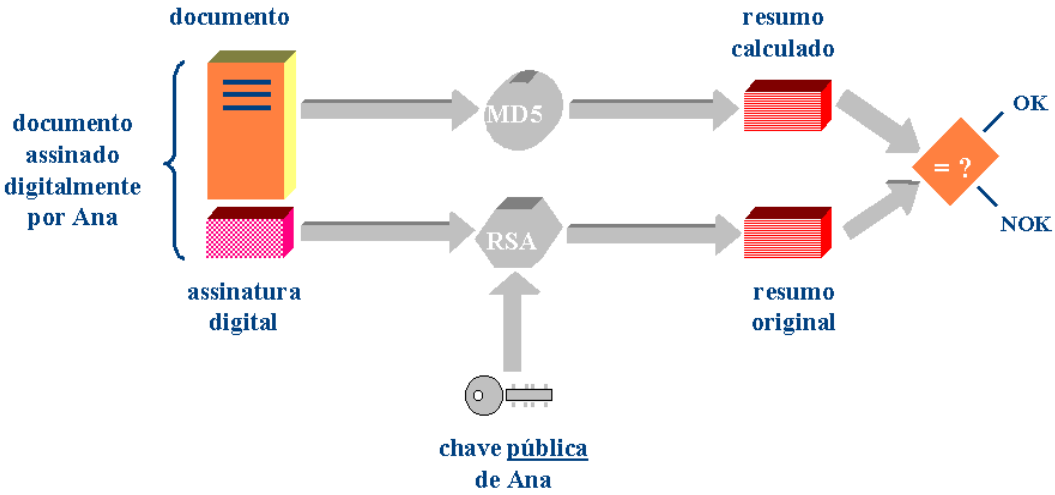
Também denominada Message Digest, One-Way Hash Function, Função de Condensação ou Função de Espalhamento Unidirecional, a função Hashing funciona como uma impressão digital de uma mensagem, gerando, a partir de uma entrada de tamanho variável, um valor fixo pequeno, o digest, ou o valor HASH.

Vários algoritmos de message digest exibem essas propriedades. Os mais utilizados são o MD5, que é uma melhoria do MD4 e o SHA. O MD4, desenvolvido em 1990 por Ron Rivest, é um algoritmo de 128 bits, ou seja de 16 caracteres de 8 bits uma vez que cada caractere ocupa 1 byte de oito bits. Na prática, não há limite quanto ao tamanho to texto a ser submetido a um algoritmo HASH, porém, o resultado obtido será sempre o tamanho determinado pelo algoritmo escolhido.

O tamanho do MD depende do algoritmo escolhido (MD1, MD2....5, SHA1, SHA256, SHA512, que é medido em bits. O SHA, desenvolvido pela NSA –National Security Agency- Agência Nacional de Segurança e pelo NIST, já denominado, -Instituto Nacional de Padrões e Tecnologia, ambos do governo dos EUA, recebe como entrada um documento qualquer sob a forma digital com um tamanho de até 2 elevado a 64 bits -18.446.744.073.709.551.616 bits- ou 2.305.843.009.213.693.952 (2,5 quintilhões) de bytes, ou caracteres.

Este valor está para o conteúdo da mensagem assim como o dígito verificador de uma conta-corrente está para o número da conta. Serve, portanto, para garantir a integridade do conteúdo da mensagem que representa. Assim, após o valor hash de uma mensagem ter sido calculado através do emprego de uma função hashing, qualquer modificação em seu conteúdo -mesmo em apenas um bit da mensagem - será detectada, pois um novo cálculo do valor hash sobre o conteúdo modificado resultará em um valor hash bastante distinto, conforme ilustração abaixo.





Só a título de curiosidade, o SHA1, do Hino Nacional Brasileiro completo é: “2072b1e8dd762481ee34558ab19a7950b05473a9” . Este trabalho digitado até a presente página gerou um SHA1 = “40c91802e669f5c937ad7af961249869f07e1712” isso pode ser testado em: http://redeicpbrasil.viainternet.com.br, entra-se com o texto e escolhe-se o algoritmo.

Atualmente a ICP – Brasil por medida de segurança, nas novas raízes V2 e V3, utilizarão apenas algoritmos SHA256 e SHA512, abolindo definitivamente o uso do SHA1, que tem expectativa de vida útil até 2013, apenas para certificados já emitidos nas raízes V) e V1.

Um documento cifrado é dito computacionalmente seguro, quando atende aos seguintes critérios:

a-) O custo para quebrar o texto cifrado excede o valor da informação cifrada.

b-) O tempo requerido para quebrar o texto cifrado excede o tempo de vida útil da informação.

5.2. Assinatura Digital e Assinatura Eletrônica -

Quando temos uma assinatura eletrônica, sabemos que esta representa um conjunto de dados, no formato eletrônico, que é anexado ou logicamente associado a um outro conjunto de dados, também no formato eletrônico, para conferir-lhe autenticidade ou autoria.

Podemos afirmar então que a assinatura eletrônica pode ser obtida por meio de diversos dispositivos ou sistemas, como login/senha, biometria, imposição de PIN etc. Um dos tipos de assinatura eletrônica é a assinatura digital, que utiliza pares de chaves criptográficas associadas a certificados digitais.

É bom ficar claro que no decorrer deste trabalho sempre que se fizer referência a assinaturas digitais, entende-se que são aquelas produzidas com a utilização de chaves criptográficas privativas associadas a certificados digitais da ICP – Brasil.

Assim como dado o HASH da mensagem que foi demonstrado acima, e repassado de interlocutor ANA, a outro interlocutor João, pode ter fica do uma questão: E se no meio do caminho um intruso intercepta a mensagem de Ana, adultera a mensagem, gera um novo HASH e manda ao João mensagem e HASH alterados? Para que a esta comunicação seja 100% confiável, precisaremos garantir, sem qualquer possibilidade de dúvida, que a mensagem é realmente de Ana.

Essa garantia é oferecida pela Assinatura Digital. Da seguinte forma: Já foi demonstrado que Ana possui um par de chaves criptograficamente ligadas, representado por sua chave privativa, a qual apenas ela tem acesso, e por sua chave pública, que como o próprio nome diz, é domínio público. Já foi demonstrado também que qualquer mensagem cifrada pela chave privativa do emissor só pode ser decifrada com a utilização da respectiva chave pública deste mesmo emissor e vice-versa.

Sendo assim, se Ana cifrar a mensagem com sua chave privativa, ela estará, na verdade, **“assinando”** esta mensagem, pois qualquer pessoa poderá decifrar a mensagem utilizando a chave pública de Ana, entretanto **apenas** Ana poderia ter sido capaz de cifrá-la.

Desta feita, soluciona-se o problema acima colocado. Se a mensagem for interceptada, mas antes foi assinada por Ana, por mais que o interceptador faça, ele nunca poderá repassar a mensagem **alterada** como se fosse de Ana, pois ele não possui a chave privativa de Ana para assinar a mensagem e endereçar novamente como se de Ana fosse. Com a certificação e assinatura digital de Ana, garantimos a autenticidade.

Outra questão: E se o sigilo for necessário? A autenticidade não é diretamente proporcional ao sigilo. Então, caso Ana deseje que apenas João consiga ler a sua mensagem, ela deverá cifrá-la uma segunda vez, agora, utilizando a chave pública de João, desta forma, apenas a chave privativa de João poderá abrir a mensagem. Esse procedimento garante a integridade e a autenticação do remetente.

Com os procedimentos descritos, pode-se afirmar que os cinco pilares de um processo eletrônico confiável foram erguidos, a saber:

AUTENTICAÇÃO:- Somente Ana poderia ter cifrado o HASH da mensagem utilizando sua chave privativa, portanto, uma vez que João consiga decifrar este HASH utilizando a chave pública de Ana, ele terá a certeza de que a mensagem é autêntica.

PRIVACIDADE:- Assim como Ana cifrou a mensagem com uma cave simétrica e enviou esta chave criptografada com a chave pública de João. Portanto, João foi o único capaz de decifrá-la com sua chave privativa.

AUTORIZAÇÃO:- Conforme demonstrado, sempre que podemos identificar o remetente e o destinatário, podemos definir o nível de autorização.

INTEGRIDADE DOS DADOS:- Se João foi capaz de calcular o HASH da mensagem e compará-lo ao HASH recebido de Ana, certificou-se que ambos os HASHs são idênticos e garantindo que a mensagem estava íntegra.

NÃO REPÚDIO:- Uma vez que apenas Ana tem acesso à sua chave privativa, utilizada para assinar a mensagem, somente ela poderia tê-la assinado, portanto Ana não poderá repudiar a autoria da mensagem.

5.3. Alguns Exemplos Práticos de Certificação Digital -

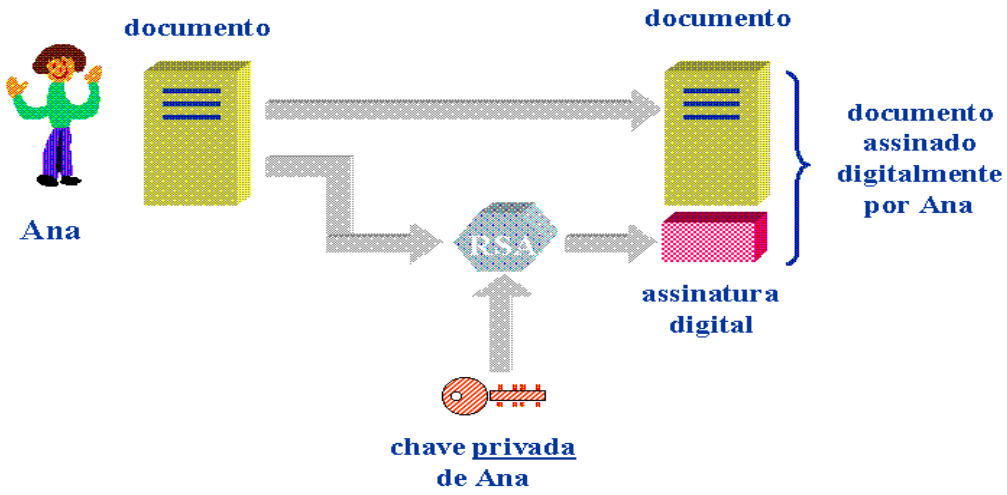
Quando o termo Processo Eletrônico Confiável, expressão diversas vezes repedido neste texto, não quer dizer que é sinônimo de processo judicial. É também um modelo para se aplicar ao judiciário, como será largamente exposto mais adiante. O conceito é amplo, servindo também a outras aplicações, a saber:

Comércio Eletrônico:-

Se imaginarmos uma compra pela Internet, podemos perceber a necessidade de todos os requisitos acima. Por exemplo, a informação que permite a transação - tais como valor e descrição do produto adquirido -precisa estar disponível no dia e na hora que o cliente desejar efetuá-la (disponibilidade), o valor da transação não pode ser alterado (integridade), somente o cliente que está comprando e o comerciante devem ter acesso à transação (controle de acesso), o cliente que está comprando deve ser realmente quem diz ser (autenticidade), o cliente tem como provar o pagamento e o comerciante não têm como negar o recebimento (não-repúdio) e o conhecimento do conteúdo da transação fica restrito aos envolvidos (privacidade).

Assinatura Digital:-

Outro benefício da criptografia aliada à certificação digital com chave pública é a Assinatura Digital, que permite garantir a autenticidade de quem envia a mensagem, associada à integridade do seu conteúdo. Por exemplo, suponha que Ana (origem) queira comunicar o nascimento de sua filha para todos os seus amigos (destinatários = João), mas queira garantir aos mesmos que a mensagem foi enviada realmente por ela. E, embora não se importe com o sigilo da mensagem, deseja que a mesma chegue íntegra aos destinatários, sem alterações como, por exemplo, do sexo da criança.



Ana então cifra a mensagem com sua chave privada e a envia, em um processo denominado de Assinatura Digital. Cada um que receber a mensagem deverá decifrá-la, ou seja, verificar a validade da Assinatura Digital, utilizando para isso a chave pública de Ana. Como a chave pública de Ana apenas decifra (ou seja, verifica a validade de) mensagens cifradas com sua chave privada, fica garantida assim a autenticidade, integridade e não-repudiação da mensagem. Pois se alguém modificar um bit do conteúdo da mensagem ou se outra pessoa assiná-la ao invés de Ana, o sistema de verificação não irá reconhecer a Assinatura Digital de Ana como sendo válida.

5.4. Criptografia Simétrica X Assimétrica -

Diante do que já foi apresentado pode ser que haja alguma dúvida sobre qual o modelo de criptografia deve ser utilizado, se simétrico ou assimétrico. A resposta é simples, um modelo híbrido.

Conforme já mencionado, o algoritmo simétrico é muito mais rápido quando utilizado no ciframento da mensagem em si. Enquanto o assimétrico, embora lento permite implementar a distribuição de chaves e a assinatura digital.

Além disso, como já também apresentado no item anterior, deve-se utilizar também o mecanismo de HASHing para o complemento da assinatura digital.

Criptografia Simétrica.	Criptografia Assimétrica.
Rápida.	Lenta.
Gerência e distribuição das chaves é complexa.	Gerência e distribuição simples.
Não oferece Assinatura Digital	Oferece Assinatura Digital.

Em resumo, os algoritmos criptográficos podem ser combinados para a implementação dos três mecanismos criptográficos básicos: o ciframento, a assinatura e o Hashing. Estes mecanismos são componentes dos protocolos criptográficos, embutidos na arquitetura de segurança dos produtos destinados ao comércio eletrônico.

Estes protocolos criptográficos, portanto, provêm os serviços associados à criptografia que viabilizam o comércio eletrônico: disponibilidade, sigilo, controle de acesso, autenticidade, integridade e não repúdio.

5.5. Protocolos que empregam Sistemas Criptográficos Híbridos -

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).

5.6. O Certificado Digital -

Durante todo o processo de explicação até aqui, de algoritmos de criptografia simétrica, assimétrica, métodos híbridos, protocolos envolvidos etc.. Porém infelizmente, o uso dos recursos criptográficos estudados até agora apenas garantem que o dono do par de chaves realizou as operações, mas quem garante que o par de chaves em questão pertence realmente a uma determinada pessoa? Não existe nenhum mecanismo que impeça que um usuário crie um par de chaves com o nome de outro usuário.

O certificado digital nada mais é do que um arquivo eletrônico que, contendo as chaves criptográficas de uma entidade (pessoa física ou jurídica, máquina ou aplicação), associa essas chaves a informações relativas à entidade, permitindo dizer se ela é quem realmente se diz ser. Esse certificado, como dito, é um arquivo digital de computador que, como os demais documentos tradicionais de identificação, além dos dados do indivíduo ou entidade, possuem também uma Chave Pública do assinante. Estes documentos eletrônicos são chancelados digitalmente pela entidade emissora, conhecida como Autoridade Certificadora, com o objetivo de interligar a Chave Pública a uma pessoa ou entidade, possuindo o mesmo valor do documento

físico, como carteira de identidade, passaporte, cartões de crédito, e utilizados da mesma forma da identificação de indivíduos ou entidades na rede que, ao serem apresentados, servem como prova de identificação. O certificado Digital, serve também como mecanismo para divulgação da Chave Pública.

Na Certificação Digital é utilizada, como base, a tecnologia de criptografia de chave pública, onde a chave pública é armazenada no certificado e a chave privada é guardada sigilosamente pelo assinante. Qualquer mensagem ou código pode ser assinado utilizando-se a Chave Privada do assinante, porém esta assinatura só será validada com a Chave Pública correspondente.

Podemos dizer que um certificado digital é uma carteira de identidade virtual.

Quanto a um documento oficial de identificação, como por exemplo o RG, é expedido pela Secretaria de Segurança Pública (SSP), atestando quem aquela pessoa portadota realmente é, e no documento estão alguns quesitos de segurança, tais como o papel especial, a chancela pública, a foto, a assinatura, e a impressão digital do portador etc..

No mundo digital, o processo não é muito diferente. Analogamente a uma estrutura hierárquica existente na expedição de um RG, a certificação digital pressupõe uma estrutura que envolve: Autoridade Raiz de Certificação, Autoridade Intermediária de Certificação e Autoridade de Registro.

PROCESSO PAPEL	PROCESSO DIGITAL
MJ – MINESTÉRIO DA JUSTIÇA	AC - RAIZ
SSP – SECRETARIA DE SEGURANÇA PÚBLICA	AC- AUTORIDADE INTERMEDIARIA DE CERTIFICAÇÃO
INSTITUTO DE IDENTIFICAÇÃO	AR – AUTORIDADE DE REGISTRO
RG	CERTIFICAÇÃO DIGITAL

Analogia entre o processo de emissão de um RG e de um Certificado Digital

5.7. Autoridade Certificadora Raiz -

A AC-Raiz 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" (art. 5º. da MP 2.200-2). A ela compete:

a)emitir, expedir, distribuir, revogar e gerenciar os certificados das AC de nível imediatamente subseqüente ao seu;

b)gerenciar a lista de certificados emitidos, revogados e vencidos;

c)executar atividades de fiscalização e auditoria das AC e das AR e dos prestadores de serviço habilitados na ICP, em conformidade com as diretrizes e normas técnicas estabelecidas pelo Comitê Gestor da ICP-Brasil;

d)exercer outras atribuições que lhe forem cometidas pela autoridade gestora de políticas.

O papel de Autoridade Certificadora Raiz da ICP-Brasil é Desempenhado pelo ITI – Instituto Nacional de Tecnologia da Informação (art. 13 da MP). O ITI foi transformado em autarquia federal vinculada ao Ministério da Ciência e Tecnologia.

Capítulo 6 - Infraestrutura de Chaves Públicas Brasileira -ICP – BRASIL-

Uma Infra-Estrutura de Chaves Públicas (ICP) é um conjunto de regimes normativos, procedimentos, padrões e formatos técnicos que viabilizam o uso em escala da criptografia de chaves públicas; constitui um modelo formado por autoridades certificadoras responsáveis pela geração e gerenciamento de chaves e certificados públicos, utilizados (como método ou tecnologia viável) para garantir a autenticidade, a integridade e a validade jurídica de documentos e transações eletrônicas.

Dependendo do modelo de ICP escolhido, os certificados emitidos por uma autoridade certificadora (AC) têm um âmbito de utilização de maior ou menor alcance. Explica-se: as autoridades certificadoras desempenham um papel crucial na Infra-Estrutura de Chaves Públicas, pois são elas quem expedem e controlam o uso dos certificados digitais. As AC's são organizadas e funcionam com base em um predeterminado número de regras e convenções, que dão forma ao próprio modelo de ICP.

Existem diferentes modelos de infra-estrutura de chaves públicas, que podem ser escolhidos de acordo com as várias necessidades. Em outras palavras, existem distintas alternativas mediante as quais as organizações podem criar relações de intercâmbio confiáveis, cuja complexidade é diretamente proporcional à quantidade de autoridades certificadoras (AC´s) envolvidas (e que podem se relacionar entre si.

Dependendo do modelo escolhido, as autoridades certificadoras estarão aptas a gerar certificados limitados ou de uso geral. Por exemplo, num modelo de uma única AC, é muito mais simples a administração do intercâmbio de certificados entre ela e os

usuários finais. Somente ela expede e controla os certificados, criando um universo de certificação limitado ao espaço das relações de seus associados.

Os usuários encontram na AC única o "ponto de confiança" comum, e assim usam seus certificados para confirmar a validez das chaves e identificar um ao outro. O processo do "caminho da certificação" passa sempre pela mesma e única AC.

A administração de um sistema (modelo) assim é muito mais simples, mas em compensação os certificados emitidos são de uso restrito para identificação dos usuários vinculados à AC única. Forma-se uma rede de confiança de espectro bastante reduzido.

A situação se complica se houver necessidade de estabelecer relação com outras pessoas (usuários) que não possuem certificados emitidos pela mesma AC. Para superar essa limitação, ou seja, para se operar a "escalabilidade" e extensão da cadeia de certificação original, criando-se novas "cadeias de confiança", dois caminhos podem ser seguidos: o primeiro, é o da certificação cruzada. Por esse meio, diferentes AC’s intercambiam certificados entre elas, ou seja, emitem certificados cruzados.

Quando um certificado cruzado é emitido, ocorre a expansão da cadeia de confiança de uma AC. Um usuário vinculado a ela passa a confiar na validade de certificados emitidos pela outra AC objeto da certificação cruzada. Considerando que o usuário confia na validade dos certificados que expede, quando ele se depara com um certificado cruzado emitido por sua AC de origem, passa a confiar na outra AC e, conseqüentemente, nos certificados por esta expedidos para seus próprios usuários finais.

Esse processo possibilita que um usuário filiado a uma determinada AC adquira confiança na validade de certificado de usuário vinculado à outra AC. O processo de certificação cruzada é um meio, como se disse, de produzir a extensão da cadeia de confiança necessária à funcionalidade em escala de uma ICP. Nesse caso, as AC´s se certificam umas às outras acima das estruturas de certificação originais.

Um outro meio de ampliar o raio de extensão da validade de certificados emitidos por uma AC é integrá-la a uma estrutura maior e mais complexa, regulada por uma unidade central, a AC – RAIZ.

A estrutura hierárquica original, formada pela AC e seus usuários, passa a fazer parte de um sistema maior, capitaneada por uma autoridade central de certificação, em que todas as demais autoridades certificadoras devem confiar. Em outras palavras, todos os "caminhos de certificação" devem passar em última análise por essa autoridade central, responsável pela garantia da cadeia de confiança e pela definição das práticas e políticas gerais de certificação. Nesse modelo, as autoridades certificadoras inferiores se certificam umas às outras dentro e abaixo da estrutura central.

A Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil foi instituída, pela já citada Medida Provisória 2.200/01, mediante adoção desse modelo de raiz única (árvore única). Deu forma legal a uma estrutura hierarquizada e centralizada – vertical –, com a previsão da existência de uma única AC-Raiz (árvore única), inicialmente regulada para operar com certificados de uso geral. A MP pretendeu instituir uma grande cadeia ou estrutura de Certificação Nacional.

Ao invés de incentivar a criação de pequenas e múltiplas estruturas de certificação, que atuariam de forma autônoma e cada qual com políticas e práticas de certificação

distintas, a Medida Provisória instituiu uma grande estrutura hierárquica com a previsão de uma Autoridade Certificadora Raiz.

A MP não proíbe qualquer organização ou empresa de criar sua própria ICP. Podem montar uma autoridade certificadora e, dependendo de requisitos técnicos e legais de operabilidade, podem requerer registro junto à ICP-Brasil. Se uma autoridade certificadora criada e mantida por uma instituição qualquer adéqua suas práticas de certificação aos regulamentos gerais da ICP-Brasil, pode vir a fazer parte de sua infra-estrutura, passando a ser mais um membro da cadeia nacional de confiança, e ampliando assim o poder de validade de seus certificados.

Uma autoridade certificadora credenciada na ICP-BR pode vender certificados que sirvam para verificar assinatura em qualquer tipo de documento ou transação, com valor probante em todo o território nacional. Em outras palavras, para que os certificados emitidos por uma autoridade certificadora adquiram, em nosso país, validade jurídica de uso geral (força probante contra terceiros), é preciso que ela esteja incorporada à ICP – Brasil.

O art. 1º. da MP 2.200-2 se resume a proclamar que 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 MP não definiu em detalhes a organização da ICP-Brasil, deixando essa tarefa para o regulamento, mas previu que "será composta por uma autoridade gestora de políticas e pela cadeia de autoridades certificadoras composta pela Autoridade

Certificadora Raiz - AC Raiz, pelas Autoridades Certificadoras - AC e pelas Autoridades de Registro – AR" (art. 2º)

6.1. Composição da ICP – Brasil -

A MP 2.200-2, embora sem definir a organização da ICP-Brasil, indicou antecipadamente os órgãos que a compõem (art. 2º), na seguinte ordem:

a) um Comitê Gestor, autoridade gestora das políticas de certificação;
b) a Autoridade Certificadora Raiz (AC-Raiz);.
c) as Autoridades Certificadoras (ACs); e
d) as autoridades de Registro (ARs)

6.2. Comitê Gestor -

O Comitê Gestor é o órgão que exerce a função de autoridade gestora das políticas de certificação da ICP-Brasil (art. 3º. da MP 2.200-2), vinculado à Casa Civil da Presidência da República e composto por cinco representantes da sociedade civil, integrantes de setores interessados, designados pelo Presidente da República, e um representante de cada um dos seguintes órgãos, indicados por seus titulares.

a) Ministério da Justiça
b) Ministério da Fazenda
c) Ministério do Desenvolvimento, Indústria e Comércio Exterior
d) Ministério do Planejamento, Orçamento e Gestão
e) Ministério da Ciência e Tecnologia

f) Casa Civil da Presidência da República, e

g) Gabinete de Segurança Institucional da Presidência da República

A coordenação do Comitê Gestor da ICP-Brasil é exercida pelo representante da Casa Civil da Presidência da República (par. 1º. do art. 3º.). Os representantes (cinco) da sociedade civil são designados pelo Presidente da República pelo período de dois anos, permitida a recondução. (par. 2º)

A Medida Provisória também definiu a competência desse Comitê Gestor (art. 4º) – estabelecendo que cabe a ele:

a) Implantar e coordenar o funcionamento da ICP – Brasil,

b) estabelecer a política, os critérios e as normas técnicas para o credenciamento das ACs das ARs e dos demais prestadores de serviço,

c) estabelecer as políticas de certificação e as regras operacionais da AC – Raiz,

d) homologar, auditar e fiscalizar a AC Raiz e os seus prestadores de serviço,

e) estabelecer diretrizes e normas técnicas para a formulação de políticas de certificados e regras operacionais das ACs e das ARs,

f) definir níveis de cadeia de certificação,

g) aprovar políticas de certificados, práticas de certificação e regras operacionais das AC s e das ARs,

h) credenciar e autorizar o funcionamento das ARs,

i) autorizar a AC – Raiz a emitir os certificados das ARs credenciadas,

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

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

Em que pese a previsão de todas essas atribuições, na prática o Comitê Gestor apenas atuará como órgão colegiado de cúpula da ICP-Brasil, definidor das políticas gerais de certificação.

A execução dessas políticas, bem como as atividades práticas de credenciamento, supervisão e auditoria das atividades dos prestadores de serviço de certificação (as AC´s e AR´s) são desempenhadas pelo ITI -Instituto Nacional de Tecnologia da Informação, já que o parágrafo único do art. 4º. da MP permite que as funções nele definidas sejam delegadas à AC – Raiz.

O próprio art. 5º. da MP, ao definir a função da AC-Raiz, a elege como autoridade "executora das políticas de certificados e normas técnicas operacionais aprovadas pelo Comitê Gestor".

6.3. Autoridades Certificadoras -

As Autoridades Certificadoras (AC´s) são as entidades componentes da cadeia de certificação responsáveis pela emissão de certificados digitais a usuários finais. Situam-se em nível inferior ao da AC-Raiz na cadeia de certificação, já que são credenciadas por esta última para emitir certificados digitais vinculando pares de chaves criptográficas ao respectivo titular (usuário final). A essas autoridades certificadoras (AC s), compete basicamente:-

a) emitir, expedir, distribuir, revogar e gerenciar certificados,

b) colocar à disposição dos usuários listas de certificados revogados e outras informações pertinentes,

c) manter registro de suas operações.

O aspecto principal de uma ICP é o da confiança, portanto, as Autoridades Certificadoras –AC s- são instituições que, antes de tudo, precisam gozar de confiança junto às artes envolvidas.

A Autoridade Certificadora –AC- (acrônimo: CA, do inglês *(Certification Authority),* é o terceiro confiável que emite o certificado. A –AC- tem a função de GARANTIR a associação de um portador

As AC´s não podem certificar nível diverso do imediatamente subseqüente ao seu, exceto nos casos de acordos de certificação lateral ou cruzada, previamente aprovado pelo Comitê Gestor d ICP – Brasil (art 9º da MP).

6.4. Autoridades de Registro -

As AR s (Autoridades de Registro) são entidades operacionalmente vinculadas a uma determinada AC. Em outras palavras, cada AC opera através de uma AR, para efeito de realizar a tarefa de identificação e cadastro dos usuários finais. Além de cadastrar e identificar usuários, as AR´s encaminham solicitações de certificados às ACs e devem manter registro de suas operações (art. 7º).

A Autoridade de Registro, ou AR, é talvez um dos mais elementos mais importantes de uma infraestrutura de chaves públicas, pois é ela o intermediário entre a Autoridade Certificadora e o cliente (aquele que pede o certificado). É a AR quem valida a identidade do cliente e se responsabiliza,perante a Autoridade Certificadora, pelo cumprimento da DPC – Declaração das Práticas de Certificação.

Qualquer pessoa, de direito público ou privado, desde que preenchendo os requisitos gerais da política de certificação da ICP - Brasil, pode requerer credenciamento com AC e AR (art. 8º) da MP.

6.5. Poderes de Fiscalização e Auditoria do ITI -

A Medida Provisória 2.200 de 24 de agosto de 2001, instituiu a Infraestrutura de Chaves Públicas Brasileira – ICP – Brasil, e transformou o Instituto Nacional de Tecnologia da Informação em autarquia. A sua função é manter uma estrutura de emissão de chaves públicas, baseando-se no princípio da terceira parte confiável, oferecendo uma mediação de credibilidade e confiança em transações entre partes que utilizam certificados digitais. Define técnicas, práticas e procedimentos a serem adotados pelas entidades a fim de estabelecer um modelo seguro e confiável.

Em razão da posição que ocupa na hierarquia da ICP-Brasil, como primeira autoridade da cadeia de certificação, sua função primordial não é a prestação de serviços de certificação para os usuários finais do sistema. Aliás, o parágrafo único do art. 5º. da MP 2.200-2 veda à AC-Raiz emitir certificados para o usuário final. Os certificados emitidos pela AC-Raiz têm como objetivo único identificar a própria AC Raiz ou as ACs de nível imediatamente subsequente ao seu.

Essa função certificadora, limitada às AC´s que se situam no segundo nível da cadeia de certificação, é desempenhada em conjunto com outra, que é a de executar atividades de fiscalização e auditoria de todas as demais entidades integrantes da ICP – Brasil.

Como executora das políticas de certificados e normas técnicas e operacionais aprovadas pelo Comitê-Gestor, a AC-Raiz realiza tarefa de fiscalização e auditoria das AC´s e AR´s prestadoras de serviços de certificação (art. 5º. da MP 2.200-2). Nessa tarefa de fiscalização, o ITI (que é a AC-Raiz da ICP-Brasil) pode inclusive aplicar sanções e penalidades, na forma da lei. (Art 14 da MP)

As auditorias que realiza têm o objetivo de verificar se todos os processos, procedimentos e atividades das AC's integrantes da ICP-Brasil (e suas AR's) estão em conformidade com as suas respectivas DPC, -Declaração de Práticas de Certificação- suas Políticas de Certificado, a Política de Segurança e as demais normas e procedimentos estabelecidos para a ICP –BRASIL.

As auditorias de conformidade verificam todos os aspectos relacionados com a emissão e o gerenciamento de certificados digitais, incluindo o controle dos processos de solicitação, identificação, autenticação, geração, publicação, distribuição, renovação e revogação de certificados.

Os tópicos cobertos por uma auditoria de conformidade incluem, dentre outros: política de segurança, segurança física, avaliação de tecnologia, administração dos serviços; investigação de pessoal, PC –Políticas de Certificação- e DPC utilizadas, contratos e considerações de sigilo. O Comitê Gestor tem baixado várias resoluções que detalham como deve ser exercida a atividade de fiscalização pelo ITI. Dentre

elas, merece destaque a Resolução n. 25, de 24 de outubro de 2003, que aprova procedimentos a serem obedecidos por este órgão.

Essa resolução regulamenta o art. 14 da Medida Provisória 2.200-2, estabelecendo que a atividade fiscalizadora do ITI tem por objetivo verificar a conformidade da atuação dos prestadores de serviços de certificação (AC's e AR's) com as Declarações de Práticas de Certificação (DPC's), Políticas de Certificado, Política de Segurança e as demais normas e procedimentos estabelecidos pela ICP-Brasil art 2º.

Portanto, o ITI, no exercício de sua atividade de fiscalização, desenvolve procedimentos voltados a verificar o cumprimento, pelas entidades credenciadas (prestadores de serviços de certificação e prestadores de serviços de suporte), das normas e regulamentos que regem a ICP – Brasil.

A citada Resolução prevê que o procedimento de fiscalização alcançará o exame de documentos, instalações técnicas e ambiente lógico do prestador de serviço de certificação, bem como seu próprio pessoal, podendo acarretar a aplicação de uma o mais penalidades. (art. 4º). Que vão de advertência ao descredenciamento.

O Projeto de Lei n. 7.316, de 2002, que dispõe sobre a prestação de serviços de certificação e define a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, e que irá substituir a MP 2.200 como "marco regulatório" dos serviços de certificação em nosso país – o projeto prevê a sua revogação -, atribui uma composição ainda mais heterogênea ao Comitê Gestor.

Não somente amplia para 16 o número de representantes da sociedade civil (integrantes de setores interessados) como prevê a participação de representantes

do Senado Federal, da Câmara dos Deputados, de tribunais superiores (um do STF, um do STJ, um do TST, um do TSE, e um do STM) e do Ministério Público Federal.

Capítulo 7. – Validade da Certificação e Aplicação nos Tribunais -

7.1. Validade Jurídica e Eficácia Probante -

Em virtude da revolução que o assunto certificado digital traz ao mundo jurídico, é comum encontrarmos pessoas discutindo os benefícios e as quebras de paradigmas que tal tecnologia nos traz. Independente do fórum onde o assunto é discutido, uma frase sempre é ouvida: a certificação digital veio imprimir “validade jurídica” aos documentos eletrônicos.

Documentos eletrônicos ou não, não têm validade jurídica, mas sim maior ou menor eficácia probante. Validade jurídica tem o negócio jurídico, conforme dispõe o artigo 104 do Código Civil, que diz: que a validade do negócio jurídico requer 1- agente capaz, 2- objeto lícito, possível determinado ou determinável. 3- forma prescrita ou não defesa em lei.

Existem situações nas quais a lei exige forma documental própria. É o caso, por exemplo, da venda e compra de imóveis, que deve ser feita por escritura pública. A regra, porém, é de não ser necessária forma especial para emissão de um documento e, mesmo quando a forma especial for exigida e não observada, é o negócio jurídico que deixa de ter validade, e não o documento que a espelha. O documento eletrônico ou não, deve servir para provar um fato.

Portanto o problema do documento, eletrônico ou não, insere-se no campo processual, diz respeito à sua eficácia probante.

A definição de Chiovenda, para documento é: documento, em sentido amplo, é: “toda representação material destinada a reproduzir determinada manifestação do pensamento, como uma voz fixada duradouramente” Assim extraímos duas conclusões básicas, conforme nos ensina Robson Machado:

a) O documento eletrônico, igualmente ao físico, se enquadra no conceito legal de documento, eis que pode representar um ato ou fato jurídico.
b) Sua plenitude depende da capacidade de ser mantido íntegro e não deteriorável, vês que sendo um suporte sujeito a adulterações imperceptíveis, caso não houvesse mecanismos apara garantir sua integridade poderia perder parte de sua confiabilidade.

Em se tratando de documento eletrônico, sua eficácia probante não deve ficar adstrita à existência, ou não, de certificação digital, mas sim da **assinatura digital**, já que, conforme demonstrado anteriormente, mediante processos de criptografia de chaves públicas, é ela quem assegura autenticidade e integridade ao documento eletrônico.

O certificado digital ingressa apenas no campo da distribuição de chaves públicas, sendo uma das formas, não exclusiva, de identificação de seus titulares. Portanto, o termo “certificado digital” deriva de uma abordagem comercial para uma tecnologia específica que já existe há décadas.

Na verdade, o termo mais importante a ser observado é “assinatura digital” a qual foi aceita pelo mundo jurídico devido à confiabilidade trazida pelos testes acadêmicos realizados durante décadas utilizando-se os conceitos da criptografia assimétrica.

Há algumas questões relevantes quando, apresentada uma prova documental eletrônica em juízo, alguém negar uma assinatura digital. A qualidade do software que gerará o par de chaves criptográficas. A guarda da chave privativa. A distribuição correta da chave pública (aqui entra a certificação digital, que, aliás, não é o único meio de provar a titularidade da chave pública). Em relações privadas, é possível prová-la até mesmo por meio de uma declaração por escrito de seu titular.

Essas questões serão relevantes quando, apresentada uma prova documental eletrônica em juízo, e alguém negar uma assinatura digital. É nesse contexto que a questão da eficácia probante do documento (e não sua validade jurídica) está inserida.

Tratando-se de documento materializado no papel, impugnar uma prova documental, basicamente representa negar a integridade do papel, ou negar a assinatura nele manuscrita.

No documento eletrônico também. Enquanto negar uma assinatura manuscrita significa basicamente negar tê-la lançado no papel, no caso de uma assinatura digital, a base é negar ter sido feito uso (intencional) da chave privativa, ou negar a titularidade do par de chaves.

Já que se está discutindo a eficácia jurídica ou não da assinatura digital, cabe aqui mais um parágrafo sobre o modelo de hierarquia seria mais conveniente utilizar. O da ICP-Brasil ou outras particulares nacionais ou estrangeiras. Basta imaginar o quão complexo seria o questionamento de uma assinatura digital efetuada em um contexto como o citado no parágrafo anterior. A quantidade de variáveis questionáveis ao se impugnar uma assinatura digital seria enorme.

Partindo da qualidade do software que gerou o par de chaves, da segurança da guarda daquele par de chaves, da segurança dos algoritmos utilizados, e, o pior,

cada novo negócio questionado poderia estar utilizando uma infraestrutura totalmente diferente da anterior, o que certamente multiplicaria a complexidade de todo o processo.

Portanto, utilizar uma infraestrutura de Chaves Públicas como o da ICP – Brasil, onde todo o contexto envolvido está largamente documentado e apoiado na legislação brasileira, significa de forma expressiva a utilização da tecnologia de assinaturas digitais, e em conseqüência, eventuais processos judiciais que a envolvam.

A utilização da infraestrutura da ICP – Brasil pode ser vista como uma declaração de que todos os procedimentos, desde a emissão até o uso de qualquer certificado digital emitido em sua hierarquia, adotam critérios técnicos preestabelecidos e apoiados na legislação vigente do país.

Dito isso, e sabendo-se que para o juiz, importa a verdade dos fatos e a capacidade do documento eletrônico de retratá-los, independente da infraestrutura utilizada, a adoção de uma infraestrutura institucional no país permite celeridade ao processo e escalabilidade na utilização da tecnologia na vida real. Em outras palavras, a utilização da ICP – Brasil, pode ser vista como um “selo de qualidade técnica” que atesta que os requisitos técnicos e procedimentos legais aceitos pelas leis brasileiras foram cumpridos com rigor. Esse rigor é a garantia de que tais requisitos são cumpridos por todos os procedimentos de fiscalização e auditoria pelo ITI, (Instituto Nacional de Tecnologia da Informação) acima descritos, como responsável pela manutenção da AC Raiz Brasileira e pela ICP Brasil.

7.2. Caminhos de Certificação -

A arquitetura de caminhos de certificados digitais utiliza cadeias de certificados para transferência de confiança, onde este caminho é formado por todos os certificados, iniciando pelo certificado da entidade final, passando por todas as ACs intermediárias até a AC-raiz.

O Caminho de Certificação é necessário para determinar a confiança ou não de um certificado. No momento de recebimento de um certificado, cabe ao sistema descobrir se ele deve ou não ser confiado. Isto é feito através do processamento do Caminho de Certificação, ou seja, a possibilidade de percorrer Toto o Caminho de Certificação, e validação do certificado, através de uma corrente de ligação entre ACs.

Antes de o sistema interpretar o certificado recebido como um certificado válido, ele monta todo o caminho de certificação e descobre se este possui algum certificado considerado “confiável” por ele. Além disso, o sistema também procurará uma brecha no Caminho de Certificação, ou seja, algum certificado que possua restrições ou que não poderá mais ser considerado válido.

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

7.3. Autoridade Certificadora AC-JUS.-

A Autoridade Certificadora do Sistema Justiça Federal (AC-Jus) teve sua origem através de uma decisão em conjunto do Superior Tribunal de Justiça, Conselho da Justiça Federal e Tribunais Regionais Federais, formalizada pela Resolução Conjunta Nº 01, de 20 de Dezembro de 2004, assinada pelo Ministro Presidente do STJ e do CJF, Edson Carvalho Vidigal.

A AC-Jus é uma das autoridades certificadora de nível intermediário na ICP-Brasil (AC-RAIZ), tendo como característica e função a definição das normas claras e transparentes a serem adotadas no âmbito do STJ, CJF e TRF's, não sendo emissora de certificados diretamente a seus titulares e sim através de Autoridades Certificadoras de nível imediatamente subseqüente ao seu. Sendo, portanto, uma Autoridade Certificadora normativa independente de outros poderes ou empresas.

O gerenciamento da AC-Jus fica a cargo do Comitê Gestor, composto pelo Presidente do STJ e CJF, Ministro Coordenador do CJF, Ministro Presidente da Comissão de Coordenação do STJ e pelos presidentes dos TRF's, com o apoio da Comissão Técnica.

Dentre as possibilidades de utilização dos certificados AC-Jus, podemos identificar o peticionamento eletrônico, a emissão de certidões negativas ou positivas e a migração gradativa dos documentos ("processo") em papel para o meio virtual, dando maior agilidade, transparência e economia, sem o comprometimento da segurança.

7.4. Assinatura Remota de Processos no TRF4.-

O Tribunal Regional Federal (TRF) da 4ª Região, em Porto Alegre, implantou a assinatura eletrônica remota de documentos. A inovação é um aprimoramento da Assinatura Eletrônica de Documentos, proposta pela vice-presidente da corte, desembargadora federal Marga Inge Barth Tessler, e lançada no ano 2005.

O projeto anterior foi desenvolvido em caráter experimental no gabinete da Vice-Presidência e depois adotado por outros desembargadores, substituindo com segurança a necessidade de os magistrados assinarem manualmente cada despacho.

Agora, em casos urgentes, mesmo estando longe do TRF, a vice-presidente pode receber eletronicamente a petição em seu notebook, acessar o sistema do tribunal, redigir a decisão e disponibilizá-la instantaneamente, com Certificação Digital garantindo a autenticidade. Após a fase de testes, ela utilizou o sistema remoto oficialmente pela primeira vez numa noite de domingo, quando despachou, em regime de plantão, um processo de caráter urgente.

O procedimento proporciona um serviço mais rápido, dispensando deslocamentos, pois não é preciso que a petição seja levada até a magistrada nem que ela vá até a sede do tribunal para assinar a decisão. “A assinatura remota é importante porque vai permitir que eu leia, escreva e assine despachos de qualquer parte de minha jurisdição”, comemorou Marga. “Poderei estar no Interior para inaugurar uma vara federal, por exemplo, receber uma petição por e-mail e já despachar.” Ela pretende usar o sistema até o final da sua gestão na Vice-Presidência, e depois seguir aproveitando a novidade quando voltar a atuar como julgadora em uma das turmas do TRF.

A inovação se tornou possível com a instalação do Sistema de Assinatura Eletrônica nos notebooks pessoais dos desembargadores. Os computadores portáteis estão

equipados com um dispositivo de acesso à Internet por conexão sem fio. Assim, mesmo que estejam em um local sem cabeamento de internet disponível, os magistrados podem entrar na rede de informática do TRF como se estivessem no prédio do tribunal.

O sistema faz uma checagem imediata, verificando a autenticidade das informações em um banco de dados oficial e validando a assinatura do magistrado quase simultaneamente, de forma segura.

O TRF4 conta hoje com um moderno sistema de processo eletrônico, dando ensejo à implantação em todo o país, a partir de 1º de agosto de 2010, todos os processos que estejam tramitando em meio físico na Justiça Federal da 4ª Região e que forem remetidos ao Tribunal Regional Federal da 4ª Região – TRF4 em razão de recurso em sentido estrito, apelação ou reexame necessário cível ou criminal, serão convertidos para o meio eletrônico passando a tramitar exclusivamente no sistema de processo eletrônico da Justiça Federal da 4ª Região - e-Proc. Do mesmo modo, a partir de 1º de setembro, os processos em razão de apelação ou reexame necessário remetidos pelas comarcas (competência delegada) serão convertidos para o meio eletrônico. Para atuar no processo eletrônico o advogado deve fazer seu cadastrado no sistema e-proc. A mudança de suporte de processos do meio físico para o processo eletrônico, no âmbito da Justiça Federal da 4ª Região, foi regulamentada pela Resolução nº 49/2010.

7.5. Implantação no TRF1 da Certificação Digital com Biometria -

O presidente do Tribunal Regional Federal da 1ª Região assinou em 22/02/2006, o primeiro despacho virtual com a utilização da Certificação Digital com biometria (impressão digital). Todos os documentos da Presidência passarão a ser assinados por meio de um smart card (cartão inteligente), que contém as informações pessoais do magistrado, inclusive a assinatura manuscrita e a impressão digital o que garante a presença do autor, recurso pioneiramente utilizado pelo tribunal.

No decorrer daquele ano e até hoje, tal funcionalidade foi disponibilizada para os demais gabinetes dos desembargadores e juízes federais, para as Varas dos JEFs e para as Turmas Recursais.

A solução de Certificação Digital do TRF vem sendo desenvolvida desde 2003 como um módulo do sistema de Execução Fiscal Virtual, podendo integrar diversos outros sistemas da Justiça Federal da 1ª Região. Sem a biometria, ou seja, com o uso de senhas tradicionais, não é possível garantir que o autor esteja presente no momento da assinatura.

Com a biometria, essa garantia é total. Somente o usuário que possui a digital cadastrada no cartão terá acesso ao seu conteúdo. Além da segurança, o sistema garantirá a legalidade e autenticidade dos processos virtuais, uma vez que os certificados utilizados são ICP-Brasil, pré-requisito para garantir a legalidade.

7.6. Evolução Digital no TRF da 3ª Região -

7.6.1 Sistema de Execução Fiscal Virtual Justiça Federal da 3ª Região -

O TRF 3ª Região não está estagnado em termos totais de tecnologia, prova disso é o arranque que foi dado em termos de revolução digital com o processamento de Execução Fiscal Virtual – 3ª Região". Solução esta que é baseada na utilização das tecnologias GED, Workflow, Criptografia, Biometria e Smart Card e tem como objetivo, agilizar o andamento de processos de execução fiscal, do Tribunal Regional Federal da 3a. Região, que atende aos estados de São Paulo e Mato Grosso do Sul, garantindo alto poder de armazenamento, segurança, performance/agilidade, bem como um alto índice de produtividade ao Órgão.

Em função do alto número de processos aguardando ajuizamento, bem como do crescente montante de novos processos, advindos das entidades exeqüentes (INSS, PGFN, etc), a Solução é dotada de uma poderosa infra-estrutura de servidores, bem como de dispositivos de alta capacidade de armazenamento, tendo como premissa para o TRF, a revisão desta infra-estrutura a cada 6 meses, caso seja identificada a necessidade, em função deste crescimento, bem como da expansão vertical e horizontal da solução prevista.

A Camada de segurança prevista para a solução foi amplamente discutida entre a equipe técnica das empresas contratadas para implementação da solução, às empresas de tecnologia do governo federal que dão apoio e subsidio tecnológico aos Órgãos exequentes que são o DATAPREV (INSS) e o SERPRO(PGFN) e envolve criptografia de arquivos e dados, assinatura e Certificação Digital, biometria e Smart Card, para oferecer um alto índice de segurança as transações e aos arquivos que estarão sendo tratados pela mesma.

Para garantir a integridade dos dados junto ao protocolo TCP/IP, serão utilizados dois algoritmos e uma camada do protocolo HTTP. São eles, 3DES, Sha1 e o protocolo SSL. O algoritmo 3DES será responsável pela encriptação de dados transportados pelo TCP/IP. O protocolo SSL proverá um canal seguro de comunicação entre aplicações onde sejam garantidas a privacidade e integridade dos dados bem como a autenticação dos participantes.

Todo o controle de acesso da aplicação será baseado em informações armazenadas no cartão SmartCard, principalmente os itens que correspondem a Certificação Digital e minúcia biométrica.

Se a minúcia biométrica apresentada pelo usuário for igual a minúcia armazenada no cartão, então, o componente de biometria local fará uma chamada a um segundo componente local de PKI,(public key infrastructure) este componente solicitará então um dado do certificado digital ex: (CPF ou RG) que por sua vez será assinado e criptografado pela chave publica do próprio certificado digital existente no cartão. Esses dados serão passados para um componente de negócios que trafegará os

dados até aplicação, a aplicação por sua vez verificará se a informação está integra e a confrontará com o banco de dados, uma vez que todos os dados estejam OK , então o componente de negócio da aplicação carregará o perfil de Trabalho do usuário. Caso a minúcia biométrica apresentada pelo usuário seja diferente da minúcia armazenada no cartão a aplicação não permitirá o acesso do usuário ao sistema.

7.6.2. Gerenciamento Eletrônico de Processos com a Certificação Digital -

O TRF3, também conta com um sistema híbrido de processamento de feitos (processos). Este sistema híbrido foi denominado GEDPRO –Gestão Eletrônica de Processos. Tal sistema é em palavras mais simples, consiste em uma tramitação processual física existente para uma tramitação gradualmente virtual. Os processos físicos continuam a existir até o seu julgamento e extinção. Porém, desde a implantação do sistema, todo o andamento processual deixou de receber os encartes corriqueiros de papel.

Esse sistema facilitou também o trabalho dos magistrados, pois separavam uma parte do seu tempo para assinar manualmente centenas de documentos processuais para levarem a julgamento. Agora todo o trabalho de processamento feito pelos funcionários que compõem o gabinete do desembargador, são reunidos em blocos digitais, que por sua vez reúnem, centenas de andamentos processuais. Tais blocos são disponibilizados seguramente pelos funcionários através do sistema ao desembargador, que com o uso de sua assinatura digital, por intermédio de smartcard, assina a documentação de forma rápida e segura, otimizando sua função de julgador.

A meta do TRF3 na utilização da Gestão Eletrônica de documentos é eliminar completamente o uso do papel, produzindo apenas documentos processuais eletrônicos, acessíveis via internet a todos os advogados e partes interessadas. Tal procedimento teve início em junho de 2008, no Gabinete do Desembargador Federal Jediael Galvão, onde foram proferidas as primeiras decisões judiciais em formato

eletrônico, com a segurança da tecnologia da certificação digital e nos termos da lei nº11. 419/2006.

7.7. Prática de Atos Mandatórios Extra Judiciais por Certificação Digital

Numa comparação feita no TRF 4ª Região, depois da implantação do Processo Eletrônico, mostrou que, enquanto um processo em vias normais de papel levou mais de 600 dias para ser resolvido, um caso semelhante conduzido digitalmente foi solucionado em 52 dias.

A Garantia da Certificação Eletrônica no Mundo Virtual também pode ser apontada em vários acordos em que o recém criado CNJ – Conselho Nacional de Justiça, firmou com a Receita Federal e Banco Central, Arisp -Ofício Eletrônico-, onde virtualmente o Juiz, através da certificação digital autentica-se e executa atos mandatórios, tais como:

A PENHORA ON-LINE, uma possibilidade criada pela Lei nº 11.382 de dezembro 2006, da constrição on-line de imóveis e determina a prioridade do uso da internet para o bloqueio de bens em ações judiciais. O Conselho Nacional de Justiça –CNJ- em abril de 2009 discutiu a adoção do sistema em reunião com corregedores de justiça. Pensa-se fazer a penhora de bens imóveis e veículos seguindo o exemplo da penhora on-line das contas bancárias –Bacen-Jud.

BACEN-JUD - Também conhecido como "penhora *on line*", trata-se de sistema informático desenvolvido pelo Banco Central que permite aos juízes solicitar informações sobre movimentação dos clientes das instituições financeiras e determinar o bloqueio de contas-correntes ou qualquer conta de investimento. O sistema está disponível a todos os ramos do Poder Judiciário, mediante convênio assinado entre o Banco Central e os tribunais superiores, ao qual aderiram os tribunais regionais e estaduais

O INFOJUD, que permite ao Juiz, por meio de certificação digital, se autenticar no site da Receita Federal e fazer consultas nas declarações de Imposto de renda de pessoas físicas e jurídicas. Antes da digitalização da justiça, quando se tratava de acolher pedido de quebra de sigilo fiscal, encaminhado pelo Ministério Público, os juízes tinham que enviar ofício à Receita Federal pelo correio.

Os juízes tinham que explicar no texto, do se tratava o processo, comunicar sua decisão e definir detalhadamente os dados que precisavam. Ao prestar esclarecimentos solicitados, as autoridades fazendárias eram obrigadas a preparar outro ofício, também encaminhado pelo correio. Essa tramitação em média, para cada pedido de informação fiscal demorava cerca de 60 dias para ser concluída. Os únicos a lucrarem com tal morosidade eram os acusados.

A Receita Federal, por exemplo, tinha que manter um setor com cerca de 100 servidores públicos, encarregados somente em responder ofícios judiciais. Isso só em São Paulo. Claro que essa morosidade só interessava aos acusados de sonegação e outros, que ganhavam tempo para reverter a decisão de quebra de sigilo fiscal.

Outra modalidade também com o uso de certificação digital foi o RENAJUD, que é um sistema on-line de Restrição Judicial de Veículos, onde após certificado e autenticado nas bases de dados do DETRAN. Permite ao juiz consultas em tempo real com os dados do RENAVAN, dos proprietários de veículos com dívidas a executar, e inserir restrições judiciais de transferência, licenciamento e circulação, além de registrar penhora sobre os veículos.

No acesso via internet ao site do Tribunal Regional da 3ª Região, pode ser constatada outra situação de garantia da certificação digital no mundo virtual, quando se lê o Diário Eletrônico, onde são publicados todos os atos judiciais e administrativos de 1ª e 2ª instâncias, com a publicação de votos, relatórios dos desembargadores e resultados de perícias e decisões de juízes. Tudo afixado no portal eletrônico e sempre confirmado pela assinatura digital de um funcionário público responsável como

um carimbo no canto superior esquerdo do início do texto, se responsabilizado pela veracidade e garantindo na íntegra o documento.

Capítulo 8. – Entrevistas -.

Entrevistas com Funcionários Públicos que Utilizam a Assinatura Digital.

Este capítulo será constituído de duas entrevistas com diretores de Subsecretarias, que fazem uso diário do recurso da assinatura digital. A primeira entrevista versa a respeito da função que assinatura digital no trâmite processual. A segunda é com um técnico responsável pela aplicação, divulgação e manutenção dessa tecnologia. Ambas no âmbito do Tribunal Regional Federal da 3ª Região.

Entrevista com funcionário responsável por remeter processos ao STJ.

Como foi para você, dispor o recurso tecnológico da assinatura digital?

Confesso que foi horrível, (risos) eu estava acostumado ao meu trabalho diário com os processos físicos, onde eu participava em diversas etapas que são realizadas por outros cinco diretores de divisão e seus respectivos funcionários. Minha rotina era verificar se estavam prontos para serem remetidos aos STJ –Superior Tribunal de Justiça, todos os processos que recebia com recurso especial. Minhas responsabilidades estão muito próximas à do desembargador responsável pela admissão/aceitação ou inadmissão/rejeição do recurso.

O Superior Tribunal de Justiça começou a exigir que os processos físicos não fossem mais para Brasília em sua forma original, isto é, em papel. Então uma equipe da tecnologia da informação do STJ, visitou o TRF3 e demonstrou a utilização de um programa que manda os processos eletronicamente para serem apreciados naquele Tribunal.

Executar suas rotinas com a tecnologia da certificação melhorou alguma coisa?

Pois é, o meu dia seguinte é que foi horrível, pois tive que aprender quase tudo de novo. Antes, como eu ia dizendo, eu só fazia as verificações técnicas do recurso e mandava pelas vias normais de malote e correio para Brasília. No dia seguinte eu tinha que me acostumar a mexer com o programa de envio, e não era só isso, pois tive que treinar todas as divisões que trabalham em sincronismo. Todos tiveram que reaprender a trabalhar. Não era apenas eu pegar um documento e enviar por email, por exemplo.

É claro que tudo não aconteceu no dia seguinte à visita do STJ, pois tivemos que passar por todos os processos de licitação e contratação de uma central de cópias e escalação de funcionários treinados para coordenar e fiscalizar o serviço terceirizado.

Então, o processo físico é totalmente digitalizado, e indexado –criação de um índice que mostra as peças processuais ali contidas-. Depois é minuciosamente comparado com o processo físico. É uma espécie de “cara–crachá”, brinca. O funcionário que faz isso assina digitalmente o processo e me manda via intranet para a caixa postal da subsecretaria.

Eu que sou o responsável pelo envio, confiro as ações anteriormente em papel. Entro no programa de envio, que nos foi disponibilizado pelo STJ, faço uma série de procedimentos, cujo principal é minha autenticação com meu cartão inserido no micro computador que utilizo, e em seguida busco pelos processos salvos em uma área determinada, que já assinei digitalmente, também com o uso do smartcard. Faço a inserção deles no programa e executo o procedimento de enviar, ele vai novamente exigir minha identificação digital, eu confirmo e o processo de envio começa.

Mas parece bem fácil não?

Fácil agora assim falando, mas no início isso foi um martírio, pois o programa de envio teve que passar por uma série de ajustes e o usuário (eu) também teve que ser ajustado. É claro que facilitou bastante, mas a tecnologia de informação aqui do TRF teve que fazer toda a parte de certificação digital dos funcionários, teve que mostrar a todos o uso correto do smartcard, o cuidado que tínhamos que tomar com nossas senhas pessoais e com nosso cartão.

A assinatura digital fica fixada, como um carimbo, nos autos que enviamos e quando retornam também são assinados digitalmente pelos responsáveis do STJ.

Essa tecnologia facilitou o seu trabalho ou atrapalhou?

Facilitou bastante, mas isso a gente só vê depois, pois no início é horrível, como toda mudança de paradigma, sempre é assustador. Depois nos acostumamos e verificamos que uma série de procedimentos que antes eram burocráticos e trabalhosos, hoje são automáticos e virtuais. Eu não preciso mais colocar trezentos documentos sobre a mesa do desembargador para serem assinados. Eu apenas comunico por e-mail que já estão disponíveis para assinatura eletrônica. Ele procura pelos documentos, verifica se estão corretos, e em caso de dúvida ele me chama para discutir o assunto, mas na maioria das vezes ele apenas confere e assina também digitalmente os lotes de processos em grau de recurso especial e pronto.

E você confia nisso que você está fazendo?

Sim confio. Admito que no início eu fiquei com o pé atrás. Mas depois com a visita do pessoal do STJ e posteriormente conversando com o desembargador, não tenho motivos para desconfiar.

A assinaturas citadas nas respostas, são feitas por intermédio de cartão smartcard com certificação raiz da ICP- Brasil, e com as Autoridades certificadoras AC-JUS e AC – Caixa Jus, com certificados tipo A3 na versão V3 com chave pública RSA de 1.024 bits.

Entrevista a seguir, é com um técnico da área de TI, responsável pelo suporte, entre outras a essa tecnologia da certificação digital.

Foi puramente profissional, ou houve alguma curiosidade mais de cunho pessoal por essa tecnologia que envolve a certificação digital?

O início dos trabalhos aqui no TRF, foi pó impulso profissional quando fui requisitado para acompanhar e suportar a implantação. Desde os tempos da graduação –há quase vinte anos- eu já acompanhava curioso a certificação digital, que já era apontado na época, como o futuro da comunicação segura e tudo o mais, mas é que eu gosto de matemática, e como tudo isso envolvia matemática e técnicas de algoritmos e tal. Depois aqui no TRF trabalhando com a segurança da informação foi um pulo que me requisitassem e aqui estou eu em meio às requisições diárias.

Antes da criação da ICP – Brasil, havia algum tipo de certificação ou demanda para seu uso aqui no TRF?

Antes dessas leis editadas pelo congresso alterando o código de processo e tal, e essas medidas tomadas pelo CJF, _conselho da Justiça Federal, não se demandava nada nesse sentido, mas tão logo incentivado, o TRF3, criou um sistema de assinatura digital, mas sem uso de chave pública, era o SRDD, -Sistema de Registro de Documentos Digitais, desenvolvido no começo de 2001. Ele não usava um serviço de assinatura baseado em chaves públicas. Limitava-se a registrar o documento emitido, gerando um “hash” dele e apondo no texto uma reprodução gráfica da assinatura do emitente, bem como um código para a verificação nesse sistema.

Evidentemente, tal tecnologia limitava a validade da assinatura no escopo do TRF da 3ª Região, Por ser proprietário (ao contrário de uma ICP) e por não possuir reconhecimento formal ou validade jurídica, ao contrário da ICP – Brasil, que possui esses atributos por força do diploma legal que a instituiu. Hoje já possuímos um “assinador” de documentos que incorpora o uso de chave pública – ICP – Brasil.

Com o constante crescimento dos negócios via internet e todas as etapas que envolvem a negociação, você vê como benéfica ou irrelevante a utilização dessa tecnologia no comércio eletrônico como garantidor da responsabilidade entre os contratantes?

Eu diria que é absolutamente necessária a utilização dessa tecnologia para conferir a integridade e autenticidade dos documentos digitais. E indo mais longe, acho também que é absolutamente benéfica a sua utilização, como um sistema em que um terceiro (uma AC da ICP – Brasil), dá a confiabilidade ao processo de assinatura, como uma

testemunha neutra da validade dos documentos. E devido ao princípio da irretratabilidade da assinatura digital, está assegurada a responsabilidade entre os contratantes.

Com o início da virtualização processual brasileira nos tribunais superiores e a OAB, listada como uma das certificadoras, seria arriscado prever uma virtualização completa nos próximos dez anos?

Nada arriscado, ao contrário, diversos fatores somam-se para que tal aconteça antes desses dez anos, começando por: Os custos da infraestrutura que tendem a cair. A impossibilidade da prestação jurisdicional com os métodos tradicionais, isto é, processo em papel que é muito lenta, onerosa e sujeita a diversos riscos relacionados com a preservação do substrato físico, (por exemplo: incêndios, enchentes e outros). A ubiguidade dos computadores, baratos e potentes, como meios para a produção, o armazenamento e a disseminação de documentos digitais.

O anonimato sempre foi uma marca do mundo virtual, até mesmo para se cometer ilícitos, essa tecnologia poderia descaracterizar a internet do futuro?

A internet é um reflexo da sociedade humana e, como tal, não deixa de ter seus problemas, inclusive servir de instrumento para a prática de crimes. Porém, não sou dos que acreditam na sua descaracterização ou mesmo na sua destruição. É preciso que as pessoas ajam com responsabilidade e com prudência. É preciso também que os organismos de Estado implementem nela seus serviços, dando-lhes acessibilidade e transparência; e, é claro, que esses organismos também se preparem de forma adequada para a prevenção e repressão dos crimes de internet, inclusive com acordos internacionais e com leis modernas.

Será que se pode imaginar uma rede social com participantes autenticados?

Sim, se ela implementar tecnologias adequadas de gestão de identidade e de acesso (por exemplo os Certificados Digitais ICP – Brasil) que poderiam servir como credenciais de autenticação.

Eu entendi, mas a pergunta seria mais no sentido dos integrantes das redes sociais, se eles aceitariam se credenciar para poderem continuar na rede e.... fui interrompido.

Desculpe mas não sou desses que perdem tempo em entrar na rede para ficar trocando fofocas, figurinhas, conversinhas e dizendo coisas banais sobre qualquer pessoal ou coisa igualmente banal ou muito séria. Isso é perda de tempo. Isso é coisa de gente muito carente reprimida que acha que a sociedade cabe dentro do computador de casa. Acho que ponto de vista é coisa séria e o que se escreve sobre seu ponto de vista é muito mais sério ainda. Acho que se alguém quer dizer qualquer coisa sobre uma pessoa ou organização, tem que ser autêntica. Não precisa sair por aí publicando seu CPF e RG e endereço, não é isso. Já vivemos numa democracia e temos direitos, obrigações e instituições que garantem isso. Ela tem que saber que se qualquer pessoa ou entidade que se sinta ofendida com suas declarações e, que se isso constituir crime ou ofensa, pode facilmente entrar com uma ação e o responsável pela autenticação, qualquer que seja a rede social, terá que fornecer os dados do usuário para que a pessoa responda na forma da lei.

Conclusão:-

Mediante todo o exposto, acredita-se ter mostrado que a tecnologia da Certificação Digital, pode e deve ser usada como garantia no interior do mundo on-line, pois este já permeia o cotidiano da maioria dos cidadãos nas suas vidas off-line. Hoje não se pode negar que as pessoas na sua grande maioria são influenciadas por um mercado de produtos que chega até elas forçosamente através de algum artifício tecnológico.

A inserção do computador na vida das pessoas, como foi parte da preocupação inicial deste trabalho, foi para chamar a atenção de que está em curso uma mudança de comportamento abrangente e silenciosa, que começa com o uso de uma máquina, que além de editar textos, fazer cálculos e guardar informações, também é um passaporte para um ambiente permeado de mídias sociais que de alguma maneira influencia as regras de convívio humano.

Historicamente podemos destacar momentos de grandes transformações sociais, como: guerras, situações epidemiológicas, regimes autoritários etc., que as causas nunca estiveram acima daquilo que chamamos de egoísmo humano, e são raríssimas as mudanças de comportamentos sociais causados por intervenções que de alguma maneira visasse o bem comum.

Desde sua criação, a internet, passa por momentos interessantes. Da necessidade de velocidade na comunicação e o compartilhamento de informações, como simples troca de um inocente correio eletrônico, evoluiu, em forma de protesto contra o abuso da indústria fonográfica e em seguida para o estímulo à pirataria, onde se adquire gratuitamente, produtos que custaram o esforço de seus autores. Entretanto, serve também para propagação de conteúdo empreendedor, onde se compra, vende troca produtos e informações.

O mercado é feroz. A virtualização de comportamentos e procedimentos têm que seguir caminhos que de alguma maneira proteja e mantenha as partes envolvidas

muito próximas da segurança da vida real. O comércio eletrônico como foi demonstrado já faz largo uso da certificação digital, mas pode evoluir ainda mais.

É justamente nessa mistura de situações e vivências heterogêneas que este trabalho procura mostrar o uso seguro de uma ferramenta, cuja finalidade é assegurar a garantia da responsabilidade que os envolvidos têm que assumir na prática de seus atos dentro do mundo virtual.

O foco da discussão aqui apresentada esteve bastante voltada aos poderes públicos, pois deles emanam normas de convívio e uso dessa tecnologia. O poder judiciário que tratou-se com muito mais amplidão é um dos poderes públicos que faz, ainda que incipiente, o uso da certificação digital, e já transforma de maneira positiva o cotidiano dos cidadãos, que podem ver um andamento processual de onde quer que estejam.

Porém, como já destacado acima, ainda é pouco informatizado o trâmite processual, mediante o clamor popular para a celeridade no judiciário. As pilhas de papeis que entulham e perturbam os fóruns brasileiros precisam acabar. O avanço tecnológico precisa ficar a favor dos cidadãos comuns, que têm suas vidas emperradas por uma decisão que nunca chega. Mas isso é apenas um reflexo dos altos prejuízos que a morosidade judiciária causa na economia nacional.

O registro das experiências acumuladas nos últimos anos no que tange ao comércio eletrônico, tem muito a oferecer como base para a evolução tecnológica no setor público, incentivando o governo federal, para que este não perca o rumo no aproveitamento em seu favor do conhecimento científico presente.

É claro que não cabe aqui ficar só discutindo as mazelas dos poderes públicos, mas também o muito que se tem feito até então. Há ainda carência na legislação no que tange ao regramento do uso de novas tecnologias voltadas ao processamento jurídico dentro dos tribunais, e também para que se consiga um ambiente eletrônico seguro.

A Certificação Digital, mostrada em destaque, surge como ferramenta tecnológica de última geração na transmissão segura de dados por meios eletrônicos, assim como todo o arcabouço de normas e procedimentos representados pelas Autoridades Certificadoras, que se somados, tornam o judiciário mais eficaz, garantindo transparência e eficiência no processo eletrônico.

Fazendo questão de descrever as minúcias, este trabalho procurou mostrar a importância da tecnologia abarcada pela Certificação Digital, que só tem a colaborar na atual crise do judiciário, haja vista, os casos de sucesso apontados, tais como o TRF da 4ª Região em Porto Alegre, em que o desembargador recebe eletronicamente uma petição em seu computador em qualquer lugar que se encontre e, por conseguinte, redige seu voto ou relatório e retransmite também eletronicamente garantido pela Certificação Digital.

Os avanços tecnológicos utilizados de forma responsável e segura, podem difundir os sucessos e, certamente conduzirão para a solução de problemas que demandam tempo e geram desperdício de dinheiro público. Faz-se necessário o desenvolvimento de um ambiente tecnológico virtual, cada vez mais seguro, onde todos os setores sociais sintam-se beneficiados com a Certificação Digital garantindo a firmeza dos pilares que sustentam o processo eletrônico confiável.

Referências Bibliográficas

BASSO, Maristela. (2000) Prudência no comércio eletrônico. em: Revista Jus Navigandi ano 5 nº 43 Julho de 2000

BRASIL, Ângela Bittencourt. (2000) Assinatura digital não é assinatura formal. Disponível em: *Revista Jus Navigand, ano 5 nº 40 mar 2000*

COLTO, Sergio Pereira em Decifrando a Fortaleza Digital –São Paulo – Universo dos Livros 2001

CARDOSO, Antonio Pessoa. O Processo nos Autos. em O processo Sem Autos- *Curitiba - Editora Juruá, 2002* e http://www.justicasempapel.com.br

CNJ – Conselho Nacional de Justiça – em http://www.cnj.gov.br

Folha – Jornal Folha de São Paulo. Editorial de 28 de fevereiro de 2011 e 19 de maio de 2010 pag A04 -Pesquisa em Acervo Digital 40 anos

DINIZ, Davi Monteiro – em Documentos Eletrônicos Assinaturas Digitais São Paulo LTR- 1999

ITI – Instituto Nacional de Tecnologia da Informação – em http://www.iti.gov.br

MACHADO, Robson Carvalho – em Certificação Digital – ICP-Brasil –os caminhos do documento eletrônico no Brasil- Niterói, RJ- Impetus – 2010.

MONTEIRO, Emiliano Soares e Mignone, Maria Eloisa – em Certificados Digitais – Conceitos e Práticas – Rio de Janeiro – Brasport- 2007

Theodoro Junior, Humberto – em Curso de Direito Processual Civil - 36 Ed. Vol 1 – Rio de Janeiro 2001

Valor - Jornal Valor Econômico de 23/02/2011 – www.valor.com.br

Veja – Revista Veja em Acervo Digital 1º de março 2006-Pg 90-92- www.veja.com.br

Wikipédia : HTTP://wikipedia.com