UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
DEPARTAMENTO ACADÊMICO DE ELETRÔNICA
CURSO DE ESPECIALIZACÃO EM CONFIGURAÇÃO E GERENCIAMENTO DE SERVIDORES E EQUIPAMENTOS DE REDES

AIRTON RUBERVAL CASAGRANDE

CERTIFICAÇÃO DIGITAL

MONOGRAFIA

CURITIBA
2011

AIRTON RUBERVAL CASAGRANDE

CERTIFICAÇÃO DIGITAL

Monografia apresentada como requisito parcial para obtenção do grau de especialista em Configuração e Gerenciamento de Servidores e Equipamentos de Redes, do Departamento Acadêmico de Eletrônica da Universidade Tecnológica Federal do Paraná
Orientador: Prof. Dr. Kleber Kendy Horikawa Nabas

CURITIBA
2011

Dedico este trabalho a
Dilce Casagrande
minha querida mãe

AGRADECIMENTOS

Agradeço a todos os professores pela dedicação e profissionalismo.

Em especial, ao meu orientador, Professor Kleber.

RESUMO

Casagrande, Airton Ruberval. **Avaliação da confiabilidade da Certificação Digital**. 2011. 31 f. Monografia (Especialização em Configuração e Gerenciamento de Servidores e Equipamentos de Redes). Universidade Tecnológica Federal do Paraná. Curitiba, 2011.

Este estudo avalia a perspectiva de aceitação e popularização do instituto da Certificação Digital a partir de sua confiabilidade junto à sociedade brasileira. Partindo de três aspectos fundamentais. Aspecto jurídico, hierárquico-administrativo e tecnológico.

Palavras-chave: ICP-Brasil. Certificação Digital. Assinatura Digital, Certificado Digital.

SIGLAS

ABNT - Associação Brasileira de Normas Técnicas

AC - Autoridade Certificadora

AC-Raiz - Autoridade Certificadora Raiz

ADE-ICP - Adendo da Infra-estrutura de Chaves públicas

AR - Autoridade de Registro

CCD - Centro de Certificação Digital

CG - Comitê Gestor da ICP-Brasil

CFTV- Sistema de Circuito Fechado de Televisão

CNH - Carteira Nacional de Habilitação

DOC-ICP - Documento da Infra-estrutura de Chaves públicas

EEPROM-Electrically-Erasable Programmable Read-Only Memory

ICP- Infra-estrutura de Chaves públicas

ICP-Brasil - Infra-estrutura de Chaves públicas Brasileira

ITI- Instituto de Tecnologia da Informação

KF - Chave de Fabricação

KP - chave de Personalização

MCT - Manual de Conduta Técnica

MP - Medida Provisória

NBR – Norma Brasileira

PCN – Plano de Continuidade do Negócio

PSS- Prestador de Serviços de Suporte

PIN - Personal Identification Number

PKI - Infra-estrutura de Chaves públicas

RAM – Memória Randômica

ROM – Memória Somente de Leitura

RSA - Rivest, Shamir e Adleman (modalidade de criptografia assimétrica)

SPC - Serviço de Proteção ao Crédito

LISTA DE FIGURAS

SUMÁRIO

1. INTRODUÇÃO

No Brasil, a primeira experiência de registro civil da população ocorreu em 1814, com o objetivo de levantar dados necrológicos mensais de óbitos ocorridos para apurar as enfermidades mais freqüentes na capital do país, então o Rio de Janeiro.

O Registro Civil de Pessoas Naturais teve início em 1850. Dois anos depois foi criado o Primeiro Regulamento de Registro Civil. Após a Proclamação da República, com a criação do Registro Civil de Identificação e dos cartórios, tem início a emissão das primeiras cédulas de identidade[1].

A primeira Carteira de Identidade foi criada em 1907 e o Sr. Edgard Costa foi o portador da Carteira de numero 1. Posteriormente passou aos Estados a responsabilidade pela emissão e pelos bancos de dados civis. No entanto, o documento somente obteve reconhecimento legal a nível nacional quase um século depois, em dezembro de 1983, quando padronizaram-se os dados impressos no documento[2].

É inegável que a criação dos Registros Civis, e posteriormente das carteira de identidade representaram um grande avanço. Mas novos desafios se apresentam.

Os níveis de interação proporcionados pelas novas tecnologias vem abrindo novos campos de oportunidades. Revolucionando as relações pessoais, sociais, comerciais, etc. As opções parecem infindáveis. Algumas barreiras, no entanto, tem impedido ou dificultado esses avanços. Dentre elas, as crescentes relações que dependem da Internet. Um meio que oferece muitos riscos e carece de confidencialidade.

Na busca por soluções, novas tecnologias tem sido empregadas. A Certificação Digital se apresenta como uma das alternativa viáveis. Em 2001, com a edição da Medida Provisória 2.200, um passo importante foi dado pelo Brasil nessa direção, com a regulamentação da Infra-estrutura de chaves públicas e reconhecimento de documentos e assinaturas digitais. Em 1997 foi instituído o número único de Registro de Identidade Civil(RIC) que traz um chip integrado, podendo ser utilizado como identidade digital por qualquer brasileiro.

1 (Disponível em:<http://www.arpensp.org.br/principal/index.cfm?pagina_id=177>Acesso em: 12/11/2011)

2 (disponível em:<http://www.stf.jus.br/portal/ministro/verMinistro.asp?período=stf&id=177>Acesso em: 12/11/2011)

1.1 TEMA

O tema trata principalmente da quebra de paradigma quanto aos meios historicamente utilizados pela opção à Certificação Digital como forma de confirmar a autenticidade de documentos eletrônicos, a identidade de seus emitentes e segurança quanto ao seu sigilo durante o tráfego via conexões remotas. A confirmação da eficiência dos aspectos que dão sustentação à Certificação Digital como base para sua aceitação e uso corrente pela sociedade em geral.

1.1.1 Delimitação do Tema

A proposta deste estudo limita-se à apreciação da eficiência dos aspectos técnicos, jurídicos e estruturais que efetivamente dão sustentação ao instrumento da Certificação Digital.

1.2 PROBLEMA E PREMISSAS

Todo processo inovador traz consigo algum risco. O surgimento de algo novo tira naturalmente o indivíduo de sua zona de conforto. Acostumados há séculos com o uso documental em formato palpável, pode tornar-se difícil a aceitação por parte da sociedade do documento digital. Da mesma forma que a Assinatura Digital é de difícil compreensão por boa parte das pessoas.

Apesar dessa tendência, historicamente as mudanças acabam se concretizando.

O esclarecimento do tema e prova de sua confiabilidade tem papel fundamental para sua aceitação.

1.3 OBJETIVOS

1.3.1 Objetivo Geral

Avaliar a confiabilidade desta nova tecnologia do ponto de vista técnico sob os aspectos da garantia de autenticidade, sigilo e reconhecimento de autoria de operações e documentos

virtuais. De sua estrutura hieráquico-administrativa e do ponto de vista jurídico, acerca da validade e segurança jurídica.

1.3.2 Objetivos Específicos

- Apresentar os principais conceitos e a estrutura hierárquica da Certificação Digital brasileira;
- Avaliar os aspectos legais que validam documentos e assinaturas digitais e criam a cadeia de confiabilidade da Infra-estrutura da ICP-Brasil.
- Apresentar e avaliar as tecnologias utilizadas no processo de certificação.
- Conceitos e funcionamento de Certificados, Assinaturas digitais e carimbo do tempo;
- Dicas de segurança;

1.4 JUSTIFICATIVA

Com a rapidez com que as mudanças ocorrem no mundo atual, muitas pessoas não conseguem acompanhá-las. Provavelmente a informática seja um dos setores onde elas aconteçam com maior rapidez. Uma vez que estas mudanças afetam a vida de todas as pessoas, direta ou indiretamente, cabe aos envolvidos na área contribuir para a sua divulgação e esclarecimento.

1.5 PROCEDIMENTOS METODOLÓGICOS

Este trabalho segue o método bibliográfico de natureza científica aplicada. Usa referenciais teóricos baseados em livros de especialistas. Também faz uso de periódicos, cartilhas e manuais encontrados em sítios de órgãos públicos, tais como ITI, Setores do Judiciário, universidades, etc. No que tange a questões de direito, referencia-se em Medidas Provisórias, Leis e normas vigentes.

1.6 EMBASAMENTO TEÓRICO

Serviram de base para aprofundamento do tema consultas a Leis e normas, além de revistas e cartilhas disponibilizadas pelo INSTITUTO NACIONAL DE TENCOLOGIA DA INFORMACAO (ITI) em seu sítio de Internet (http://www.iti.gov.br/).
A disponibilidade bibliográfica nas livrarias é escassa. No entanto, diversos autores renomados disponibilizam suas obras para venda via Internet.
Além de Trabalhos acadêmicos disponibilizados via Internet.

1.7 ESTRUTURA

Este trabalho é composto por uma introdução como primeiro capítulo, traçando um breve histórico sobre o surgimento do Registro Civil Brasileiro, que deu origem às primeiras carteiras de identidade até o novo Registro de Identificação Civil(RIC). Seguido da apresentação do problema e premissas. Apontando a seguir os objetivos gerais e específicos deste trabalho. Logo após, 3 capítulos explicativos:
capitulo 2 - aborda conceitos da Certificação Digital, estrutura da ICP-Brasil, entidades que a compõem, suas atribuições, além das garantias oferecidas pela ICP-Brasil;
capitulo 3 - legislação, com a apreciação da MP 2.200, a validade jurídica de documentos e assinaturas digitais; normatização da ICP-Brasil; Fiscalizações e Auditorias.
capitulo 4 - tecnologias: *hardware*, criptografia e funcao *hash* na assinatura digital, certificado digital e carimbo do tempo e cuidados ao utilizar a Certificação Digital;
Ao final conclusões sobre o tema e as referências;

2. CERTIFICAÇÃO DIGITAL

2.1 CONCEITO

Segundo definição do Professor Luiz Gustavo Cordeiro da Silva,

> Certificação Digital é um conjunto de técnicas e processos que propiciam mais segurança às comunicações e transações eletrônicas, permitindo também a guarda segura de documentos.
> Permite que informações transitem pela Internet com maior segurança. É baseada na existência de Certificados Digitais emitidos por uma Autoridade Certificadora(AC), considerada confiável pelas partes envolvidas. (Silva, AT EL., 2008 p.X) Garantindo o conteúdo de mensagens ou textos, sua autoria e data em que foi assinada. Baseia-se no princípio da terceira parte confiável, que oferece confiabilidade entre partes que se utilizem de Certificados Digitais. Para isso utiliza-se de uma Infra-estrutura de chaves públicas, cuja principal função é definir técnicas e procedimentos.
> A Medida Provisória 2.200-2, de agosto de 2001 estabelece a Infra-estrutura de Chaves públicas Brasileira – ICP-Brasil. (Silva, AT EL., 2008 p.XII)

2.2 ESTRUTURA DA ICP-BRASIL

2.2.1 Hierarquia

Possui uma estrutura em formato de árvore, vinculando hierarquicamente as organizações que a compõem.

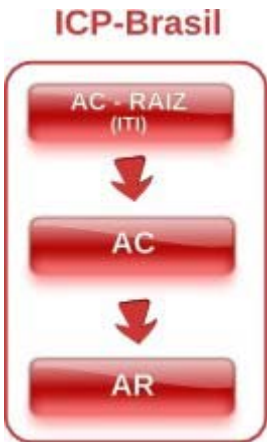

Figura 1- estrutura em árvore
Fonte: Instituto Nacional de Tecnologia da Informação (ITI)

Autoridade Certificadora Raiz(**AC-Raiz**)

A Autoridade Certificadora Raiz da ICP-Brasil é a primeira autoridade da cadeia de certificação. É executora das Políticas de Certificados e normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil. Portanto, compete à AC-Raiz emitir, expedir, distribuir, revogar e gerenciar os certificados das autoridades certificadoras de nível imediatamente subseqüente ao seu. É também encarregada de emitir a lista de certificados revogados e de fiscalizar e auditar as autoridades certificadoras, autoridades de registro e demais prestadores de serviço habilitados na ICP-Brasil. Além disso, verifica se as Autoridades Certificadoras (AC) estão atuando em conformidade com as diretrizes e normas técnicas estabelecidas pelo Comitê Gestor [3].

Autoridade de Certificação(**AC**)

Um autoridade de certificação é uma entidade encarregada de emitir certificados para indivíduos, computadores ou organizações, sendo que o certificado é que confirmam a identidade e outros atributos do usuário do certificados,para outras entidades.

Uma AC aceita uma solicitação de certificado, verifica as informações do solicitador e, em seguida, usa sua chave privada para aplicar a assinatura digital no certificado. A CA emite então o certificado para que o usuário do certificado o use como uma credencial de segurança dentro de uma infra-estrutura de chave pública (PKI). Emitem, expedem, distribuem, revogam e gerenciam os certificados, bem como colocam à disposição dos usuários, listas de certificados revogados, além de manter o registro de suas operações[4].

Autoridade de Registro(**AR**)

São entidades operacionalmente vinculadas à determinada AC. Compete-lhes identificar e cadastrar usuários na presença deste, encaminhando solicitações de certificados às AC e manter registros de suas operações.(Silva, AT EL., 2008, p.84)

Prestador de Serviços de Suportes(**PSS**)

São empresas contratadas por uma AC ou AR para realizar atividades de disponibilização de infra-estrutura física e lógica e disponibilidade de recursos humanos especializados.(Silva, AT EL., 2008, p.84)

Titulares de Certificados

São entidades, pessoas físicas ou jurídicas, que podem ser titulares de certificados digitais emitidos por uma das AC integrantes da ICP-Brasil.
(Silva, AT EL., 2008, p.84)

3(Disponível em:<http://www.iti.gov.br/twiki/bin/view/Certificacao/EstruturaIcp>Acesso em: 11/11/2011)

4(Disponível em:<http://technet.microsoft.com/pt-br/library/cc781802(WS.10).aspx> Acesso em: 07/11/2011)

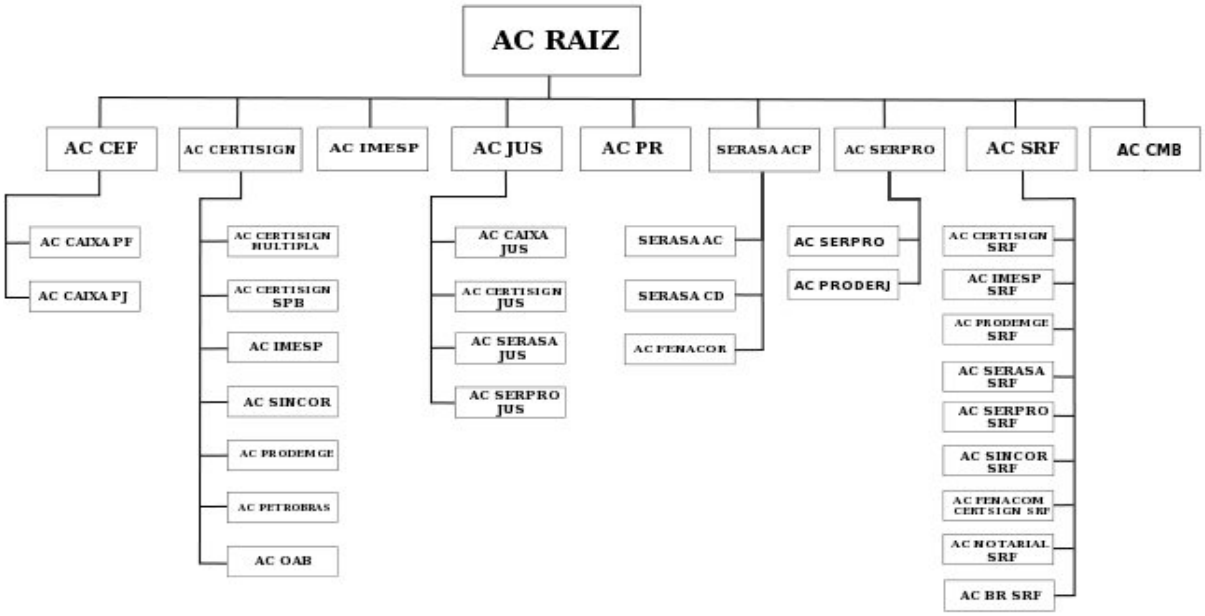

Figura 2 - Estrutura hierárquica da ICP-Brasil
Fonte: Instituto Nacional de Tecnologia da Informação (ITI)

2.2.2 Garantias Oferecidas pela ICP-Brasil

A ICP-Brasil possui uma série de peculiaridades que oferecem diversas garantias aos titulares e usuários de certificados:

- O par de chaves criptográficas deve ser gerado sempre pelo próprio titular e sua chave privada de assinatura é de seu exclusivo controle, uso e conhecimento;
- Os documentos assinados com processo de certificação da ICP-Brasil possuem presunção de validade jurídica;
- São utilizados padrões internacionais para os certificados, bem como algoritmos criptográficos e tamanhos de chaves que oferecem nível de segurança aceitável internacionalmente;
- As instalações e procedimentos das entidades credenciadas possuem um nível preestabelecido da segurança física, lógica, de pessoal e procedimental em padrões internacionais;
- As entidades estão sujeitas a uma auditoria previa ao credenciamento, e auditorias anuais para manter-se credenciadas;
- É obrigatória a validação presencial dos titulares para obtenção de certificados;

(Silva, AT EL., 2008 p. 80)

3 LEGISLAÇÃO

Um dos apectos mais relevantes da Certificação Digital, do ponto de vista da credibilidade, é o reconhecimento legal de documentos e assinaturas digitais. O embasamento jurídico no Brasil começa a partir da edição da Medida Provisória n.º 2.200-2, de 24 de agosto de 2001 que cria, em seu artigo primeiro, a Infra-estrutura de Chaves públicas Brasileira(ICP-Brasil) com a finalidade de validar documentos, assinaturas digitais e transações eletrônicas.

> Art 1°.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 pressupõe uma hierarquia como a base em uma ordem de poderes, atribuições e responsabilidades criando uma cadeia de confiança. Também atribui ao recém criado órgão, a obrigatoriedade de garantir autenticidade e integridade de documentos, ou seja, a definição de métodos, padrões e tecnologias para cumprir esta finalidade.

> Nesta hierarquia, como órgão máximo está a Raiz, Autoridade Certificadora Raiz(AC-Raiz) e como autoridade gestora de políticas está o Comitê Gestor da ICP-Brasil (CG) assim representado:
>
> Casa Civil da Presidência da República;
>
> Gabinete de Segurança Institucional da Presidência da República;
>
> Ministério da Justiça;
>
> Ministério da Fazenda;
>
> Ministério do Desenvolvimento, Indústria e Comércio Exterior;
>
> Ministério do Planejamento, Orçamento e Gestão;
>
> Ministério da Ciência e Tecnologia.

O artigo 2° especifica a ordem em que se estabelece o funcionamento dos órgãos que compõem a ICP-Brasil. Cria com isso Autoridades Certificadoras(AC) e Autoridades de Registro(AR). Esta, hierarquicamente vinculada a AC, que por sua vez é vinculada à ICP-Raiz.

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

O artigo 5º da MP 2000-2, reedição da MP 2000 amplia suas atribuições.

> Art.2° À AC Raiz, primeira autoridade da cadeia de certificação, executora das Políticas de Certificados e normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil, compete emitir, expedir, distribuir, revogar e gerenciar os certificados das AC

> de nível imediatamente subseqüente ao seu, gerenciar a lista de certificados emitidos, revogados e vencidos, e executar atividades de fiscalização e auditoria das AC e das AR e dos prestadores de serviço habilitados.

3.1 NORMATIZACÃO DA ICP-BRASIL

A ICP-Brasil é normatizada por meio de Medidas Provisórias, Decretos, Resoluções, Instruções Normativas e Portarias.

A Estrutura Normativa é composta por Documentos(DOC-ICP), Adendos(ADE-ICP) e Manuais de Condutas Técnicas(MCT)[5].

> Os documentos que descrevem as práticas e políticas de qualquer AC no âmbito da ICP-Brasil são:
> Declaração de Praticas de Certificação(DPC): descreve práticas e procedimentos de certificação adotadas pela AC;
> Políticas de Certificado (PC): descreve políticas de um tipo específico de certificado Digital emitido por uma AC;
> Políticas de Segurança(PS): este documento descreve as diretrizes de segurança adotadas pela AC. Por exemplo, a DOC-ICP-02 preve a criação de um Plano de Continuidade do Negócio(PCN) que deve ser implementado e testado, pelo menos uma vez por ano, para garantir a continuidade dos serviços críticos ao negócio.(Silva, AT EL. 2008, p. 52)

3.2 FISCALIZACÃO E AUDITORIAS

O juiz de Direito Sr. Demócrito Reinaldo Filho entende a edição da MP 2.200 como sendo o "marco regulatório" da Certificação Digital no Brasil. E que as atribuições do ITI em conjunto com o Comitê Gestor, lhes confere características de Agência Reguladora.

> A edição da MP 2.200 representa um Marco Regulatório da Certificação no Brasil...a forma autárquica conferida ao ITI, órgão executor das políticas de certificação, e a composição híbrida do Comitê Gestor, autoridade gestora das políticas de certificação, conferem a eles autonomia estrutural e política, características próprias das agências reguladoras tradicionais. Ao ITI cabe desempenhar as atividades de fiscalização e auditoria[6]

5(Disponível em: <http://www.iti.gov.br/twiki/bin/view/Certificacao/DocIcp>Acesso em: 07/11/2011)
6(REINALDO FILHO, Demócrito.Disponível em: <http://www.boletimjuridico.com.br/ doutrina/texto.asp?id=897> Acesso em: 8. 11.2011).

A chave privada de uma AC é seu bem maior. Se for comprometida poderá afetar sua credibilidade de forma irreversível. Segundo o Diretor-Presidente do ITI, Renato Martini:

> O leitor mais desavisado deve por vezes pensar que os requisitos de segurança física e lógica exigidos na ICP-Brasil são demasiados. No entanto, deve ele perceber, que num criptossistema civil como o ICP-Brasil o mais fundamental, o que deve receber sigilo total, é a chave privada da AC. Todo o requisito de segurança tem em última instância esse desiderato: preservar a chave criptográfica da AC.
> (Luz, Clarissa P. da ,**Centro de Certificação Digital – Construção, Administração e Manutenção**,prefácio)

Cabe o ITI fiscalizar e auditar o cumprimento das normas por parte das AC, AR e PSS , conformidade das atividades exercidas e níveis de segurança exigidos em instalações físicas, lógicas e de pessoal.

3.2.1 Instalações Físicas, Lógicas e Pessoal

Centro de Certificação Digital (CCD)

Clarissa P. da Luz descreve em seu livro intitulado Centro de Certificação Digital (CCD) sua participação na montagem do Centro de Certificação Digital do ITI. A partir desta experiência demonstra como construir um CCD em conformidade com os requisitos da ICP-Brasil.

De início elenca fatores que considera relevantes acerca da localização:

> Localização do edifício, a salvo de inundação, incêndio próximo, deslizamento de terra, transporte com carga perigosa, comoção civil ou queda de objetos(plataforma de lançamentos). A construção deverá oferecer setorização eficaz contra incêndio,isolamento térmico, impermeabilização e drenagem eficaz.
> Não deverá haver identificação pública externa das instalações do CCD.
>
> Níveis de segurança exigidos
> ...deverão ser definidos pelo menos quatro níveis de segurança de acesso e mais dois, para armazenamento das informações mais sensíveis.
>
> Sala-cofre
> O acesso ás sala-cofre devera ser constituída por ambiente fechado e fisicamente protegido, dedicado exclusivamente à certificação digital, não permitindo a visibilidade das operações de emissão e renovação de certificados. A célula devera ser hermeticamente fechada, devendo haver vedação em todos os elementos que a compõem, tais como fundo, teto e paredes. O corredor da Área de Infra-estrutura devera constituir o único acesso aos compartimentos internos da sala-cofre.
> As característica dos cofres deverão seguir os critérios de segurança física para armazenamento de mídias estabelecidos na norma ABNT NBR 11.515, e o atendimentos a esses requisitos devera ser comprovado por meio de atestado ou laudo.

Portas de acesso

As portas de compartimentos internos devera ter fechamento e travamento automáticos, com abertura por sistema de controle de acesso eletrônico. Deverão ser compostas por chapas de aço ou material com resistência e características equivalentes ou superiores...

CFTV

Deverá dispor de Sistema de Circuito Fechado de Televisão, sensores de movimento em quantidade suficiente e posições tais que permitam o acompanhamento de todas as ações realizadas em todos os compartimentos da área de produção

Alta disponibilidade

Através de um sistema de alimentação redundante de no-break e sistema para geração de energia com dois geradores independentes, com reserva de energia para 12 horas devendo operar de forma contínua, estar disponível de 24x7x365, a fim de evitar prejuízo ás atividades AC.

Controle de segurança de pessoas

Segurança tem mais haver com fatores humanos, processos e procedimentos, do que com tecnologia. Os incidentes de segurança, em sua maioria são causadas por pessoas, de forma acidental ou proposital.
Portanto , quanto mais preparados estiverem os funcionários de uma organização, menos riscos ela correrá e mais segura será. Previamente as contratações, deveram ser feitos levantamentos de dados pessoais, como Antecedentes criminais, histórico creditício no SPC, SERASA, Dívida ativa, entre outros. Deverão ser consideradas ainda, informações sobre os dois últimos empregos, como cargo, motivo da saída, conceito profissional. Alem de três referências profissionais e a verificação de grau acadêmico adequado ao cargo.
Poderá ainda, se o candidato possuir CNH, ser requisitado o prontuário de Departamento de Transito. Entrevista pessoal com propósito de avaliar o equilíbrio emocional , ajuste de personalidade e atributos pessoais exigidos ao cargo pretendido.
Estas exigências se aplicam inclusive a empregados terceirizados e Prestadores de serviços contratados. Treinamentos voltados à capacitação com atualização periódica, sempre comprovados por certificação do órgão responsável pelo treinamento.

Acesso às instalações

O controle de saída e entrada de material da CCD devera ser registrada no Livro de Ocorrências da recepção O ingresso ás instalações exigira uso de cartões de acesso aos empregados, fornecedores e prestadores de serviços que deverão ser submetidos a detectores de metal.

3.2.2 Auditorias

A Resolução 44 do ITI, que estabelece os critérios e procedimentos para realização de auditorias nas entidades de ICP-Brasil, define os seguintes tipos de auditorias a serem realizadas nessas entidades:

Pré-operacional – realizada previamente aos seu credenciamento na ICP-Brasil;

Operacional – realizada no mínimo uma vez por ano para fins de continuidade do credenciamento;

As Auditorias são realizadas pelo CG da ICP-Brasil ou seus prepostos;
pela AC-Raiz; Autoridades Certificadoras; Empresas de auditoria especializada e independentes cadastradas junto à ICP-Brasil; ou órgãos de auditoria interna de AR no caso de empresas que os possuam por forca de lei e cadastradas junto à ICP-Brasil.

Auditoria pré-operacional de AC

1. segurança de pessoal;
2. segurança física;
3. segurança lógica;
4. segurança de rede;
5. segurança da informação;
6. gerenciamento de chaves criptográficas e do certificado da própria AC; e
7. gerenciamento do ciclo de vida dos certificados emitidos;

(Silva, AT EL., 2008, p.100)

Auditoria operacional de AC

Verifica os mesmos itens que na pré-operacional e a partir dos dados coletados na pré-operacional é possível avaliar se a AC está realizado adequadamente os procedimentos previstos.

As AR e PSS também recebem Auditorias pré-operacionais e operacionais através da avaliação de requisitos específicos. (Silva, AT EL., 2008, p.100)

4 TECNOLOGIAS

4.1 CRIPTOGRAFIA

A palavra criptografia é originaria dos gregos *kryptus*, que quer dizer oculto e *graph*, escrever. Segundo o professor Luiz Gustavo cordeiro da Silva,

> Dentre as diversas tentativas de definir criptografia de maneira precisa, pode-se dizer, de um modo simples, que criptografia é a ciência de fazer com que o custo de adquirir uma informação de maneira imprópria seja maior que o custo obtido com a informação.
>
> Ela prevê formas de embaralhar ou cifrar mensagens visando torná-las inelegíveis e que posteriormente se possa obter a mensagem original. Para isso faz uso de chaves.
> Chave é um valor numérico para cifrar e decifrar um texto.
> a segurança de um criptossistema pode então ser mensurado baseado no tamanho do espaço de chaves e no poder computacional atualmente disponível.

Avanços tecnológicos que aumentam o poder computacional diminuem o tempo de quebra de um algoritmo criptográfico, em contrapartida, o aumento do tamanho da chave dificulta sua quebra.

> Criptografia de chave secreta
> Também conhecida como criptografia de chave simétrica Utiliza uma única chave secreta para criptografar e descriptografar um texto.
>
> Criptografia de chave pública
> Também conhecida com criptografia de chave assimétrica, utiliza duas chaves distintas, uma pública e outra privada. Entre elas existe uma relação matemática que torna inviável derivar a chave privada a partir de uma chave pública. Devido a uma relação matemática, uma mensagem criptografada a partir de uma determinada chave pública pode ser decifrada com sua chave privada correspondente e uma mensagem cifrada com a chave privada pode ser decifrada com o uso da chave pública correspondente.
> A principal vantagem da criptografia em chave pública em relação a criptografia baseada em chave secreta é a segurança implícita do mecanismo de gerencia de chaves.
> Em um sistema de criptografia simétrica, qualquer pessoa que escutar ou interceptar a chave em transito poderá ler, modificar, e forjar qualquer mensagem cifrada ou autenticada por esta chave. O processo de geração, transmissão e armazenamento das chaves é chamado de gerenciamento de chaves.
> De modo a resolver este problema de gerenciamento, Whiffield Diffie e Martin Hellman introduziram o conceito de criptografia de chave pública ou assimétrica, em 1976. As idéias expressa no algoritmo de Diffie-Hellman, utilizado exclusivamente para distribuição de chaves foram estendidos em outros algoritmos de criptografia de chave pública como RSA, para permitir aplicações que incluem não apenas o gerenciamento de chaves, mas também a aplicação em sistemas de cifração e de assinatura digital.
> Segurança dos sistema RSA A segurança do sistema depende de duas suposições críticas:
> A fatoração é necessária para quebrar o sistema.
> A fatoração é difícil e qualquer aproximação que possa ser usada para quebrar o sistema é no mínimo, tão difícil quanto a fatoração

4.1.1 Assinatura Digital e Resumo Hash

O CG assim definiu a Assinatura Digital e função de *hash* através da Resolução Nº 62 de 09 de janeiro de 2009:

> Assinatura eletrônica
> o conjunto de dados sob forma eletrônica, ligados ou logicamente associados a outros dados eletrônicos, utilizado como método de comprovação da autoria.
>
> Assinatura digital ICP-Brasil é a assinatura eletrônica que:
> a) esteja associada inequivocamente a um par de chaves criptográficas que permita identificar o signatário;
> b) seja produzida por dispositivo seguro de criação de assinatura;
> c) esteja vinculada ao documento eletrônico a que diz respeito, de tal modo que qualquer alteração subseqüente neste seja plenamente detectável; e
> d) esteja baseada em um certificado ICP-Brasil, válido à época da sua aposição.
>
> Função *hash*
>
> Uma transformação matemática que faz o mapeamento de uma seqüência de bits de tamanho arbitrário para uma seqüência de bits de tamanho fixo menor – conhecido como resultado *hash* ou resumo criptográfico – de forma que seja muito difícil encontrar duas mensagens produzindo o mesmo resultado *hash* (resistência à colisão) e que o processo reverso também não seja realizável (dado um resultado *hash*, não é possível recuperar a mensagem que o gerou).

Segundo o professor Luiz Gustavo Cordeiro da Silva,

> Assinatura digital é um conjunto de dados usados para garantir a integridade e autenticidade de uma determinada mensagem. O autor usa sua chave de assinatura para assinar a mensagem e enviá-la junto com a assinatura digital para um destinatário.
> A mensagem original primeiramente é aplicada como entrada de um algoritmo de resumo *hash*, depois o resultado é criptografado usando a chave privada do autor. O resultado desta criptografia é denominado Assinatura Digital da mensagem.

Figura 4 – Assinatura digital – geração de resumo *hash*
Fonte: Instituto Nacional de Tecnologia da Informação (ITI)
RESOLUÇÃO 62

> O destinatário recebe a mensagem e usa uma chave de verificação para verificar a origem da mensagem e garantir que ela não foi modificada enquanto estava em trânsito.
> ...o destinatário recebe a mensagem com a assinatura digital e começa o processo de verificação da assinatura.
> Primeiramente, é necessário aplicar o mesmo algoritmo de resumo usado para assinar a mensagem, gerando assim o resumo de mensagem atual. Aplicando a chave pública do autor para descriptografar a assinatura digital, é possível obter o resumo de mensagem esperado.
> Se os resumos esperado e atual tiverem o mesmo valor, então a mensagem não foi alterada e pode-se afirmar que foi realmente assinada com a chave do autor, senão, a mensagem foi adulterada ou o par de chaves que foram usadas não eram um par de chaves relacionadas.
> (Silva, AT EL., 2008 p.21)

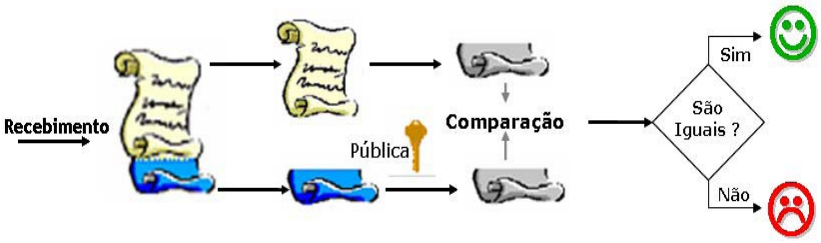

Figura 5 - Confirmação de Assinatura Digital
Fonte: Instituto Nacional de Tecnologia da Informação (ITI)
RESOLUÇÃO 62

A certeza inequívoca de que o signatário de um par de chaves criptográficas está vinculado a um documento eletrônico especifico, é possível graças ao algoritmo *hash*. Que, além disso, permite detectar que quaisquer alterações realizadas no documento subseqüente à assinatura, sejam percebidas.

4.1.2 Certificado Digital

> Um certificado de chave pública, é uma declaração assinada digitalmente que estabelece uma ligação do valor de uma chave pública com a identidade da pessoa, do dispositivo ou do serviço que contém a chave particular correspondente. A maioria dos certificados de uso comum se baseia no padrão de certificado X.509v3.
>
> Os certificados também são emitidos de uma Autoridade de Certificação para outra, a fim de estabelecer uma hierarquia de certificação.
> O emissor e assinante do certificado é uma Autoridade de Certificação.
>
> Normalmente, os certificados contêm as seguintes informações:
>
> **a)** O valor da chave pública da entidade.
> **b)** As informações sobre o identificador da entidade, como nome e endereço de e-mail.
> **c)** O período de validade (período de tempo durante o qual o certificado é considerado válido).

d) Informações sobre o identificador do emissor.
e) A assinatura digital do emissor, que atesta a validade do vínculo entre a chave pública da entidade e as informações de identificação da entidade.

Um certificado só é válido pelo período de tempo nele especificado; cada certificado contém datas *Válido de* e *Válido até*, que definem os prazos do período de validade. Quando o prazo de validade de um certificado termina, a entidade do certificado vencido deve solicitar um novo certificado.

Se for preciso desfazer o vínculo declarado em um certificado, esse pode ser revogado pelo emissor. Cada emissor mantém uma lista de certificados revogados, que pode ser usada pelos programas quando a validade de um determinado certificado é verificada.

Usos dos certificados

Como os certificados geralmente são utilizados para estabelecer identidade e criar relações de confiança para a troca segura de informações, as autoridades de certificação podem emitir certificados para pessoas, dispositivos (como computadores) e serviços que estejam sendo executados em computadores. Os certificados podem ser emitidos para uma série de funções, como autenticação de usuários na Internet, autenticação de um servidor *Web*, correio eletrônico seguro.

Os certificados também podem ser usados para verificar a autenticidade do código do software que você obtém por meio de *download* da Internet.

Eles podem ser usados para:

1. Autenticação, que verifica a identidade de alguém ou de algo.
2. Privacidade, que garante que essas informações só estarão disponíveis ao público a que se destinam.
3. Criptografia, que oculta informações para que leitores não autorizados não consigam decifrá-las.
4. Assinaturas digitais, que fornecem não-repúdio e integridade de mensagens [7]

7 Disponível em:<http://technet.microsoft.com/pt-br/library/cc728388(WS.10).aspx> Acesso em:07/11/2011)

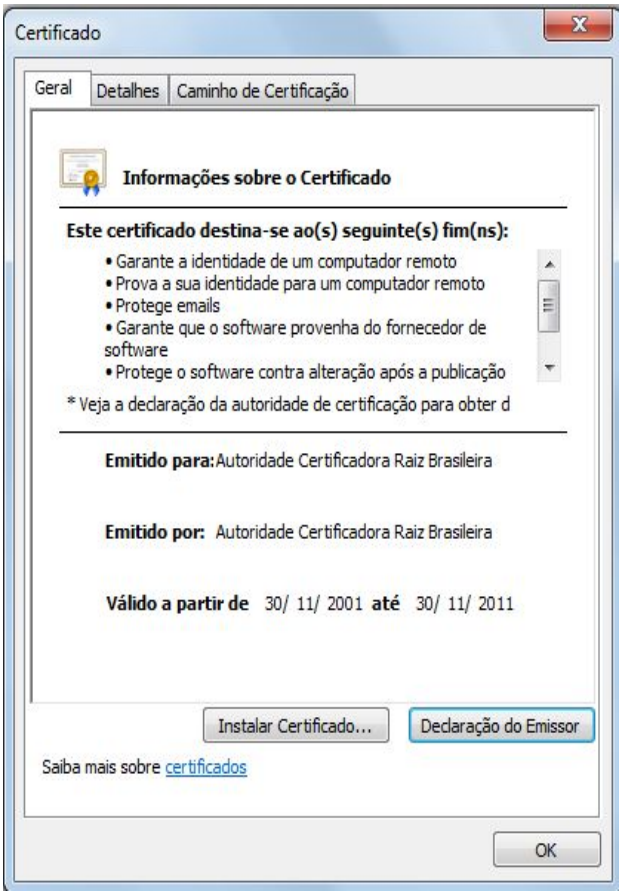

Figura 3 - Certificado Digital da AC-Raiz

Fonte: Instituto Nacional de Tecnologia da Informação (ITI)

4.1.3 Carimbo do Tempo

Algumas operações efetuadas com o uso da Certificação Digital requerem a informação da data exata em que ocorreram e outras exigem ainda a hora exata da ocorrência. A exemplo dos prazos processuais.

Segundo o coordenador de Operações do ITI, Luiz Carlos Porto "... o carimbo de tempo oferece ainda mais confiabilidade e segurança ao documento digital, pois é uma certidão digital, que recebe da Autoridade Certificadora um carimbo com o momento exato – data e hora - em que ele foi emitido. Uma prova irrefutável da existência da informação digital".

4.1.4 Cuidados ao Utilizar a Certificação

Cuidados a serem tomados por titulares de Certificados Digitais segundo a REVISTA DIGITAL do sítio do ITI:

> • A senha de acesso da chave privada e a própria chave privada não devem ser compartilhadas com ninguém;
> • Caso o computador onde foi gerado o par de chaves criptográficas seja compartilhado com diversos usuários, não é recomendável o armazenamento da chave privada no disco rígido, pois todos os usuários terão acesso a ela, sendo melhor o armazenamento em disquete, smart card ou token;
> • Caso a chave privada esteja armazenada no disco rígido de algum computador, deve-se protegê-lo de acesso não autorizado, mantendo-o fisicamente seguro. Nunca deixe a sala aberta quando sair e deixar o computador ligado.
> Utilize um protetor de tela com senha. Cuidado com os vírus, eles podem danificar sua chave privada;
> • Caso o software de geração do par de chaves permita optar entre ter ou não uma senha para proteger a chave privada, recomenda-se a escolha pelo acesso por meio de senha. Não usar uma senha significa que qualquer pessoa que tiver acesso ao computador poderá se passar pelo titular da chave privada, assinando contratos e movimentando contas bancárias. Em geral, é bem mais fácil usar uma senha do que proteger um computador fisicamente;
> • Utilize uma senha longa, intercalando letras e números, uma vez que existem programas com a função de desvendar senhas. Deve-se evitar o uso de dados pessoais. A senha nunca deve ser anotada, sendo recomendável sua memorização.
> (ITI - REVISTA DIGITAL - 1º semestre 2010)

4.2 HARDWARE

Smart cards e Tokens

Como afirma Conrado Leiras Matos[6]

> Acredita-se que *Smart Cards* possa oferecer mais segurança e confidencialidade que outros tipos de informação ou armazenamento de informação. O *Smart Card* é um dispositivo de segurança intrínseca. Ele é um local seguro para armazenamento de informação como chaves privadas, números de contas, e informações pessoais como informações biométricas, ou então para executar processos *off-line* como encriptação e descriptação de chaves públicas e privadas.

Considerando a importância crucial de preservar as chaves privadas de acessos indevidos, os cartões inteligentes tem papel fundamental para dar credibilidade à Certificação Digital. O armazenamento da chave privada em arquivo, a ser instalada diretamente no *hard disk*, fragiliza a segurança da chave e deve ser evitado.

> Processo de montagem do *smart card* até o usuário final.
>
> A estrutura física do cartão geralmente, é composta de até 3 elementos. O cartão de plástico, um circuito impresso e um chip de circuito integrado são embutidos no cartão.
>
> Um circuito integrado consiste de um microprocessador, memória apenas de leitura ROM , RAM não estática e EEPROM que manterá seu estado quando a alimentação for removida... o tamanho do chip é restringido a alguns milímetros.

Ciclo de Vida de um *Smart Card*

Existe um sistema operacional dentro de cada *Smart Card* que pode conter um número de identificação do fabricante, tipo de componente, número de série, informação do perfil, entre outros. A área do sistema pode conter diferentes chaves de segurança, como a chave do fabricante ou de fabricação (KF) e a chave de personalização. Toda essa informação deve ser mantida sigilosa e não ser revelada a outros do fabricante para o provedor de aplicação, e então para o portador do cartão. A produção do *Smart Card* é dividida em diferentes fases. Limitação na transferência de dados é incremental em diferentes fases a fim de proteger as diferentes áreas do *Smart Card*. Existem cinco fases para um ciclo de vida.

Fase de Fabricação

fase é conduzida pelos fabricantes de *chip*. O circuito integrado de silicone é criado e testado nessa fase. A chave de fabricação (KF) é adicionada para proteger o chip de modificações fraudulentas até que ele seja montado no suporte plástico do cartão. A KF de cada chip é única e deriva chave mestra do fabricante do cartão. Outros dados de fabricação serão escritos no chip até o fim dessa fase. Então o chip está pronto para ser entregue ao fabricante do cartão com a proteção da KF.

O processo de cadastramento de fornecedores é critico e deve obecer um rigido controle na escolha. A qualidade do produto pode definir o nivel de seguranca ao usuario final.

Fase de Pré-personalização

Essa fase é conduzida pelos fornecedores de cartão. Nessa fase, o chip será montado no cartão de plástico que deverá ter o logo do provedor da aplicação impresso. A conexão entre o chip e o circuito impresso será feita e o conjunto da unidade será testado. Para aumentar a segurança e para permitir a entrega segura para o emissor do cartão, a chave de fabricação será substituída por uma chave de personalização (KP), que não poderá mais ser modificada. Instruções físicas de acesso à memória também serão desabilitadas O acesso ao cartão será feito usando apenas endereçamento lógico de memória. Isso preservará a área do sistema e de fabricação de serem acessadas ou modificadas.

Fase de Personalização

Essa fase é conduzida pelos emissores do cartão. Ela completa a criação de estruturas lógicas de dados. Os conteúdos de arquivos de dados e dados de aplicações serão escritos no cartão. Informação da identidade do proprietário do cartão, PIN, e desbloqueador de PIN serão armazenados também. Ao fim, uma trava de utilização será escrita ao cartão para indicar que essa fase chegou ao fim.

Fase de Utilização

Essa é a fase para o uso normal do cartão pelo seu proprietário. O sistema de aplicação, os controle de acesso lógico aos arquivos entre outros estarão ativados. O acesso à informação do cartão estará limitado pelas políticas de segurança configuradas de acordo com a aplicação.

A Fase de Fim de Vida (Fase de Invalidação)

Existem duas formas que o cartão pode entrar nessa fase. Uma é iniciada pela aplicação que escreve a chave de invalidação para um arquivo individual ou arquivo mestre. Todas as operações incluindo escrita e atualização serão desabilitadas pelo sistema operacional. Apenas instruções de leitura poderão continuar ativas para propósitos de análise. Outra maneira de fazer o cartão entrar nessa fase é quando o sistema de controle bloqueia irreversivelmente o cesso porque tanto o PIN e o desbloqueador do PIN são bloqueados, bloqueando todas as operações.

O *smart card* constitui um elemento fundamental da infraestrutura de chave pública (PKI) que a Microsoft integra atualmente no Windows: ele estende de fato as soluções puramente de *software* tais como a autenticação de cliente, a abertura de sessão, e o correio eletrônico seguro. *O smart card* constitui essencialmente um ponto de convergência para os certificados de chave pública e de chave associada, já que: ele garante um armazenamento inviolável para a proteção das chaves privadas e de todas outras informações pessoais; ele permitir isolar o cálculo crítico para a segurança, relativos à autenticação, às assinaturas eletrônicas e a troca de chaves de toda outra parte não concernida do sistema; ele fornece um certo nível de portabilidade que permite deslocar as referências e outras informações de ordem privada entre os computadores utilizados no local de trabalho, no domicílio ou em deslocamento.

O *smart card* estende o processo de autenticação de chave pública propondo a armazenagem segura da chave privada e um motor criptográfico que cuide das assinaturas eletrônicas e a troca de chave.

6(Disponível em: http://www.gta.ufrj.br/grad/01_2/smartcard/smartcard.html,acessado>Acesso em em:31/10/2011)

CONCLUSÃO

Embasamento jurídico:

O entendimento do juiz de Direito Sr. Demócrito Reinaldo Filho é de que as atribuições concedidas em conjunto ao Comitê Gestor e à AC-Raiz são, em termos práticos, equivalentes ao funcionamento de uma Agência Reguladora. E que a edição da MP 2.200 representa o marco regulatório da Certificação Digital Brasileira. Consoante ao reconhecimento da validade jurídica de documentos virtuais e suas assinaturas, cria uma rede de confiança na ordem estrutural da Certificação no Brasil, através da ordenação legal da infra-estrutura de chaves públicas Brasileira.

O arcabouço jurídico que rege um tema, naturalmente sempre apresenta lacunas.
E com a Certificação Digital não deverá ser diferente. Situações novas, inusitadas muitas vezes, que ensejarão a necessidade de adequar a legislação de tempos em tempos. Isto é natural, pois a justiça é um organismo vivo, e tem que se adaptar às constantes mudanças sociais. Conclui-se que, a legislação vigente atende suficientemente seus objetivos, mas deverá ser aprimorada.

Aspectos Tecnológicos:

Informações coletadas sobre o *smart card* atestam a garantia da proteção da chave privada do titular do certificado. O próprio site da Microsoft garante isto "... *smart card* constitui essencialmente um ponto de convergência para os certificados de chave pública e de chave associada, já que: ele garante um armazenamento inviolável para a proteção das chaves privadas e de todas outras informações pessoais".
O autor Conrado Leiras Matos, no entanto, coloca alguma dúvida sobre a segurança total do cartão ao afirmar "... acredita-se que *Smart Cards* possa oferecer mais segurança e confidencialidade que outros tipos de informação ou armazenamento de informação". Mas logo a seguir, em seu texto, atesta a sua confiabilidade, observando a segurança intrínseca que o cartão apresenta "... O *Smart Card* é um dispositivo de segurança intrínseca e um local seguro**",** e ainda aponta uma outra grande vantagem, a execução de processos *off-line* de encriptação e descriptação. Avaliando esses fatos, pode-se afirmar que o cartão é plenamente confiável, embora com a ressalva de que, na área da informática é sempre difícil afirmar que um sistema é totalmente seguro.

Outro ponto relevante sobre a segurança tecnológica é o sistema criptográfico adotado pela Certificação Digital, o assimétrico. Praticamente elimina a fragilidade no gerenciamento de chaves, muito comum na criptografia simétrica.
Como utiliza duas chaves, uma pública e outra privada diretamente vinculadas entre si e a um usuário específico, qualquer documento cifrado a partir de uma chave pública de uma pessoa, somente poderá ser decifrado com sua chave privada correspondente e da mesma pessoa. Assim o

sigilo de uma mensagem ou documento estará totalmente garantido pois, “devido a uma relação matemática, uma mensagem criptografada a partir de uma determinada chave pública (somente) pode ser decifrada com sua chave privada correspondente...”

Já o processo inverso, cria o conceito de Assinatura Digital, onde “... uma mensagem cifrada com a chave privada (somente) pode ser decifrada com o uso da chave pública correspondente”.

Ou seja, se uma mensagem ou documento cifrado pode ser decifrado a partir da uma chave pública de alguém, incontestavelmente foi cifrada a partir da chave privada desse alguém. Não haverá, portanto, como negar sua autoria(não-repudio).

Mas a Assinatura Digital requer outra nuance. O vínculo, também incontestável, ao documento a que a assinatura corresponde.

Para cumprir esta exigência se apresenta outra técnica, a função *hash*. Quando da cifragem de um documento, o *hash* cria um resumo aleatório do documento original, conhecido como resumo *hash*. Ao decifrá-lo deverá gerar novamente o mesmo valor de resumo *hash*. Se houver divergência, atestará que o documento assinado foi modificado.

Terceira parte confiável

Como afirmado anteriormente, a chave pública, como o próprio nome diz, deve ser divulgada publicamente. Este papel cabe à Autoridade Certificadora que emitiu o certificado vinculado à mesma. E é o conceito da terceira parte confiável que se apresenta como um dos principais atributos da Certificação Digital, pois permite a centralização e publicidade das chaves públicas de seus titulares.

E de nada adiantaria, se a terceira parte confiável (AC) não prezasse pela segurança de suas instalações e procedimentos.

Então, é muito pertinente o relato do Senhor Diretor-Presidente do ITI, Renato Martini:

“... o leitor mais desavisado deve por vezes pensar que os requisitos de segurança física e lógica exigidos na ICP-Brasil são demasiados”.

E a princípio, podem até parecer demasiados.

Mas o aprofundamento do tema leva a compreensão da sua afirmação. Pois a instituição da Certificação Digital sobrevive de sua credibilidade. Principalmente, por tratar-se de assunto inovador e de difícil compreensão para a maioria das pessoas.

Mas também, porque labora sobre um produto não palpável, diferentemente do papel, mais suscetível à degradação.

As exigências não são por demais, portanto.

Tem a rigidez na medida certa, proporcional à credibilidade que almeja.

REFERÊNCIAS

Certificados Digitais, Disponível em:<http://technet.microsoft.com/ptbr/library/cc728388(WS.10).asp>

Conrado Leiras Matos, Disponível em: <http://www.gta.ufrj.br/grad/01_2/smartcard/smartcard.html>, acessado 31/10/2011.

Instituto Nacional de Tecnologia da Informação(ITI) <http://www.iti.gov.br>

Luz, Clarissa P. da, **Centro de Certificação Digital – Construção, Administração e Manutenção,** Rio de Janeiro: Editora Ciência Moderna Ltda., 2008.

REINALDO FILHO, Demócrito.**A ICP-BRASIL e os poderes regulatórios do ITI e do CG**.**Boletim Jurídico**, Uberaba/MG, a. 4, no 151. Disponível em: <http://www.boletimjuridico.com.br/ doutrina/texto.asp?id=897> Acesso em: 8 nov.2011.

Silva, Luiz Gustavo Cordeiro da; Silva, Paulo Caetano da; Batista, Eduardo Mazza; Homolka, Herbert Otto; Aquino, Ivanilso Jose de Souza Júnior; Lima, Marcelo Ferreira de. **Certificação Digital – Conceitos e Aplicações**, Rio de Janeiro: Editora Ciência Moderna Ltda., 2008.

Supremo Tribunal Federal (Disponível em:<http://www.stf.jus.br/portal/ministro/verMinistro.asp?periodo=stf&id=177>em 12/11/2011)