UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANA
DEPARTAMENTO ACADÊMICO DE ELETRÔNICA
CURSO DE ESPECIALIZACÃO EM TELEINFORMÁTICA E REDES COMPUTADORES

SÉRGIO LUIZ DE CARVALHO

AUTORIDADES CERTIFICADORAS E SEGURANÇA NA ASSINATURA DIGITAL

MONOGRAFIA DE ESPECIALIZAÇÃO

CURITIBA
2014

SÉRGIO LUIZ DE CARVALHO

AUTORIDADES CERTIFICADORAS E SEGURANÇA NA ASSINATURA DIGITAL

Monografia apresentada como requisito parcial para obtenção do grau de Especialista em Teleinformática e Redes de Computadores, do Departamento Acadêmico de Eletrônica da Universidade Tecnológica Federal do Paraná.
Orientador: Prof. Dr. Armando Rech Filho

CURITIBA
2014

DEDICATÓRIA

Dedico esse trabalho a todos que de uma maneira ou de outra, contribuíram para que eu chegasse até aqui nos meus estudos e lado profissional. Também aos meus pais como forma de agradecimentos e prova de reconhecimento a todo o esforço realizado para minha formação.

AGRADECIMENTOS

Agradecemos aos nossos familiares e amigos que nos deram o apoio necessário durante todas as fases desse curso especialização e na realização deste trabalho. Também à Universidade Tecnológica Federal do Paraná e todos os professores que contribuíram para minha formação, em especial ao professor Dr. Walter Godoy Júnior e ao professor orientador Dr. Armando Rech Filho que gentilmente participou desse projeto. Também às pessoas que passaram pelas nossas vidas, pelas amizades tivemos oportunidades de conhecer, que em algum dia podemos nos reencontrar e desfrutar novamente de uma grande amizade.

EPÍGRAFE

“O primeiro passo em direção ao sucesso é o conhecimento.”

(Nicola Tesla)

RESUMO

CARVALHO, Sérgio Luiz de. **Autoridades Certificadoras e Segurança na Assinatura Digital**. 2014, 36f. Monografia (Especialização em Teleinformática e Redes de Computadores) – Universidade Tecnológica Federal do Paraná. Curitiba, 2014.

Este trabalho de pesquisa tem como finalidade apresentar o funcionamento e confiabilidade das autoridades certificadoras e segurança nas assinaturas digitais, de forma analisar as suas características principais e disseminar sobre o seu conhecimento, pois ainda atualmente é desconhecido por muitos estudantes e pessoas. A certificação digital é uma assinatura com validade jurídica que garante proteção às transações eletrônicas e outro serviço via Internet, permitindo que pessoas e empresas se identifiquem e assinem digitalmente de qualquer lugar do mundo com mais segurança e agilidade. Essa nova tecnologia que se utiliza de chaves criptográficas, refere-se a uma solução para aos problemas encontrados nas vulnerabilidades das informações passadas nas redes. Portanto, desse modo à certificação digital oferece um conjunto de mecanismos que dá a garantia das autenticações, confidencialidade e integridade dos dados proporcionando maior segurança aos usuários. Esta pesquisa foi realizada baseada em livros, sites e artigos bem como a troca de informações com profissionais especialistas na área de tecnologia.

Palavras-chave: Certificação Digital, Segurança, Criptografias, Vulnerabilidade, Tecnologia.

ABSTRACT

CARVALHO, Sérgio Luiz de. **Certification Authorities and Security for Digital Signatures.** 2014. 36f. Monografia (Especialização em Teleinformática e Redes de Computadores) - Universidade Tecnológica Federal do Paraná. Curitiba, 2014.

This research aims to present the operation and safety reliability of the certifying authorities in digital signatures, in order to analyze its main characteristics and disseminate knowledge; it is still currently unknown to many students and people. The certification is a digital signature with legal validity that ensures protection to electronic transactions and other services via the Internet, allowing people and businesses to identify and digitally sign anywhere in the world with more safety and agility. This new technology that makes use of encryption keys refers to a solution for the problems encountered in the vulnerabilities of the information flowing in the networks. So this way the digital certification provides a set of mechanisms to guarantee the endorsements of confidentiality and integrity of data providing greater security to users. This research was conducted based on books, websites and articles as well as the exchange of information with specialists in the area of technology.

Keywords: Digital Certification, Security, Encryptions, Vulnerability, Technology.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE SIGLAS

AC	Autoridades Certificadoras
AC-RAIZ	Autoridades Certificadoras de mais alto nível do ICP
ACT	Autoridade de Carimbo do Tempo
ANS	Agência Nacional de Saúde Suplementar
AR	Autoridade de Registro
CPF	Cadastro de Pessoa Física
CG	Comitê Gestor da ICP-Brasil
DPC	Declaração de Práticas de Certificação
ICP	Infra-estrutura de Chaves Publicas
ITI	Instituto de Tecnologia da Informação
IP	Internet Protocol
ISO	International Organization for Standardization
LAN	Local Area Network
LCR	Lista de Certificados Revogados
PEP	Prontuário Eletrônico de Paciente
PSS	Prestadora de Serviço de Suporte
PC	Política de Certificação
PCN	Plano de Continuidade do Negócio
PS	Política de Segurança
PIN	Personal Identificatio Number
PUK	PIN Unlock Key
PKI	Public Key Infraestructure
RNP	Rede Nacional de Ensino e Pesquisa
TCP	Transmission Control Protocol
TSIG	Transaction Signatures
TTL	Time To Live
UDP	User Datagram Protocol

SUMÁRIO

1. INTRODUÇÃO

Durante o início e as primeiras fases de sua existência as redes de computadores foram principalmente utilizadas por militares e universidades e tendo como propósito a finalidade de compartilhar trocas de mensagens, entre outros poucos recursos nessa época que permitia essa tecnologia. Sob estas condições de uso nas redes a segurança nunca precisou da necessidade de maiores cuidados, mas atualmente com crescimento de milhões de usuários na Internet há uma preocupação maior, pois geralmente muitos utilizam essas redes de modos e maneiras diferentes, tais como, por exemplo, operações bancárias, operações de comércio eletrônico o que tem tornado o acesso remoto às informações confidenciais comum. Portanto, com a crescente competitividade no mundo dos negócios e aumento nas redes, as empresas e pessoas buscam adequar-se aos avanços tecnológicos novos. Assim sendo, para resolver alguns dos problemas encontrados e enfrentados foi criada a certificação digital, que é um mecanismo cada vez mais utilizado para transmitir dados e informações que precisam uma maior segurança. É ideal a certificação porque evita que usuários mal intencionados busquem se passar por outro e tenham acesso às informações trocadas pelas partes, e também que haja ruptura ou alteração da informação, o certificado dá garantia da identificação das partes envolvidas.

> " O certificado digital é um documento eletrônico que identifica pessoas e empresas no mundo digital, comprovando sua identidade. Permite acessar serviços on-line e assinar documentos eletrônicos com possibilidade de certificação da autenticidade e da integridade ..." (CORDEIRO, 2008, P.07).

Vale ressaltar a importância da referência que diversas instituições têm estabelecido normas de sua aplicação na certificação digital, por exemplo, Supremo Tribunal Federal que se utiliza esse método para dar um maior andamento dos processos nos tribunais. Também a Receita Federal não considera mais documentos com validade jurídica, como no caso os documentos fiscais federais das prefeituras e de estados que não tiverem a autorização pelos certificados da ICP-Brasil. Essas atividades de reprodução e emissão de notas fiscais terão a definição de ser eletrônicas assim como livros fiscais juntamente com utilização da certificação digital.

O objetivo desta pesquisa é apresentar um referencial teórico capaz de proporcionar esclarecimentos sobre certificação digital disseminando a sua utilização, buscando resolver as dúvidas sobe seu funcionamento, ajudando assim os usuários a alcançarem um ambiente mais seguro.

São os objetivos específicos dessa pesquisa:

- Apresentar e avaliar as tecnologias empregadas e utilizadas pela ICP-Brasil no processo da certificação digital.
- Demonstrar as normas legais e aspectos jurídicos que validem os documentos dos certificados digitais.
- Verificar o funcionamento dos certificados digitais e detalhamento do carimbo do tempo.
- Citar alguns casos de uso de certificados digitais.

Esta pesquisa segue o método bibliográfico de natureza científica aplicada. Usa referenciais teóricos baseados em livros e profissionais especialistas. Também faz o uso cartilhas, revistas e manuais encontrados em sites de órgãos públicos, tais como ITI, Setores do Judiciário e Universidades. No que tange a questões de direito, referencia-se em medidas provisórias, Leis e regulamentos e normas vigentes. Para cumprir com os objetivos propostos: o trabalho está assim estruturado; o capítulo 2 descreve os princípios da criptografia; o capítulo 3 trata da certificação digital; o capítulo 4 descreve as estruturas de certificação digital; o último capítulo 5 mostra algumas práticas e procura dos certificados digitais.

2. CRIPTOGRAFIA

A palavra criptografia teve o surgimento nos radicais gregos *Kriptos* oculto e *grapho* escrita, é o nome dado à ciência ou arte de codificar mensagens usando uma fórmula, que também é utilizada depois para decodificar a mesma mensagem. Assim atualmente esta fórmula é chamada de algoritmo, desse modo a criptografia se tornou essencial para garantir a privacidade das comunicações e principalmente em redes de computadores privadas e públicas por onde circulam dados e informações pessoais de empresas, governos e outros. Existem basicamente dois tipos de criptografia utilizados que são a simétrica ou de chave privada, e a assimétrica ou chave pública, e principais características de cada uma são as seguintes:

2.1 CRIPTOGRAFIA SIMÉTRICA

São do modo mais antigo, em que a chave é o elemento que fornece o acesso à mensagem oculta trocada entre duas partes, sendo igual simetria para ambas as partes envolvidas e deve permanecer em segredo absoluto. Basicamente essa chave tem a características de ser representada por uma senha, usada tanto pela pessoa que é remetente para codificar a mensagem numa ponta e como da outra pessoa que é o destinatário para decodificá-lo no outro lado.

> “ Criptografia de chave secreta também e chamado, usa uma chave secreta para criptografar uma mensagem de texto cifrado e a mesma chave para decifrar o texto cifrado em texto pleno...”(CORDEIRO, 2008, P.17).

As principais vantagens desta fórmula são a facilidade de operação e uso e a rapidez com que executam os seus processos criptográficos. A desvantagem dela é que a senha precisa ser compartilhada por duas ou mais pessoas envolvidas, e durante a esse processo de compartilhamento a senha pode ser interceptada e fica vulnerável. Qualquer terceiro em que tiver acesso à senha poderá descobrir o conteúdo secreto dessa mensagem. A figura 1 logo abaixo mostra o modelo de codificação e decodificação da chave simétrica.

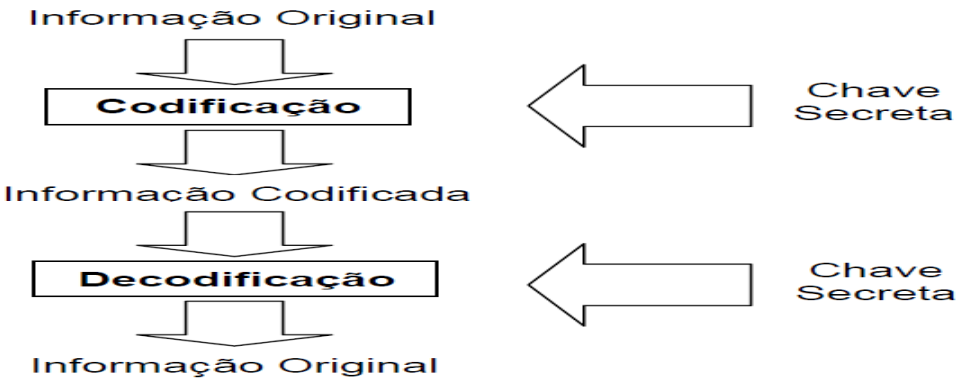


Figura 01: Uso da Criptografia Simétrica.

Fonte: Cert (2014).

2.2 CRIPTOGRAFIA ASSIMÉTRICA

São do tipo surgido na década de 1970, a qual faz parte de um algoritmo de criptografia que no processo de segurança funciona usando duas chaves diferentes assimétricas e complementares, uma privada e outra pública. Assim sendo, nessa nova fórmula as chaves não são apenas senhas, mas arquivos digitais muito mais abrangentes e complexos que eventualmente são associados a uma senha. Basicamente a chave pública fica disponível para qualquer pessoa que queira se comunicar com outra de modo muito mais seguro, mas a chave secreta deverá ficar em poder só apenas do titular. É com a chave privada que a pessoa destinatária poderá decodificar a sua mensagem que foi processada na criptografia para ele com sua respectiva chave pública. Para entender melhor, por exemplo, basta pensar num cadeado normal e comum que resguarda um determinado bem da pessoa, onde cadeado que fica exposto é a chave pública, e apenas a pessoa que tiver uma chave particular, a privada, conseguira abrir o seu cadeado assim poderá acessar sua mensagem. A figura 2 logo abaixo chamada mostra o modelo de codificação e decodificação da chave assimétrica.

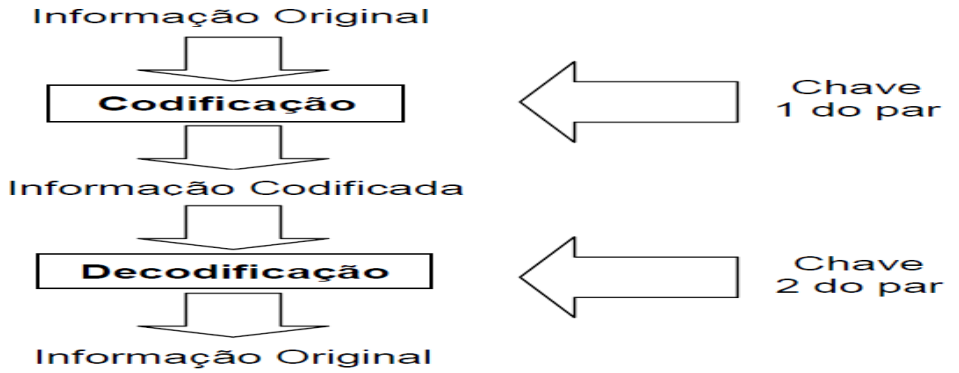


Figura 02: Uso da Criptografia Assimétrica.

Fonte: Cert (2014).

A principal vantagem desta fórmula é sua grande segurança, pois não é preciso e nem se deve compartilhar a chave privada, sobre a qual o dono deve manter segredo absoluto. Por outro lado, o tempo dessa operação de processamento de mensagem com a criptografia assimétrica é muita vez maior do que a criptografia simétrica, isso pode limitar e reduzir o seu uso em determinadas situações cotidianas.

2.3 ASSINATURA DIGITAL

A assinatura digital é um código associado a uma mensagem eletrônica que permite demonstrar de forma única e exclusiva a comprovação da autoria de um determinado número de conjuntos de dados. Essa assinatura comprova que a pessoa criou ou concorda com o documento assinado digitalmente, seria como ela tivesse feito de próprio punho e comprova a autoria de um documento escrito. Essa verificação da origem dos dados e informações é feita com a chave da pessoa que é remetente.

A fórmula para autenticação dos algoritmos de criptografia de chave pública é usado em conjunto com uma função, também conhecida como *hash* e segundo Costa (2006), o *hash* é o resultado da ação de algoritmos que fazem o mapeamento de uma seqüência de bits de tamanho fixo menor conhecido como resultado *hash.* E muito difícil encontrar duas mensagens produzindo o mesmo resultado, e que o processo reverso também não seja realizável, ou seja dado um *hash* não é possível recuperar a mensagem que gerou. A figura 3 mostra esse modelo.

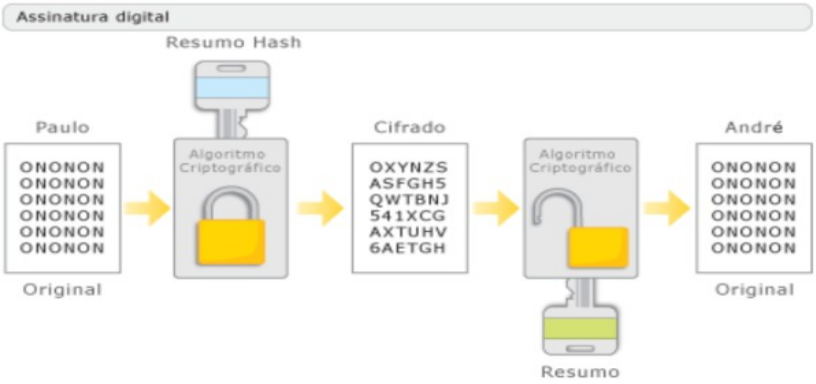


Figura 03: Detalhe da Assinatura Digital usando *Hash*.

Fonte: Cert (2014).

2.4 CRIPTOGRAFIA X.509

Os algoritmos criptográficos viabilizam o comércio eletrônico tendo disponibilidade, sigilo, controle de acesso, autenticidade e integridade sendo parte da sua funcionalidade a capacidade de gerenciamento e segurança. E existem no mercado diversos tipos, como tais “PGP”, ”SPDK/SDSI”, ”SET” entre outros, entretanto o ICP-Brasil adota o padrão “X.509 V3”.

O X.509 V3 é um padrão utilizado e recomendado pela “ITU-T”, para infra-estruturas de chaves públicas “ICP”, que especifica o formato dos certificados digitais, de tal maneira que possa proteger firmemente um nome a uma chave pública, permitindo autenticação muito forte. Assim sendo faz parte da série X.500 de recomendações para uma estrutura global, baseada em nomes distintos para localização, utilizado pelo “S/MINE”, “IPSEC”, “SSL/TLS” e “SET”, baseado em criptografia com chave pública “RSA” assinatura digital com *hashing*. Logo abaixo, quadro 1 mostra o seu formato.

Nome do Campo	Descrição
Versão	Número da Versão X.509 do certificado, tendo como valor válido apenas 1, 2 ou 3.
Número de Série	Identificador do Certificado é representado por um numero inteiro. Não deve haver o mesmo número emitido de série por uma mesma Autoridade Certificadora.
Algoritmo de Assinatura	Identificador do algoritmo usado para a Assinatura do Certificado pela Autoridade Certificadora.
Emissor	Nome da Autoridade Certificadora que produziu e assinou o Certificado.
Tempo de validade	Duração que determina quando um certificado deve ser considerado válido.
Assunto	Identifica o dono da chave pública do certificado. O assunto deve ser único para cada assunto no certificado emitido por uma autoridade certificadora
Chave Pública	Contém o valor da chave pública do certificado junto com informações de algoritmos com o qual a chave deve ser usada.
Identificador Único de Emissor “Opcional”	Campo para permitir o reuso de um emissor com o tempo.
Identificador Único de Assunto “Opcional”	Campo para permitir o reuso de um assunto com o tempo
Extensão “Opcional”	Campos complementares com informações adicionais.

Quadro 01: Descrição do Formato X.509 V3.

Fonte: ITI (2014).

3. CERTIFICAÇÃO DIGITAL

De acordo com a ICP-Brasil (2014), existe uma infra-estrutura para emissão dos certificados digitais, e a autoridade de certificadora raiz brasileira é a principal no compromisso de normas e gerenciamento de geração dos pares de chaves criptográficas e certificados. Também possui atribuições como emissão, expedição e distribuição de certificados para as autoridades certificadoras de nível mais baixo. Um certificado digital é usado para ligar uma entidade a uma chave pública e privada, e no caso de uma infra-estrutura de chaves públicas “ICP”, o certificado é assinado pela autoridade certificadora “AC”, que emitiu no caso chamando de um modelo de teia de confiança. O certificado é assinado pela própria entidade e assinado por outros que confiam naquela entidade. Em ambos os casos as assinaturas contidas e registradas em um certificado são atestados feitos por uma entidade que forma uma confiança nos dados e informações sejam contidas naquele certificado. Logo abaixo a figura 4 mostra mais detalhe da hierarquia.

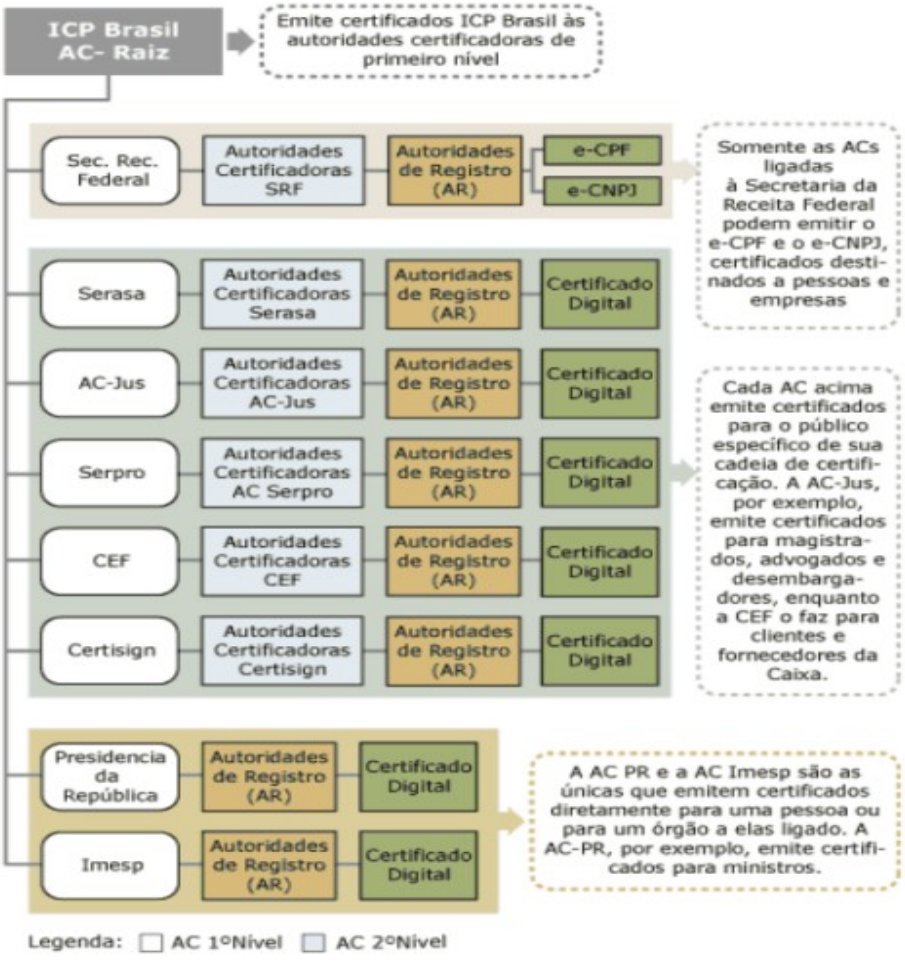


Figura 04: Detalhe da Estrutura da Hierarquia “AC” Brasileira.

Fonte: ICP-Brasil (2014).

Para garantia de seu funcionamento uma autoridade certificadora “AC” deve cumprir certas normas estabelecidas segundo ICP-Brasil (2014), o que é igual ao que ocorre no mundo tradicional.

Por exemplo, uma empresa que vende parcelado aceita alguns determinados documentos para identificar o comprador antes de efetuar a venda do produto. Estes documentos sempre são emitidos pela Secretaria de Segurança de cada estado e pela Secretaria da Receita Federal no caso o “RG” e o “CPF”. Assim, existe uma relação de confiança estabelecida com esses órgãos, da mesma forma os usuários podem escolher uma “AC” a qual for mais conveniente para confiar na emissão de seus certificados digitais. Para a emissão dos certificados as autoridades certificadoras possuem deveres e obrigações que são expostos em um documento público chamado de Declaração de Práticas de Certificação “DPC”, e entre as atividades da “AC” o mais importantes é verificar informações da identidade da pessoa titular. Quanto melhor definidos e mais detalhados e abrangentes os procedimentos adotados por uma “AC” maior será sua confiabilidade. O Comitê Gestor da ICP-Brasil, é o órgão governamental que especifica todos os procedimentos que devem ser adotados pelas “AC”. Elas se, submetem às normas e resoluções do Comitê Gestor, quanto ao cumprimento dos processos e procedimentos, que são fiscalizados, por exemplo, exame de documentos, instalação técnicas, também o pessoal especializado. Se alguma dessas regras for irregular poderá ter aplicações de penalidades e multas, que podem ocorrer no caso até o descredenciamento. Logo abaixo a figura 5 mostra seu funcionamento.

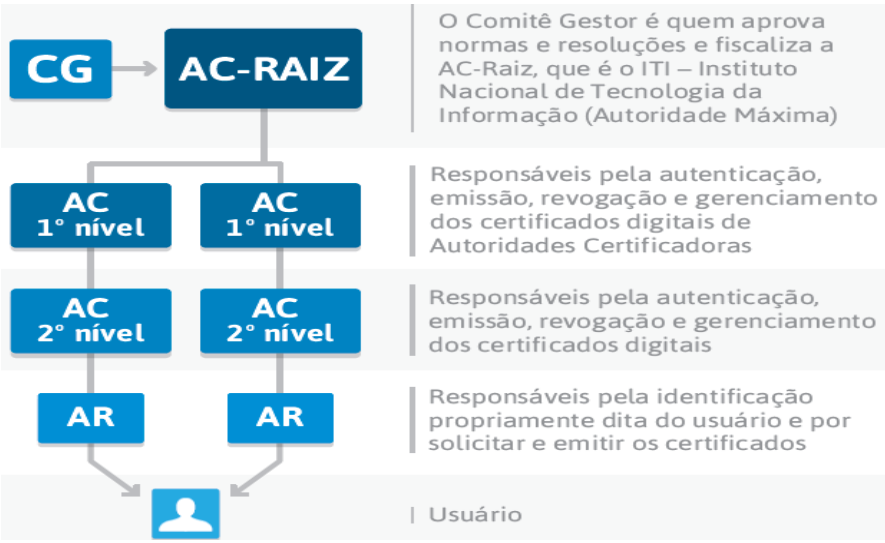


Figura 05: Funcionamento da Autoridade Certificadora até aos Usuários.

Fonte: ITI (2014).

Conforme é mostrado, as entidades certificadoras, para se tornarem parte dessa cadeia de confiança elas passam por um grande processo de credenciamento exigente, o qual estabelece diversas obrigações e procedimentos, normas e técnicas para o seu funcionamento nessa atividade,

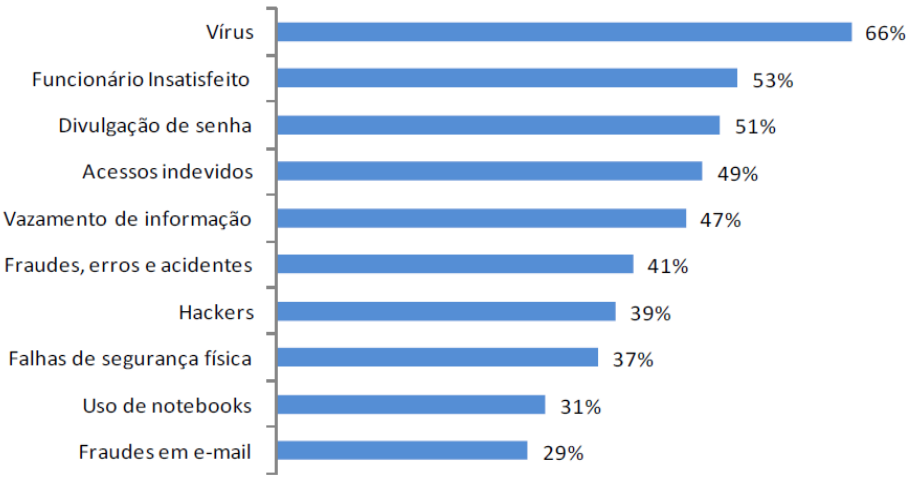
onde cada entidade exerce funções específicas. Logo abaixo segue mais detalhamento segundo ITI (2014):

- Comitê Gestor “CG”: responsável pelo controle e aplicação das políticas e procedimentos e normas e técnicas;
- Autoridade Certificadora Raiz “AC-Raiz”: responsável por todo o comando de execução, fiscalização e administração, logo está no topo da hierarquia;
- Autoridades Certificadoras ”AC”: estão subordinada à AC-Raiz, e são incumbidas de organizar e gerenciar os certificados como emitir, revogar, a um nível inferior;
- Autoridades de Registro “AR”: são responsáveis pelo gerenciamento operacional entre o solicitante e as Autoridades Certificadoras;
- Prestador de Serviços de Suporte “PSS”: são contratados pelas Autoridades Certificadoras ou Autoridades de Registro para disponibilização de recursos físicos, lógicos e especializados;
- Auditorias Independentes: são contratadas pela Autoridade Certificadoras Raiz para realizarem inspeções operacionais, técnicas, lógicas nas organizações de nível inferior ao dela;
- Titulares de Certificados: são os solicitantes da certificação digital, estão relacionados diretamente com as Autoridades de Registro;

3.1 PREOCUPAÇÃO COM A SEGURANÇA DA INFORMAÇÃO

Conforme está relacionada com a política de segurança da informação segundo o pesquisador Martinez (2012), pode-se considerar informação o conteúdo de dados que some valor para um indivíduo ou organização e que poderá ser de uso restrito ou público. Para garantir a segurança da informação, um sistema deve possuir, obrigatoriamente, capacidade de confidencial idade, assegurando que apenas quem for autorizado terá acesso aos dados, integridade, garantindo e veracidade dos dados; disponibilidade, para que sempre esteja acessível aos membros autorizados pelo proprietário da informação. Contudo, antigamente muito tempo atrás empresas, governos e pessoas utilizavam diversos recursos no caso assinaturas às canetas, carimbos e selos para comprovar não serem falsos os seus documentos emitidos, isso dava a expressar a concordância em registrar em declaração as sua autenticidade, mas isso gastava muito tempo e dinheiro nessa burocracia. Para solucionar essa situação buscou-se o meio virtual, que está relacionado a essa nova tecnologia na certificação digital, uma maneira mais rápida e precisa. Assim sendo, nesse exemplo

na seguinte suposição, uma pessoa está numa viagem de negócios e precisa enviar diversos documentos sigilosos à matriz de sua empresa ou governo, e por ser muito distante local o jeito mais tranqüilo mais rápido de fazer isso é utilizando o meio on-line. Entretanto, se a pessoa fizer a escolha de enviar todos os documentos em papel, provavelmente os faria com o uso de carimbos e assinaria à caneta para comprovar a originalidade e autenticidade e dando a sua responsabilidade sobre eles. Certamente utilizaria um serviço de entrega postal de sua confiança pessoal e o instruiria a deixar apenas com a pessoa responsável do destino, mais isso gastaria muito tempo e podendo acontecer algo errado com entrega. Mas também como colocar medidas práticas de segurança de documentos, se pessoa digitalizar a sua assinatura por meio de um aparelho de “Scanner” não seria um procedimento muito bom se realizar, porque qualquer um pode alterá-la em simples programa de edição de imagem e enviando esses documentos sem proteção via e-mail, igualmente teria seus riscos. Segundo Menezes (2006), a espionagem empresarial e a contra-espionagem começam, portanto a desenvolver diferentes mecanismos de proteção para o tráfego de informações, criando consequentemente um ambiente mais seguro com alto grau de entropia. No quadro 2 abaixo estão relacionadas as várias ameaças à segurança da informação atualmente.



Quadro 02: Principais Ameaças a Segurança da Informação

Fonte: Menezes (2006).

3.2 CONFERÊNCIA DAS ASSINATURAS

A certificação digital traz diversas facilidades e conforto. A assinatura manuscrita é muito complicada, pois se restringe ao modelo de atribuição de autoria a um determinado documento. No caso da manuscrita as assinaturas possuem um padrão igual e possuindo características pessoais próprias e biométricas de cada indivíduo, sendo feita de algo visível e tangível no papel responsável à relação das informações que estão impressas no papel a essa assinatura. A autenticidade da

assinatura é feita por base em uma comparação visual a uma assinatura verdadeira tal como aquela da identidade no documento original e oficial registrado. Nos documentos eletrônicos é diferente, pois não existe uma forma simples de estabelecer e aproximar o documento com a assinatura física, onde a representação eletrônica e feita por meio de uma seqüência de bits um e zeros, e essa assinatura gerada é diferente para cada documento.

No momento o governo brasileiro criou e estabeleceu e está relacionada aos aspectos legais a medida provisória numero 2.200-2, de 24 de agosto de 2001 que define as regras para criação da ICP-Brasil, associada à utilização de certificados digitais no Brasil, procedimentos legais e necessários para criação de uma entidade e se tornar uma “AC” intermediária e assim poder emitir certificados digitais para outras entidades garantindo sua autenticidade e integridade. A Lei número 11.419 de 19 dezembro de 2006 fundamenta os processos judiciais eletrônicos no Brasil, dando validade jurídica aos trâmites eletrônicos por essas entidades realizados.

3.2.1 Quais são as Vantagem e Aplicações da Certificação Digital

As principais vantagens da certificação digital é que permite grande agilidade, redução de custos, dá maior controle e segurança, logo beneficia diversos segmentos e setores da economia na nossa sociedade. O uso dessa tecnologia facilita as obrigações cotidianas dentre as vantagens pode-se citar segundo ITI (2014):

- Dispensa o reconhecimento de firma em cartório;
- Redução de custos, redução no volume de papéis da burocracia.
- Aumenta credibilidade digital das partes envolvidas;
- Atribui validade jurídica a documentos eletrônicos;
- Contribuintes podem acessar informações junto aos órgãos públicos permitindo que realize cópias de documentos, consiga segunda via de impostos entre muitas outras;
- Redução nas filas bancos, repartições públicas e outras áreas.
- Acompanhamento de processos jurídicos on-line;
- É ecologicamente mais correto para economia e sustentabilidade;
- Dá autenticidade digital;
- Evita fraudes digitais ocasionadas por terceiros;

3.2.2 Utilidades do Certificado Digital

As principais formas de utilização do certificado digital são de várias possibilidades, dependendo muito da área de atuação da pessoa que vai utilizar e de certa forma onde ela trabalha em algum determinado setor, mas para maior entendimento de seu funcionamento observa-se no caso, no site da Receita Federal do Brasil que permite e disponibiliza diversos serviços on-line sendo protegidos por sigilo fiscal. Pode-se citar segundo a Receita Federal:

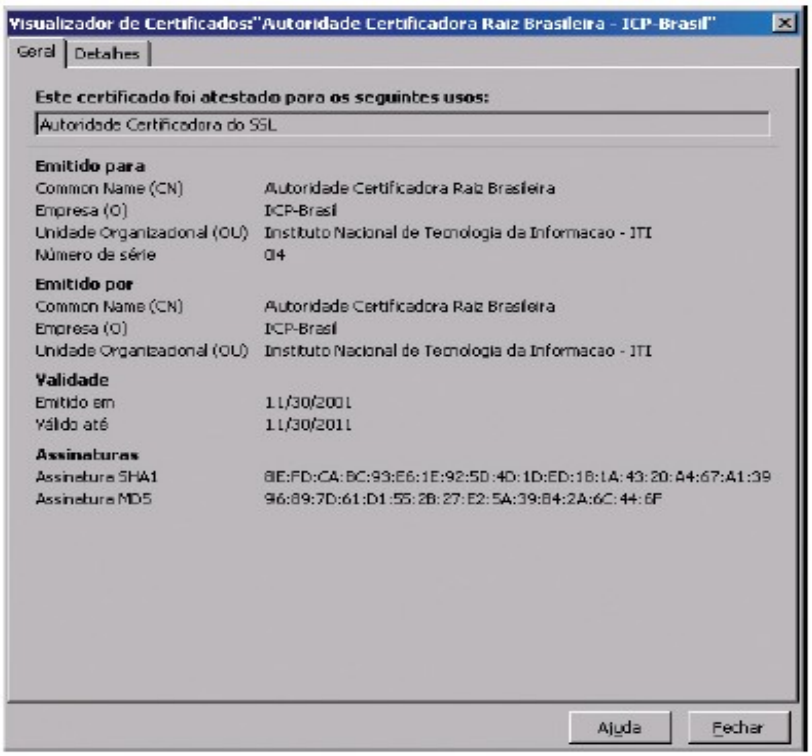
- O “e-CPF” é o certificado digital destinado à pessoa física, a qual poderá realizar serviços, assinar e autenticar; é utilizado pela Receita Federal do Brasil;
- O “e-CNPJ” é o certificado específico para pessoa jurídica, onde empresa solicita e pode realizar serviços on-line, assinar e autenticar de forma digital;
- Permitem a pesquisa detalhada de sua situação fiscal no momento, permitindo verificar pendências, irregularidades problemas e outras;
- Consulta e emissão do comprovante de inscrição do “CNPJ” da empresa;
- Consulta de parcelamentos de débitos;
- Permite obter cópias de declarações dos últimos anos de exercícios;
- Pode inscrever alterar e consultar a matrícula do “CEI”, cadastro específico do “INSS”;
- Envio de E-mail autêntico que comprova que foi a própria pessoa quem enviou, através de algum programa de E-mail preferencial da pessoa, que deseja adicionar a assinatura;
- Disponibiliza ao usuário imprimir cópia das informações de rendimentos;
- Responsáveis de empresas que possuem “e-CPF” podem operar o sistema “SISCOMEX”, obrigatório para empresas que desejam importar e ou exportar;
- Consultar quais empresas a pessoa é sócia ou acionista e quais empresas já participou como sócio e ou acionista;
- Consultar valores informados por outras empresas, fontes pagadoras para a Pessoa Jurídica;
- Transações bancárias em meios eletrônicos, com alto nível de segurança e maior proteção para o correntista no acesso aos mais variados serviços;
- Consultar todas as declarações como, “DIPJ”, “DSPJ”, ”DCTF”, “DACON” e” DIRF”;
- Fornecer Procuração eletrônica ao contador ou terceiros, possuidores de certificado digital o “e-CPF” ou “e-CNPJ”;
- Receber mensagens enviadas pela Receita Federal, através de ambiente seguro, inclusive e-mails com informações diárias de mudanças na legislação Tributária;

4. ESTRUTURA DE CERTIFICAÇÃO DIGITAL

De acordo com Serasa Experian (2014), o certificado digital é um documento eletrônico que garante proteção às transações on-line e à troca virtual de documentos, mensagens e dados, com validade jurídica. Com este dispositivo, os sistemas de informação podem validar e reforçar os mecanismos de segurança on-line, utilizando a tecnologia para garantir a privacidade e confirmar a autenticidade das informações dos usuários, empresas e instituições na rede. O certificado digital cumpre a função de relacionar uma pessoa a uma chave publica. Um certificado apresenta seguintes as informações necessárias:

- Nome da pessoa ou entidade a ser associada à chave pública.
- Período da validade do certificado.
- Chave pública.
- Nome e assinatura da entidade que assinou o certificado.
- Numero de série.

O quadro 3 mostra detalhes do certificado digital.



Quadro 03: Detalhes do Certificado Digital ICP-Brasil.

Fonte: ITI (2014).

4.1 TIPOS DE CERTIFICADOS DIGITAIS

Basicamente são disponibilizados os certificados digitais previstos pela ICP-Brasil que está no topo da hierarquia, que tem as condições e disponibilidade para manter a sua classificação atual conforme as particularidades, e também quanto aos seus requisitos de segurança e de proteção da chave privativa. São apresentados os certificados com as seguintes opções e tipos:

- Os certificados do tipo “A” são certificados digitais utilizados para a assinatura de documentos, transações eletrônicas; etc. Têm como meta provar a autenticidade e autoria por parte do emissor o autor, garantindo também a integridade do documento.
- Os certificados do tipo “S” são utilizados somente para proporcionar sigilo ou criptografia de dados. São os certificados digitais utilizados para o envio e ou armazenamento destes documentos sem expor o seu conteúdo.
- Também conhecido como time-stamping “T”, é o serviço de certificação da hora e do dia em que foi assinado um documento eletrônico, com identidade do autor. A figura 6 logo abaixo mostra os tipos de certificados.

Figura 06: Os Tipos de Certificados.

Fonte: ITI (2014).

Para a escolha do certificado deve-se saber qual será finalidade e o uso, o que se deseja fazer e qual a área de atuação da solicitante, pois isso depende muito das necessidades do cliente. Seguem os passos básicos da escolha e do seu funcionamento. Logo abaixo na figura 7 mostra-se como obter um certificado.

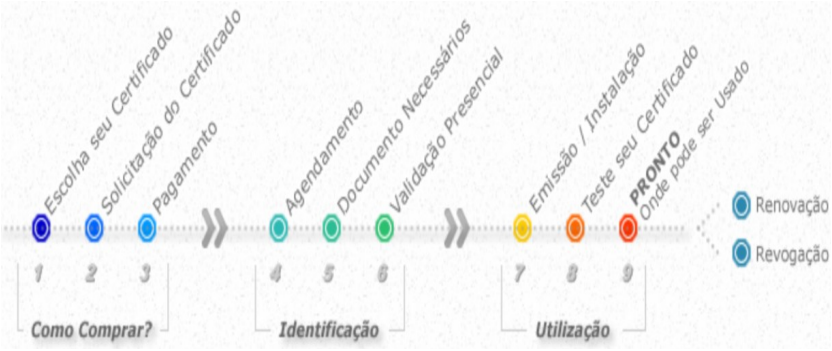


Figura 07: Passos para obter o Certificado.

Fonte: Certising (2014).

Existe na ICP-Brasil descrição dos certificados com os tipos previstos que são série A1, A2, A3 e A4, com grau de crescente de segurança que está relacionada à tecnologia utilizada da modalidade de armazenamento e força criptográfica. As da série S1, S2, S3 e S4 reúnem os certificados de sigilo que são utilizados na codificação de vários documentos, de bases de dados e mensagens e de outras informações eletrônicas sigilosas, e todos são diferenciados pelos tipos de nível de segurança e validade de tempo previsto. O quadro 4 mostra os tipos de certificados.

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

Quadro 04: Funcionamento de Tipos Certificados.

Fonte: ICP-Brasil (2014).

Para conhecimento melhor segue a descrição e os termos dos certificados, de acordo com glossário ICP-Brasil, utilizados na versão 1.2, de 03/10/2007.

- O tipo A1 e S1, são os certificados em que a geração de chaves criptográficas é feita por software e seu armazenamento pode ser feito em hardware ou repositório protegido por senha cifrado por software, a sua validade no máximo é de um ano somente. Sendo freqüência de publicação da lista de certificados revogados “LCR” no máximo 48 horas e no máximo admitido para conclusão do processo de revogação 72 horas.
- O tipo A2 e S2, são os certificados em que a geração das chaves criptográficas é feita em software e as mesmas são armazenadas em um cartão inteligente ou *token*, ambos sem capacidade de geração de chaves e protegidos por senha, tem a validade de dois anos. “As chaves criptográficas tem no mínimo 1024 bits, sendo a freqüência da publicação da lista de certificados revogados” no máximo de 36 horas e o prazo máximo admitido para conclusão do processo de revogação é de 54 horas.

- O tipo A3 e S3, são os certificados em que a geração e o armazenamento das chaves criptográficas são feitos em cartão inteligente ou *token*, ambos com a capacidade de geração de chaves e protegidos por senha, ou hardware criptográfico aprovado pela ICP-Brasil, as chaves têm no mínimo de 1024 bits a validade de três anos. Sendo a freqüência de publicação da lista de certificados revogados “LCR” de no máximo de 24 horas e o prazo máximo admitido para conclusão do processo de revogação 36 horas.
- O tipo A4 e S4, são os certificados em que a geração e o armazenamento das chaves criptográficas são feitos em cartão inteligente ou *token*, ambos com a capacidade de geração de chaves e protegidos por senha, ou hardware criptográfico aprovado pela ICP-Brasil, as chaves têm no mínimo 2048 bits, com validade máxima do certificado é de três anos. Sendo a frequência de publicação da “LCR” no máximo de 12 horas e o prazo admitido para conclusão do processo de revogação 18 horas.

As mídias ou hardware criptográficos mais utilizados para certificados segundo ITI (2014):

O *Smart Card* é um tipo de cartão plástico semelhante a um cartão de crédito com um ou mais micro chips embutidos, capaz de armazenar e processar dados. O *Smart Car*d pode ser programado para desempenhar inúmeras funções, inclusive pode ter capacidade de gerar novas chaves públicas e privadas e de armazenar certificados digitais e pode ser utilizado tanto para o controle de acesso lógico como para controle de acesso físico.

O *Token* é um hardware para o armazenamento do certificado digital de forma muito segura, sendo parecido com o do *Smart Card* e a grande diferença é que ele possui conexão com o computador em via de USB e o *Smart Card* necessita de uma leitora. A figura 8 mostra mídias de segurança.

Figura 08: Mídias de Segurança, *Token* e *Smart Card*.

Fonte: ITI (2014).

4.2 TEMPO DE VALIDADE E REVOGAÇÃO

O ciclo de tempo do certificado digital é diferente dos documentos tradicionais pessoais, segundo ICP-Brasil (2014), no caso ele possui um período de prazo de validade homologado, entretanto, é só reconhecido assinar um documento enquanto estiverem válidos, e as assinaturas não serão aprovadas após o certificado expirar ou finalizar. Quando o certificado for revogado antes do tempo definido para terminar, a solicitação deve ser encaminhada à “AC” que produziu o certificado. As justificativas do solicitante podem ser relacionadas a vários fatores como insegurança da chave privada, alterações de informações dos dados do certificado ou qualquer outro motivo e acontecimento. Assim a “AC” recebe a solicitação e verifica o pedido, adiciona o número de série do certificado a uma lista chamada de certificados revogados “LCR” e a publica periodicamente.

As publicações das “LCR” são mencionadas na declaração de práticas de certificação “DPC” que produziu o certificado, normalmente o certificado possui um campo com um apontador para um endereço funcionando na Internet que relata e contém o arquivo com a ”LCR”; essas publicações são feitas a cada período de tempo seguindo padrão ”AC” a definido na programação.

Estas listas podem ser consultadas, e verificado se um certificado permanece válido ou deixou de funcionar. Após a revogação ou expiração do certificado, todas as novas assinaturas tornam-se inválidas, mas cada documento possui um carimbo de tempo onde é adicionada a hora e data específica que determina em qual o período o documento foi assinado. Assim, um documento assinado dentro do período de validade do certificado continua válido ao longo da sua existência. A figura 9 mostra a linha de tempo do certificado.

Figura 09: Linha de Tempo do Certificado.

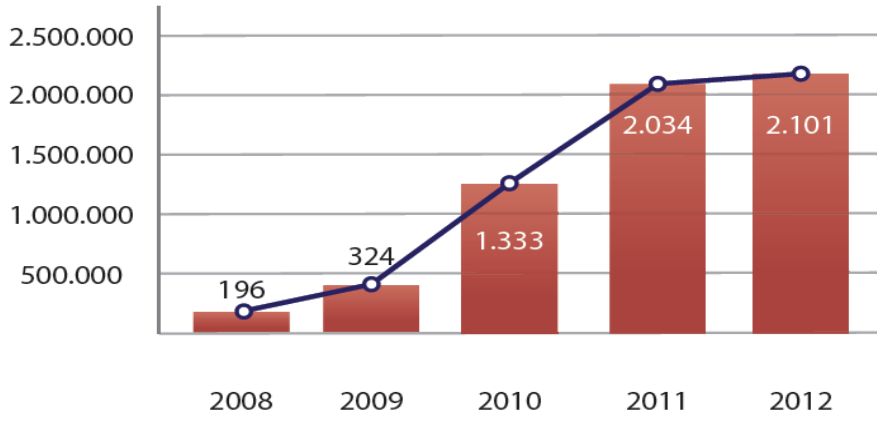
Fonte: ITI (2014).

5. INDICADORES DE USO CERTIFICADO DIGITAL

Agora nesse capítulo, demonstra-se o crescimento da certificação digital no Brasil, e o aumento de sua procura confirmando um grande mercado.

5.1 EXPANSÃO DO MERCADO DE CERTIFICAÇÃO

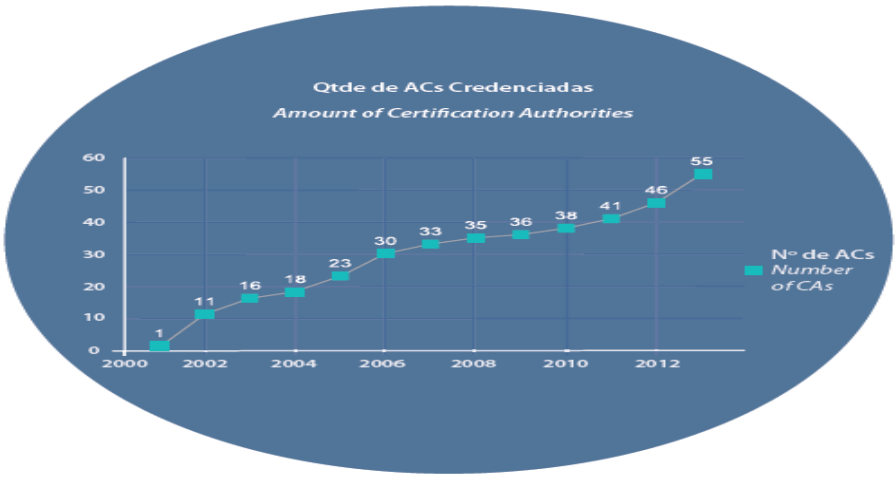
A avaliação das estatísticas dos indicadores da utilização e da quantidade de certificados digitais vem mostrando um grande aumento a cada dia, segundo o sistema nacional brasileiro a ICP-Brasil, em 2012 atingiu o marco de mais de dois milhões de certificados digitais emitidos exatos 2.101.377. Ainda de acordo com assessor técnico da auditoria e fiscalização ITI Alexandre Menezes Ribeiro o uso por pessoas jurídicas foi de o que 76%, ainda é predominante em comparação às pessoas físicas. A futura aprovação da Proposta de Emenda Constitucional "PEC" que autoriza o recolhimento de assinaturas com certificação digital pela Internet para projetos de Lei de iniciativa popular também causará aumento do uso dessa tecnologia. O assessor destaca ainda que a utilização de dispositivos móveis como *Tables* e *Smartphones* impulsionarão o uso da certificação digital pelas pessoas. Ribeiro diz que a entrada de novas "AC" e "AR" no mercado deverá estimular a concorrência de mercado e, consequentemente baixar o preço do certificado digital. O quadro 5 logo abaixo mostra o crescimento dos certificados emitidos por ano Brasil.



Quadro 05: Crescimento dos Certificados Emitidos por Ano.

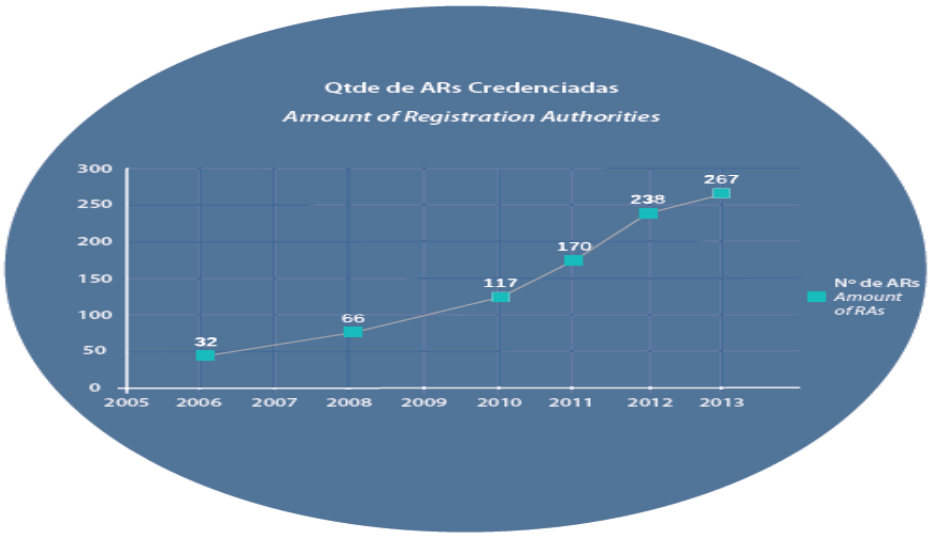
Fonte: ITI (2014).

Tratando-se de números e indicadores no passado, segundo o pesquisador Wilson Hirata em seu artigo “Desafios da ICP-Brasil” Hirata (2013), após completados 11 anos de implementação, a infra-estrutura de chaves brasileiras atingiu um aumento superior a 180%, indo de 16 autoridades certificadoras “AC” credenciadas para 46 em 2012. Em quantidade de autoridade de registro “AR”, nos últimos quatro anos, a ICP-Brasil apresenta um aumento superior a 260%, indo de 66 em 2008 para 238 “AR” em 2012. Atualmente a certificação digital passa por uma grande fase de expansão mercado no consumidor, assim a sua aceitação faz por parte dessa novidade de inovação tecnológica. Logo abaixo nos quadros 6 e 7 mostra o aumento das “AC” e “AR” credenciadas.



Quadro 06: Aumento ao Logo dos Anos “AC” Credenciadas.

Fonte: ITI (2014).



Quadro 07: Quantidade de Autoridade de Registro “AR” Credenciadas.

Fonte: ITI (2014).

Outros exemplos do uso certificado digital serão implantados e atribuídos na identificação da carteira estudantil, onde esse modelo estará mais protegido e terá vantagem importante, pois a pessoa ligada à instituição terá seus direitos garantidos para seu uso particular, e logo que pessoa deixar essa instituição de estudo perderá esse benefício automaticamente, e não será mais de uso de falsificação por terceiros.

Outro bom uso é na área hospitalar, uma situação na qual o médico dispõe de todas as informações prévias do paciente no ato da consulta no prontuário eletrônico do paciente “PEP”, tratando-se de um modelo assinado digital, que representa um grande avanço nessa atividade profissional. O “PEP” é mais seguro que o prontuário de papel e suas informações podem ser compartilhadas com outros médicos, mesmo de outros hospitais, onde está sempre atualizada, e indicando quem foi o último médico alterar os dados do paciente, logo a possibilidade de erro é reduzida trazendo uma maior agilidade. Dessa forma, também os atentados médicos estarão mais protegidos contra fraudes e manipulação. A Agência Nacional de Saúde Suplementar “ANS” estabeleceu um padrão de troca e informações para registros de dados e intercâmbio, onde as prestadoras de serviços de saúde e operadoras de planos de saúde são obrigadas repassar os dados imediatamente para o sistema.

Um exemplo prático é avanço tecnológico pelo quais os Tabelionatos de Notas estão participando, pois estão disponibilizado a seus clientes físicos e jurídicos, serviços utilizando certificados digitais, podendo possibilitar diversos serviços com segurança, legalidade e a exclusiva chancela notarial. O procedimento muito semelhante ao que todos conhecem no balcão dos cartórios, ou seja, o usuário terá em mãos uma cópia autenticada sem a retenção das informações pelo referido cartório. O custo sempre é mais baixo e depende da certidão e processo que o usuário pedira requisita no cartório digital, tudo isso é realizado através do certificado digital que protege todas essas fases.

CONCLUSÃO

Esta pesquisa pode verificar e analisar que a certificação digital é uma realidade atual positiva, pois a rede de computadores tem como objetivo atrativo decisivo a possibilidade de relação e interação a fim de facilitar o acesso às comunicações e informações seja em uma rede privada ou pública. Desse modo, a tendência é que seu crescimento se torne maior e seja comum para todas as pessoas, e que um pouco mais no futuro todas terão um certificado digital em seu registro de nome, motivo que a segurança é uma preocupação de todos sejam elas físicas ou jurídicas.

Com o resultado desse trabalho conclui-se que o mercado de autoridades certificadoras é bastante promissor, pois fundamenta a necessidade de ter um mecanismo para a segurança brasileira e global muito importante sendo igual ao mundo tradicional. Na era da tecnologia da informação atualmente, são encontrados e descobertos diversos problemas e vulnerabilidades nesse ambiente virtual o que possibilita várias pessoas mal intencionadas a terem vantagens ilícitas e de cometer erros e condutas fazendo a causar danos consideráveis e prejuízos às suas vítimas e a outras pessoas também. Assim sendo, é essencial buscar uma determinada solução, desse modo à certificação digital desempenha um grande papel de forma a beneficiar e a favorecer os seus usuários, pois segundo a ICP-Brasil, a certificação é uma identidade no meio eletrônico, que permite realizar diversos serviços na esfera digital, com validade jurídica, agilidade, facilidade de acesso e substancial redução de custos.

Portanto, a presente pesquisa foi de grande importância já que permitiu dar esclarecimento e conhecimento maior a respeito desse assunto, mas certificação digital não é uma solução milagrosa, pois existem sempre novas ameaças relacionadas à insegurança relativa aos sistemas e nas redes virtuais, nas quais o certificado digital é um componente valioso e obrigatório na segurança todos atualmente. Buscando influenciar para melhor conhecimento para essa nova condição de segurança, como sugestão de pesquisas futuras, sugere-se um estudo mais aprofundado sobre esse tema, por exemplo, segurança na criptografia quântica.

REFERÊNCIAS BIBLIOGRÁFICAS

AQUINO, J.; CORDEIRO L. G. C., **Certificação Digital Conceitos e Aplicações - Modelos Brasileiro e Australiano**. 1a ed. Rio de Janeiro: Editora Ciência Moderna, 2008.

CERTISIGN. **Segurança na Certificação Digital**. Disponível em: <http://www.certisign.com.br/atendimento-suporte/certificado-digital/instalacao-e-emissao-de-certificado-a1> Acesso em: 08 fev. 2014.

CERT. **Centro de Estudos Resposta e Tratamento de Incidentes de Segurança no Brasil** <http://cartilha.cert.br/criptografia/> Acesso em: 30 abr. 2014.

COMER, D. **Redes de Computadores e Internet**. 2a.ed. Porto Alegre: Bookman 2001.

CORDEIRO, L. G. S. **Certificação Digital.** Rio de Janeiro, Ciência moderna, 2008.

COSTA, D. G. DNS: **Um guia para administradores de Redes**. Rio de Janeiro: Brasport, 2006.

HIRATA, W**. Desafios da ICP-Brasil**. Brasília: Revista Digital ITI, 2013.

ICP-Brasil. Instituto Nacional de Tecnologia da Informação. **Infra-Estrutura de Chaves** <http://www.iti.gov.br/publicacoes/manuais > Acesso em: 18 jun. 2014.

ITI. Instituto Nacional da Tecnologia da Informação. **Certificação** <http://www.iti.gov.br/certificacao-digital > Acesso em: 27 jan. 2014.

MARTINEZ, G. H. **Sobre A Certificação Digital** <http://fgh.escoladenegocios.info/revistaalumni/artigos/edEspecialMaio2012/vol2_noespecial_artigo_26.pdf > Acesso em: 19 fev. 2014.

MENEZES, J. C. **Gestão da Segurança da Informação**. 1A ed.Campinas: Editora J. H. Mizuno, 2006.

PORTAL TRIBUTÁRIO. **Normas legais** Disponível em: <http://www.normaslegais.com.br> Acesso em: 23 mar. 2014.

RFB. **Certificação Digital.** Receita Federal do Brasil**.** Disponível em: <http://www.receita.fazenda.gov.br/atendvirtual/orientacoes/default.htm> Acesso em: 07 mar. 2014.

SERASA EXPERIAN. **Certificação Digital.** Disponível em: <http://www.serasaexperian.com.br/certificados> Acesso em: 21 jan. 2014.

STARLIN, G. **TCP/IP**: Internet, Intranet e Extranet. Rio de Janeiro: Book Express, 2001.

THOMPSON, M.A. **Proteção e Segurança na Internet**. São Paulo: Érica, 2002.

TANENBAUM, A. S. **Redes de Computadores.** 4a. Edição, Campus, 2003.