CERTIFICAÇÃO DIGITAL:
A UTILIZAÇÃO DA CERTIFICAÇÃO DIGITAL EM DOCUMENTOS, TRANSAÇÕES COMERCIAIS E JURÍDICAS*

Dannylo Bento Martins Pinheiro[1]
Francisco Rosa Camargo Neto[2]

RESUMO: Com o avanço da Tecnologia da Informação, surgiu a necessidade de se interagir com o mundo digital de maneira ágil e segura. Uma solução para esta necessidade é a certificação digital, que assegura a autenticidade das informações que transitam pela rede. A certificação digital permite que informações transitem pela rede (Internet) com maior segurança. Entre outras funções, a certificação digital, pode ser utilizada para, por exemplo, evitar que hackers interceptem ou adulterem as comunicações realizadas via internet. Também é possível saber, com certeza, quem foi o autor de uma transação ou de uma mensagem, ou, ainda, manter dados confidenciais protegidos contra leitura por pessoas não autorizadas. O presente artigo apresenta os principais conceitos de certificação digital, contribuindo assim para a correta e segura utilização da certificação digital.

Palavras-chave: Certificação digital. Assinatura digital. Criptografia. Certificados.

ABSTRACT: With the advancement of information technology, the need to interact with the digital world in a fast and safe. A solution to this need is a Digital Certificate, which ensures the authenticity of information transiting the network. A digital certificate allows transit through the information network (Internet) with greater security. Among other functions, digital certification can be used, for example, prevent hackers from tampering or intercepting communications made via internet. It is also possible to know for sure who was the author of a transaction or a message, or even to keep sensitive data protected from reading by unauthorized persons. This article presents the main concepts of digital certification, thus contributing to the correct and safe use of digital certification.

Keywords: Digital Certificate. Digital Signature. Encryption. Certificates.

1 INTRODUÇÃO

Nos últimos anos a informática tem avançado gradativamente e estreitado o relacionamento e comunicação entre as pessoas, computadores e equipamentos por meio da rede de computadores e principalmente na internet. Com a proliferação das transações realizadas pela internet e o aumento do comércio eletrônico, surge à necessidade de mecanismos que garantam a segurança e proteção destas

* Trabalho de conclusão de curso na modalidade de artigo científico apresentado como requisito para obtenção do título de tecnólogo em Gestão da Tecnologia da Informação, da Faculdade Serra da Mesa, sob orientação do Prof. Esp. Lindomar José Rocha.

[1] Tecnólogo de Gestão da Tecnologia da Informação. E-mail: dannylogti@gmail.com.
[2] Tecnólogo em Gestão da Tecnologia da Informação. E-mail: fcncamargo@gmail.com.

operações. Neste cenário a certificação digital desponta como tecnologia que fornece, aos seus usuários, confiabilidade, integridade e segurança. A certificação digital também proporciona a seus usuários o direito de propriedade e não repúdio, pois a mesma garante a todo documento e transações assinados digitalmente, por entidade devidamente certificada, valor jurídico e não pode ser contestada por quem a assinou.

> O certificado, na prática, equivale a uma carteira de identidade virtual ao permitir a identificação de uma pessoa no meio digital/eletrônico quando enviando uma mensagem ou em alguma transação pela rede mundial de computadores que necessite validade legal e identificação inequívoca. Um certificado digital contém dados de seu titular, tais como nome, identidade civil, e-mail, nome e assinatura da Autoridade Certificadora que o emitiu, entre outras informações. É importante saber que essa tecnologia confere a mesma validade jurídica ao documento assinado digitalmente do equivalente em papel assinado de próprio punho. (ITI, 2012)

Para que os objetivos da certificação digital sejam alcançados se faz necessário que uma terceira parte faça a mediação entre quem emitiu o certificado e quem necessita comprovar a veracidade das informações. Aqui no Brasil, essa terceira parte é a Infra Estrutura de Chaves Públicas Brasileiras - ICP-Brasil.

> 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 subsequente ao seu. (ITI, 2012)

O presente artigo tem como propósito apresentar a certificação digital como forma de se obter maior segurança á seus usuários, visto que, muitas pessoas não se preocupam com tal aspecto. Serão apresentadas também as principais utilizações dos certificados e alguns tipos de certificados existentes atualmente.

2 REDES DE COMPUTADORES

Uma rede e formada por qualquer tipo de dispositivo capaz de enviar ou receber dados entre si. Uma rede de computadores pode ser formada por, além de dois ou mais computadores, outros dispositivos como, impressoras, repetidores,

Revista Fasem Ciências | Vol. 2, n. 2, jul.-dez./2012

pontes, roteadores, scanners, etc., a fim de compartilhar recursos, dados, informações e outras. Com baixa taxa de erro e grande capacidade de fluxo de dados, transmissões chegando a vários gigabits por segundo, essas redes podem ser restrita ou privada. "Pode-se caracterizar uma rede local como sendo uma rede que permite a interconexão de equipamentos de comunicação de dados numa pequena região" (SOARES, 1995, p. 10).

Existem tipos diferentes de redes de computadores, porem, vamos dar focos nas mais convencionais. Lans, Mans, Wans.

LANs (Local Área Network): São redes locais e de acesso restritos a um ambiente corporativo, estações de trabalho, domestico etc." As redes locais, muitas vezes chamadas LANs, são redes privadas contidas em um único prédio ou em um campus universitário com até alguns quilômetros de extensão". (TANEMBAUM, 2003, p. 18).

MANs (Metropolian Área Network): Tem similaridade com a LANs porem com a dimensão geográfica, velocidade e o número de usuários ligados a ela serem muito mais superiores, sua dimensão pode se estender a varias regiões e interligando varias cidades e organização vizinhas. Segundo Tanembaum (2003, p.19):

> Uma rede metropolitana, ou MAN, abrange uma cidade. O exemplo mais conhecido de uma MAN é a rede de televisão a cabo disponível em muitas cidades. Esse sistema cresceu a partir de antigos sistemas de antenas comunitárias usadas em áreas com fraca recepção do sinal de televisão pelo ar.

WANs (Wide Área Network): São redes que abrangem áreas geográficas determinadas, como continentes, países vizinhos e outros, através de circuitos e satélites etc., são redes de uso público e privado, transmitindo dados a milhões de usuários em todo mundo, um grande exemplo e a compra pela internet, podendo ser feita em outros continentes. “Uma rede geograficamente distribuída, ou WAN (Wide área network), abrange uma grande área geográfica, com frequência um país ou continente". (TANEMBAUM, 2003, p. 20).

Revista Fasem Ciências | Vol. 2, n. 2, jul.-dez./2012

3 PROTOCOLO

Praticamente vivemos baseados em protocolos, a humanidade tem seus próprios protocolos, regras, conjuntos de boas maneiras, respeito, como "licença ou, por favor," isso tudo faz com que a sociedade caminhe em constante união.

No hardware e no software os protocolos tem finalidade de garantir a integridade dos dados transmitidos e determinar os caminhos que os pacotes devem percorrer. Exemplo, um roteador determina o caminho certo em que determinada mensagem ou dados devem ir através do endereçamento do computador a receber a mensagem. "O protocolo é um conjunto de regras que controla o formato e o significado dos quadros, pacotes ou mensagens trocadas pelas entidades pares contidas em uma camada" (TANEMBAUM, 2003, p. 39).

Dentre os protocolos destacam-se dois modelos que servem como referência: OSI (Open Systems Interconnection) e o TCP/IP (Transmission Control Protocol/Internet Protocol).

O modelo OSI não é muito usado e nem é considerado uma arquitetura de redes, pois não especifica os serviços, protocolos e camadas usados. Ele foi uma tentativa de padronização da ISO (International Standards Organization), esse modelo apresenta sete camadas: Física, Enlace ou ligação de Dados, Redes, Transporte, Sessão, Apresentação e Aplicação.

O modelo TCP/IP e o mais comum na atualidade sendo usado mundialmente, ou seja, a Internet, possuindo quatro camadas apenas, que são: Inter-redes, Transporte, aplicação, Host/Rede. Segundo Tanembaum (2003, p. 40):

> Os modelos de referência OSI e o modelo de referência TCP/IP. Embora os protocolos associados ao modelo OSI e o raramente seja usados nos dias de hoje, o modelo em si e de fato bastante geral e ainda valido, e as características descritas em cada camada ainda são muito importante. O modelo TCP/IP tem características opostas: o modelo propriamente dito não é muito utilizado, mais os protocolos têm uso geral.

4 INTERNET

É uma rede que permite a comunicação entre milhões de equipamentos, com uma alta velocidade de comunicação, podendo realizar tarefas em todo o mundo sem sair de sua casa, podendo acessar e-mail, blogs, estações de trabalho, isto

tudo através de diversos tipos de aparelhos com celular, notebooks, tabletes entre outros, tudo isso sendo compartilhados através da WEB, esses compartilhamentos são chamados de sistemas finais. "A internet pública é uma rede de computadores mundial, isto é, uma rede que interconecta milhões de equipamentos de comunicação em todo o mundo" (KUROSE; ROSS, 2010, p. 2).

5 SEGURANÇA NA REDE

A segurança na rede vem se tornando um assunto muito discutido, com os grandes números de pessoas usando a internet, a segurança de suas informações vem se tornando mais e mais vulneráveis e sujeita a invasão e publicação indevidas de conteúdo na WEB, podemos identificar diversos fatores, como: confidencialidade, autenticidade, integridade e disponibilidade de controle de acesso às informações.

Confidencialidade: Define através de permissões quem pode ou não acessar as informações ali guardadas. "Confiabilidade é a proteção dos dados transmitidos contra ataques passivos. Com relação ao conteúdo de uma transmissão de dados, vários níveis de proteção podem ser identificado". (STALLINGS; WILLIAM, 2008, p.10)

Autenticidade: Como o próprio nome fala autentica as informações do documento encaminhado. "O serviço de autenticação refere-se a garantir de que uma comunicação é autêntica". (STALLINGS; WILLIAM, 2008, p.18).

Integridade: Visa proporcionar uma informação confiável e segura durante o processo de transmissão da informação entre os indivíduos, proporcionando integridade a informação. Ainda de acordo com Stallings e William (2008, p.10):

> Assim como a confiabilidade, a integridade pode ser aplicada a um fluxo de mensagens, uma única mensagem ou campos selecionado dentro de uma mensagem. Novamente, a técnica mais útil e direta é a proteção total do fluxo.

Disponibilidade e controle de acesso: Delimita quem pode acessar as informações dentro da rede. "No contexto da segurança de redes, o controle de acesso é a capacidade de limitar e controlar o acesso aos sistemas e aplicações hospedeiras por meio de enlace de comunicação" (STALLINGS, WILLIAM, 2008, p.09).

Revista Fasem Ciências | Vol. 2, n. 2, jul.-dez./2012

São esses fatores que garantem a segurança de uma rede, lembrando que um elo fraco pode enfraquecê-la toda, permitindo que um hacker faça uma invasão pelo ataque em massa.

6 CRIPTOGRAFIA

A palavra criptografia deriva dos termos gregos *Kryptós*, que quer dizer oculto, e *graph,* escrever. A criptografia é uma informação distorcida, que busca ocultar ou dificultar a leitura de uma mensagem pelos interceptadores, fazendo com que somente o destinatário correto consiga decifrar a mensagem. Em dicionários de língua portuguesa, pode ser encontrada a seguinte definição para a palavra criptografia: escrita secreta por meio de abreviaturas ou de sinais convencionados de modo a preservar a confidencialidade da informação. Segundo SILVA e LUIZ et al (2008, p. 13):

> 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 do que o custo obtido com a informação.

6.1 Criptografia simétrica

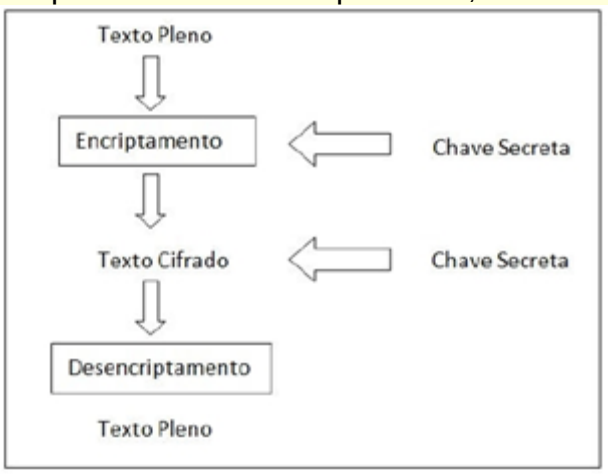
É baseada na cumplicidade de quem envia e de quem recebe a informação, e somente com o código correto trocado entre eles as mensagens podem ser decodificadas. Podemos chamá-la de "Criptografia de Chave Secreta". Segundo Silva e Luiz et al (2008, p.17):

> Criptografia de chave secreta (também chamada de criptografia simétrica) usa uma chave secreta para criptografar uma mensagem de texto cifrado e a mesma chave para decifrar o texto cifrado em texto pleno.

Um modelo ilustrativo deste mecanismo demonstrado por Silva e Luiz et al (2008) pode ser observado na figura 01, que ilustra o uso de chave secreta baseada na cumplicidade dos códigos para encriptamento e desencriptamento dos dados.

Revista Fasem Ciências | Vol. 2, n. 2, jul.-dez./2012

Figura 01 – Encriptamento e desencriptamento, usando chave secreta.



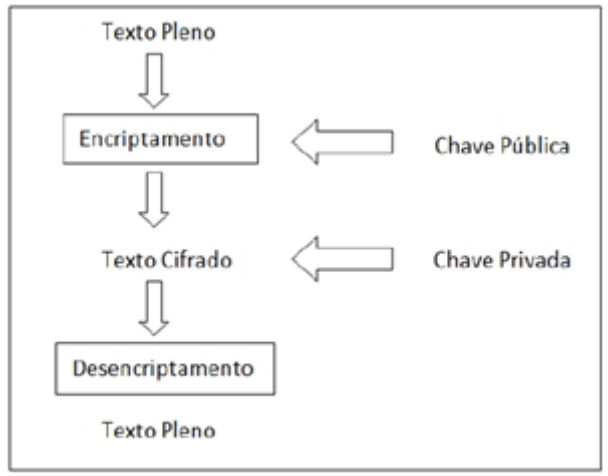
Fonte: (SILVA, LUIZ et al, 2008, p. 17)

6.2 Criptografia assimétrica

Esta criptografia também é conhecida de como "Criptografia de Chave Publica", ela funciona com algoritmos de duas chaves, ou seja, uma chave codifica e a outra diferente descodifica a mensagem. Esse pares de chave necessita exclusivamente uma da outra, ex. a chave 1 somente e decodificada pela chave 2 do mesmo par.". Segundo SILVA e LUIZ et al (2008, p.18):

> A criptografia de chave pública (também chamada de criptografia assimétrica) envolve duas chaves distintas, uma pública e uma privada. A chave privada é mantida em segredo e nunca deve ser divulgada. Por outro lado, a chave pública não é secreta e pode ser livremente distribuída e compartilhada com qualquer pessoa.

Figura 02 – Encriptamento e desencriptamento, usando chaves pública e privada.



Fonte: (SILVA, LUIZ et al, 2008, p. 19)

Revista Fasem Ciências | Vol. 2, n. 2, jul.-dez./2012

6.3 Algoritmos de resumo

A Função Resumo (algoritmo de *hash*) como o próprio nome já diz tem como objetivo realizar resumos a partir dos arquivos que ela recebe. Para que um algoritmo de resumo seja considerado seguro, no sentido de criptografia, é necessário que seja inviável computacionalmente identificar a mensagem original de entrada baseando-se somente no seu resumo; não deverá possibilitar encontrar-se uma mensagem particular que tenha um resumo específico e deverá ser computacionalmente inviável se encontrar mensagens diferentes com o mesmo resumo. Com o resumo a mensagem fica integra, possibilitando uma maior confiabilidade da mensagem. "O propósito de uma função resumo é produzir uma "impressão digital" da mensagem". (MONTEIRO; MIGNONI, 2007, p. 08).

6.4 Assinatura digital

Para entender assinaturas digitais imagine a seguinte situação: Certa pessoa se encontra em determinado local do planeta e necessita enviar documentos confidenciais a outra pessoa que se encontra a milhares de quilômetros. Sabendo que o meio mais rápido de enviar tais documentos será utilizando a internet, surge então uma dúvida: Como o destinatário poderá comprovar que os documentos recebidos são realmente de sua autoria?

É neste contexto, então, que surge a Assinatura Digital. Segundo Monteiro e Mignoni (2007, p. 10):

> Uma Assinatura Digital é um algoritmo de autenticação, que possibilita ao criador de um objeto unir ao objeto criado, um código que irá agir como uma assinatura. Esta assinatura confirma que o objeto não foi alterado, desde o ato de sua assinatura e permite identificar o assinante, fato conhecido como Autenticação.

No processo de assinatura digital o destinatário utiliza uma chave de verificação para averiguar a origem da mensagem recebida e ter certeza de que a mesma não foi alterada enquanto estava sendo enviada. Ainda de acordo com Monteiro e Mignoni (2007, p. 11):

> As chaves de assinatura e verificação são distintas, garantindo que

Revista Fasem Ciências | Vol. 2, n. 2, jul.-dez./2012

> o destinatário possa somente verificar a assinatura, mas não será capaz de forjá-la. Devido ao fato de não ser computacionalmente viável forjar uma assinatura sem a posse da chave de assinatura, o autor não pode repudiar o fato que assinou uma mensagem.

A assinatura digital também faz uso do algoritmo de *hash*. Primeiramente a mensagem original é transformada em um resumo (*hash*), o resultado desse resumo é criptografado utilizando para isso a chave privada do autor da mensagem. O resultado desta criptografia se denomina assinatura digital. Segundo Silva e Luiz et al (2008, p. 22):

> Assinar uma mensagem inteira ao invés de seu resumo, embora seja possível, não é recomendado por vários motivos. Primeiramente, assinar uma mensagem inteira dobra a quantidade de informação que deve ser enviada. Além disso, as operações de criptografia de chave pública são geralmente mais lentas, fazendo com que o custo de criptografar uma mensagem inteira acarrete problemas de desempenho. E, por último, um criptoanalista pode usar a grande quantidade de texto cifrado junto com a mensagem original para tentar um ataque de análise de mensagens criptografadas.

7 AUTORIDADES CERTIFICADORAS E DE REGISTROS

As autoridades certificadoras (A/C) são organizações confiáveis que emitem certificados digitais para outras entidades ou indivíduos que necessitam se identificar no meio digital, a autoridade certificadora é a terceira parte envolvida nas relações entre uma entidade e outra. "Cada Certificado Digital emitido é certificado e garantido pela A/C responsável pela sua emissão. A A/C recebe e autentica a solicitação de certificado, emite e chancela digitalmente o certificado e gerencia os certificados emitidos" (MONTEIRO; MIGNONI, 2007, p. 17).

As A/C são entidades devidamente credenciadas à AC-Raiz (ITI - Instituto Nacional de Tecnologia da Informação), e têm a função de emitir, expedir, distribuir, revogar e gerenciar os certificados digitais, vinculando pares de chaves criptográficas ao respectivo titular, bem como colocar à disposição dos usuários listas de certificados revogados e outras informações pertinentes, além de manter registro de todas as suas operações. O par de chaves criptográficas será gerado sempre pelo seu próprio titular e, sua Chave Privada será de seu exclusivo controle, uso e conhecimento.

Quanto as Autoridades de Registro (A/R), são entidades vinculadas a uma

determinada Autoridade Certificadora, cabe a elas receberem os pedidos de novos certificados com as funções de identificar os titulares dos certificados digitais e aprovarem as solicitações de certificados, para que os titulares possam baixar seus certificados. É um serviço desempenhado por Agentes de Registro, por exemplo, as Agências dos Correios são Autoridade de Registro da Autoridade Certificadora do SERPRO-RFB. Segundo Monteiro; Mignoni (2007, p. 18):

> A AR (Autoridade de Registro) é uma entidade responsável pela verificação das informações fornecidas pelos requisitantes dos certificados. A AR atua como um órgão de apoio à AC, podendo inclusive exigir que o requisitante compareça pessoalmente a AR para garantir a veracidade das informações. Também pode lhe ser confiada à tarefa de registrar outras entidades.

8 CERTIFICAÇÃO DIGITAL

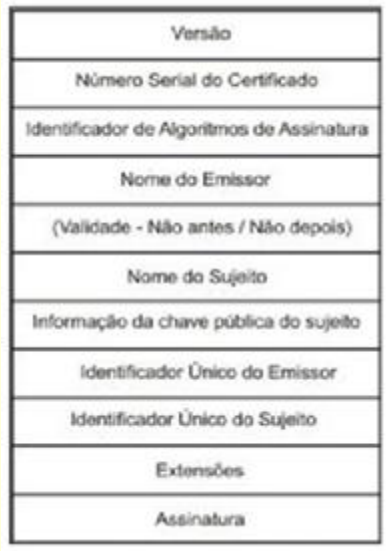
Para entende certificação digital vamos primeiramente entender o que é um certificado digital. Imaginemos a seguinte situação: Eduardo decide fazer uma viagem à Recife, para isso ele compra uma passagem de avião pela internet e no dia marcado ele se encaminha ao aeroporto munido de sua passagem e seus documentos pessoais, Eduardo se apresenta no balcão da companhia que comprou a passagem, a atendente confere a passagem e "os documentos pessoais de Eduardo" para comprovar que não se trata de outra pessoa tentando voar em seu lugar, documentos conferidos Eduardo estará apto a embarcar em seu voo. Analisando tal situação e fazendo uma comparação com certificados digitais pode-se dizer que o certificado digital funciona como uma espécie de identidade digital do seu portador. Segundo Silva e Luiz et al (2008, p.18):

> De uma forma genérica, um certificado digital é a versão digital de um documento de identidade. Quando é necessário comprovar sua identidade, o certificado é utilizado como forma de presença, por mostrar a chave privada que se relaciona com uma chave pública.

O certificado digital é um arquivo de computador que carrega em si os dados pessoais do indivíduo ou da entidade a qual foi emitido e, além disso, possuem também uma chave pública do assinante. Qualquer pessoa tem a possibilidade de produzir seu próprio certificado digital e usá-lo, sabendo disso: o que garantiria a segurança da parte que necessita de comprovação de identidade do proprietário do

certificado em questão, sabendo que qualquer pessoa é capaz de produzir um certificado digital? Pensando nisso foram criadas as ACs (Autoridades Certificadoras).

Figura 03 – Modelos de certificação digital



Fonte: (SILVA, LUIZ et al, 2008, p. 19)

> Os Certificados Digitais são compostos por um par de chaves (Chave Pública e Privativa) e a assinatura de uma terceira parte confiável - Autoridade Certificadora - A/C. As Autoridades Certificadoras emitem, suspendem, renovam ou revogam certificados, vinculando pares de chaves criptográficas ao respectivo titular. Essas entidades devem ser supervisionadas e submeter-se à regulamentação e fiscalização de organismos técnicos. No meio físico, para que uma credencial de identificação seja aceita em qualquer estabelecimento, a mesma deverá ser emitida por um órgão habilitado pelo governo. No meio digital ocorre o mesmo - devemos apenas aceitar Certificados Digitais que foram emitidos por Autoridades Certificadoras de confiança (CERTISIGN, 2012).

Quando é necessário comprovar a identidade, o certificado digital é utilizado como forma de autenticar a presença, através da chave privada da entidade em questão e sua respectiva chave pública, a qual deve ser previamente certificada por uma Autoridade Certificadora Confiável (uma terceira parte envolvida confiável, homologada pela Infraestrutura de Chaves Públicas).

> O objetivo é confirmar a identidade do usuário na Web, no correio eletrônico, transação on-line, transação eletrônica, informação eletrônica, cifrar chaves de sessão (utilizadas para cifrar grandes

> volumes de dados) e assinatura de documento eletrônico, conferindo validade jurídica e garantindo a segurança de suas informações (VOLPI, 2001).

O certificado digital utiliza a criptografia de chave pública adaptada a sua necessidade. A informação só será considerada certificada com a possibilidade de uso do par de chaves pública e sua respectiva chave privada. Portanto, pode-se comparar este sistema a um cadeado composto por duas chaves distintas, mas interligadas: uma para abrir e outra para trancá-lo: com uma das chaves se assina o certificado digital e, com a outra, se verifica o certificado e, se for o caso, decifra-se a informação (se esta foi previamente cifrada). A chave pública do signatário precisa estar contida no certificado digital para a verificação das informações contidas no documento. Esta pode ser checada na Infraestrutura de Chaves Públicas em utilização.

A certificação digital permitiu uma nova interpretação na maneira como as pessoas se interagiam com os negócios e transações on-line, pois instituiu validade jurídica nas ações realizadas pelo meio on-line, trazendo para os usuários maior segurança, credibilidade, comodidade e agilidade.

> Com validade jurídica vigente na legislação brasileira, a assinatura eletrônica com Certificado Digital substitui o papel com total garantia de autenticidade da autoria, integridade do conteúdo do documento (se uma vírgula for alterada, sabe-se que houve alteração do seu conteúdo) e privacidade. (CERTISIGN, 2012).

Segundo Certisin (2012), podemos destacar algumas vantagens que a certificação digital trouxe para nossa realidade, como:

- Os contribuintes podem renegociar dívidas com o governo federal: os certificados digitais ou códigos de acesso são necessários para a validação do parcelamento da dívida;
- Na era do TI Verde: Para fugir dos inconvenientes de percas de documentos e além disso alcançar o lema "ecologicamente correto", muitas empresas têm adotado uma ferramenta fundamental para migração das cópias impressas para o formato eletrônico: a Certificação Digital;
- Entrega da DIPJ (Declaração do Imposto de Renda Pessoa Jurídica): Companhias tributadas pelo lucro real ou arbitrado deverão entregar a

Revista Fasem Ciências | Vol. 2, n. 2, jul.-dez./2012

declaração com certificação digital;

- Mais produtividade: Menos papel e mais tempo garantem mais produtividade e competitividade a seus usuários;
- Evite fraudes digitais: A Certificação Digital garante sigilo, autenticidade e integridade para você executar transações eletrônicas com mais segurança;
- Segurança na Web: Nos dias de hoje, em que a Internet é um dos principais canais de comunicação entre pessoas, à segurança das informações trocadas na rede, assim como a integridade dos websites, são pontos essenciais para uma interação positiva e bem sucedida;
- O cidadão no centro das atenções: Órgãos públicos investem em melhorias na gestão de processos para diminuir burocracia e beneficiar o contribuinte;
- Ferramenta para agilizar processos jurídicos: Justiça do Trabalho investe em tecnologia para acabar com a papelada que lota tribunais e atrasa julgamentos;
- SPEED e NE-e: Sistemas Tributário e Fiscal em evolução: O sistema tributário e fiscal brasileiro vem mostrando sinais de evolução nos últimos anos para agilizar a dinâmica de processos e proteger a comunicação com os contribuintes. O primeiro passo importante nesse sentido foi a criação do Sistema Público de Escrituração Digital (SPED), implementado com o objetivo de modernizar o sistema atual e substituir o repasse em papel de informações aos fiscos por arquivos digitais.

8.1 Tipos de certificados

Os tipos básicos de certificados oferecidos no Brasil pelas autoridades certificadoras, são basicamente e-CPF e e-CNPJ do tipo: A1, A2, A3, A4, para assinatura e S1, S2, S3 e S4 para sigilo. Quanto mais alto o número mais complexo é o nível de criptografia do certificado. Existem outros tipos de certificados, como o SSL, que basicamente é para sites.

A série A (A1, A2, A3 e A4) reúne os certificados de assinatura digital, utilizados na confirmação de identidade na Web, em e-mail, em redes privadas

virtuais (VPN) e em documentos eletrônicos com verificação da integridade de suas informações. A série S (S1, S2, S3 e S4) reúne os certificados de sigilo, que são utilizados na codificação de documentos, de bases de dados, de mensagens e de outras informações eletrônicas sigilosas. Os oito tipos são diferenciados pelo uso, pelo nível de segurança e pela validade.

Nos certificados do tipo A1 e S1, as chaves privadas ficam armazenadas no próprio computador do usuário. Nos tipos A2, A3, A4, S2, S3 e S4, as chaves privadas e as informações referentes ao seu certificado ficam armazenadas em um hardware criptográfico - cartão inteligente (*smartcard* - figura 06) ou cartão de memória (*token* USB ou pen drive - figura 05). Para acessar essas informações você usará uma senha pessoal determinada no momento da compra.

Figura 04 – Tipos de certificados

Tipo de certificado	Chave criptográfica			Validade máxima (anos)
	Tamanho (bits)	Processo de geração	Mídia armazenadora	
A1 e S1	1024	Software	Arquivo	1
A2 e S2	1024	Software	Smart card ou token, sem capacidade de geração de chave.	2
A3 e S3	1024	Hardware	Smart card ou token, com capacidade de geração de chave.	3
A4 e S4	2048	Hardware	Smart card ou token, com capacidade de geração de chave.	3

Fonte: (CERTISIN, 2012)

Figura 05 – *Token*

Fonte: (CERTISIN, 2012)

Figura 06 – *Smartcard*

Fonte: (CERTISIN, 2012)

Certificados mais comuns:

- A1 - de menor nível de segurança, é gerado e armazenado no computador do usuário. Os dados são protegidos por uma senha de acesso. Somente com essa senha é possível acessar, mover e copiar a chave privada a ele associada;
- A3 - de nível de segurança médio a alto, é gerado e armazenado em um hardware criptográfico, que pode ser um cartão inteligente ou um token. Apenas o detentor da senha de acesso pode utilizar a chave privada, e as informações não podem ser copiadas ou reproduzidas.

9 APLICAÇÃO

Será abordada neste tópico a parte prática da certificação digital, voltada para as empresas da cidade de Uruaçu-GO, e também outras cidades que se interessarem por tal trabalho, serão apresentados os métodos e sugestões para que tais empresas possam se beneficiar ao máximo de tais aplicações.

Como observamos neste mesmo trabalho, a certificação digital é de enorme importância a todas as partes envolvidas nos processos. Com o surgimento dos negócios e transações eletrônicas realizadas através da internet e a busca constante dos usuários por meios de garantirem a própria segurança, a certificação digital se tornou uma tecnologia imprescindível para o bom relacionamento entre fornecedores, governo, empresas, clientes e também usuários comuns, proporcionando economia de tempo, redução de custos, desburocratização de processos, validade jurídica nos documentos eletrônicos, possibilidade de eliminação de papéis, autenticação na Internet com segurança, etc.

Revista Fasem Ciências | Vol. 2, n. 2, jul.-dez./2012

Para obter um Certificado Digital, o interessado (Pessoa Física que responderá pela empresa), deve fazer a solicitação via Internet a uma das Autoridades Certificadoras filiadas a ICP-Brasil. No Brasil, órgãos como a Receita Federal e o SERPRO, dentre outros atuam como AC. Em seguida, a certificadora entrará em contato com o solicitante para comunicar que o interessado poderá se dirigir a uma Autoridade de Registro (AR), ou seja, levar os documentos necessários à obtenção do certificado a uma das localidades que presencialmente farão a identificação da pessoa e a vinculação a um certificado digital. Esta será a única etapa em que o cidadão ou responsável pela empresa terá que se dirigir a um local portando os documentos físicos exigidos.

Abaixo temos um exemplo passo a passo de como determinada entidade poderá comprar, agendar, validar e obter o seu e-CPF, seu e-CNPJ ou sua NF-e para começar a utilizar a certificação digital. (Observe que tomaremos como escolha para este exemplo a Autoridade de Registro dos Correios):

1º Passo: Escolher uma Autoridade Certificadora da ICP-Brasil ou Autoridade de Registro, escolher o tipo de certificado e preencher o cadastro (Caso tenha escolhido o tipo A3, lembre- se de que é necessário ter a mídia "TOKEN" ou "SMART CARD" disponível neste momento). Imprima duas vias do Termo de titularidade (não assine as vias);

2º Passo: Após a solicitação e emissão do Termo de Titularidade, compareça em até 48 horas a uma agência credenciada (AR) com o Termo de Titularidade e a documentação exigida, apresente a documentação a um dos agentes registradores e efetue o pagamento do certificado digital, caso isso não seja possível, descarte o Termo de Titularidade emitido e faça uma nova solicitação imprimindo novo Termo de Titularidade;

3º Passo: Proceda a baixa do seu certificado digital no mesmo computador e com o mesmo login (identificação de usuário) utilizado no momento da solicitação (PASSO 1). Atente-se para executar esses procedimentos em, no máximo, 72 horas a partir da solicitação do certificado. Caso tenha escolhido o tipo A3, grave o certificado na mídia escolhida ("TOKEN" ou "SMART CARD").

Observações:

Executando os passos 1, 2 e 3 no mesmo dia, evita-se a ocorrência de

Revista Fasem Ciências | Vol. 2, n. 2, jul.-dez./2012

problemas durante a baixa e eventual perda do certificado digital. Atente-se para executar esses procedimentos em, no máximo, 72 horas a partir da solicitação do certificado.

O certificado do tipo A1 é como um arquivo comum do sistema operacional, assim recomenda-se fazer uma cópia de segurança para um disquete, CD ou outro tipo de mídia externa para evitar a perda do certificado nos casos de problemas no computador.

10 CONCLUSÃO

O uso da certificação digital hoje se tornou indispensável visto que, cada vez mais o mundo se torna digital e surge a necessidade de se identificar quem é quem nesse meio. A certificação digital trouxe com ela a segurança para os usuários (comuns ou profissionais), pois permite implementar o não repúdio e a identificação de pessoas, sejam elas jurídicas ou físicas, no mundo digital.

A certificação digital ainda encontra barreias a serem rompidas, como a cultural. Hoje, apesar de grande parte de a população possuir acesso a internet e outras tecnologias, é difícil desvincular da mente das pessoas que para um documento ter validade jurídica não necessita, necessariamente, ser transcrito em papel e assinado a próprio punho. Observa-se também que a certificação digital, quando comparada ao uso do papel, ainda está “engatinhando”, pois o uso deste além de milenar está amplamente difundido por toda a sociedade mundial. Essa barreia cultural vai aos poucos se desfragmentando, pois as pessoas estão cada dia mais interagindo nos meios digitais e buscando formas para se protegerem em tais meios.

A certificação digital é uma das principais ferramentas utilizadas para garantir a segurança, integridade e identidade das informações envolvidas. Ela é de enorme valia, mas deve ser utilizada juntamente com outros métodos como, boas políticas de segurança, criptografia de dados, análises de ameaças, etc. Deve-se buscar minimizar os riscos na segurança e estabelecer regras e parâmetros que dificultem ao máximo a perda e vazamento das informações.

REFERÊNCIAS

CERTISIGN [2012]. **Por dentro da Certificação Digita**. Disponível em: <http://www.certisign.com.br/certificacao-digital/por-dentro-da-certificacao-digital>. Acesso em: 02 de Maio de 2012.

ITI [2012]. **Certificado Digital Como Obter**. Disponível em: <http://www.iti.gov.br/twiki/bin/view/Certificacao/CertificadoObterUsar>. Acesso em: 07 de Maio de 2012.

MONTEIRO, E.; MIGNONI, M. **Certificados Digitais**. Conceitos e Práticas. Rio de Janeiro: Brasport, 2007.

NAKAMURA, E. T. **Segurança de redes em ambientes cooperativos**. São Paulo: Novatec Editora, 2007.

ROSS, KUROS E. **Redes de Computadores e a Internet**. Trad. Opportunity Translations. 5. ed. São Paulo: Pearson, 2010.

SILVA, L. et al. **Certificação Digital**. Conceitos e Aplicações. Modelos Brasileiro e Australiano. Rio de Janeiro: Editora Ciência Moderna, 2011.

STALLINGS, WILLIAM. **Criptografia e Segurança de Redes**. Trad. Daniel Vieira. 4. ed. São Paulo: Pearson Prentice Hall, 2008.

TANENBAUM, A. S. **Redes de Computadores**. Trad. Vanderberg D. de SOUZA. 17. ed. Rio de Janeiro: Elsevier, 2003.

VOLPI, M. M. **Assinatura digital**: aspectos técnicos, práticos e legais. Rio de Janeiro: Axcel Books do Brasil, 2001.