Certificação Digital: Tecnologia Indispensável na Segurança das Transações Eletrônicas

Francisco das Chagas Fontenele Marques[1], Isaac de Sousa Castro[1], Jaclason Machado Veras[1]

[1]Universidade Aberta do Piauí (UAPI) – Universidade Federal do Piauí (UFPI)
Rua Tenente Rui Brito, 1430 - Centro - CEP: 64240-000 - Piracuruca - PI – Brasil

{fcfmar, isaacscastro}@hotmail.com, jaclason@gmail.com

Abstract. *This article describes the digital certification system implemented in Brazil, demonstrating the usability and the technological processes involved, from design and regulation, emphasizing the need to use your face to the issues of security and confidentiality, speed and legal validity, which are essential for validating electronic transactions.*

Resumo. *Este artigo descreve o sistema de certificação digital implantado no Brasil, demonstrando a usabilidade e os processos tecnológicos envolvidos, desde a concepção e regulamentação, enfatizando a necessidade de seu uso frente às questões de segurança como sigilo, agilidade e validade jurídica, indispensáveis para validação das transações eletrônicas.*

1. Introdução

Diante da popularização da internet e do mundo digital, facilidades como acesso ilimitado a qualquer tipo de informação e comunicação entre pessoas e instituições têm crescido juntamente com a preocupação e discussão de conceitos relativos à segurança dessas informações. Atualmente, a emissão de documentos eletrônicos tem se tornado necessário para empresas e pessoas físicas, como meio de viabilizar a segurança e autenticidade das informações. Algumas técnicas antes utilizadas para expressar concordância e autenticidade de documentos, como assinaturas através de canetas, carimbos, selos, entre outros, tem sido substituídas por outras mais precisas para validar a identidade das informações disponíveis no meio digital, mas, surgem dúvidas como assegurar, demonstrar concordância ou assumir responsabilidades em transações eletrônicas.

A solução para estes questionamentos, citados anteriormente, está na certificação digital, ou seja, na inclusão de recursos associados à assinatura digital que permite de forma segura e eficaz a execução de transações financeiras e movimentações de documentos on-line. Assim, é através do uso dessas técnicas de segurança das informações, que a validade ou não das informações disponíveis podem ser testadas, dando a elas caráter comprobatório ou falso.

A Certificação Digital é uma tecnologia de segurança para as relações eletrônicas, que provê um sistema de identificação de pessoas e entidades no meio eletrônico, que combate o anonimato, a despersonalização e a insegurança em relação ao interlocutor Ottoni (2005).

De maneira geral a certificação digital vincula uma identidade a um par de chaves eletrônicas que pode ser usado para criptografar e assinar informações digitais. Tal certificação possibilita evitar que pessoas usem chaves falsificadas para personificar outros usuários. Este processo utiliza em conjunto com a criptografia os certificados digitais fornecendo uma solução mais completa, assegurando a identidade de todas as partes envolvidas em uma transação.

A certificação digital se torna indispensável à segurança das informações eletrônicas garantindo benefícios como: a desburocratização das atividades, aumento da produtividade das empresas, avanços efetivos para transações econômicas privadas ou com o governo e redução de custos operacionais.

As seções posteriores estão dispostas da seguinte forma: uma visão geral sobre a certificação digital embasados nos tipos de criptografia é apresentada na seção 2. A seção 3 descreve as particularidades do certificado digital. Na seção 4, é realizada uma abordagem sobre as entidades certificadoras. E, finalmente, a seção 5 apresenta as conclusões e trabalhos futuros dos autores.

2. Certificação Digital

A certificação digital pode ser entendida como um mecanismo de segurança para informações ou uma credencial, para autenticar pessoas, empresas, máquinas, aplicações, dentre outras, definindo os dados pertencentes àquela pessoa ou organização. Esta certificação funciona baseada em um documento eletrônico e com o uso de uma assinatura digital.

O uso da certificação digital nos processos eletrônicos assegura alguns aspectos como: privacidade (é a garantia de que as informações trocadas nas transações eletrônicas não serão lidas por terceiros); Integridade (é a garantia de que as informações trocadas nas transações eletrônicas não foram alteradas desde que foram assinadas); Autenticidade (é a garantia de identidade da origem e destino da transação) e Não Repúdio (é a garantia de que somente o titular do Certificado Digital poderia ter realizado determinada transação, impedindo que os integrantes de uma transação venham a contestar ou negar uma transação após sua realização).

Diante deste contexto, na computação a criptografia é essencial para garantir a segurança das informações, mas, esta garantia só é completada com a utilização da assinatura digital, pois existe a possibilidade de interceptação de uma informação criptografada, através de ataques como *Man-In-The-Middle (MITM)*, onde caso a informação não esteja assinada a criptografia sozinha não pode assegurar a Integridade das mensagens.

2.1 Criptografia

A Criptografia é o estudo de códigos e cifras, cujo nome vem do grego *kryptos*, que significa oculto, e *graphen*, que significa escrever. Já a palavra cifra vem do hebraico *saphar*, que significa dar números Silva (2004).

O uso da criptografia é constatado desde os tempos antigos, em geral para fins militares, tendo sido usada de várias maneiras até evoluir aos modernos algoritmos criptográficos usados na certificação digital.

O processo de criptografia pode ser entendido como uma série de algoritmos que fazem o embaralhamento dos bits desses dados a partir de uma determinada chave ou par de chaves, dependendo do sistema criptográfico escolhido (*Vide* Figura 1).

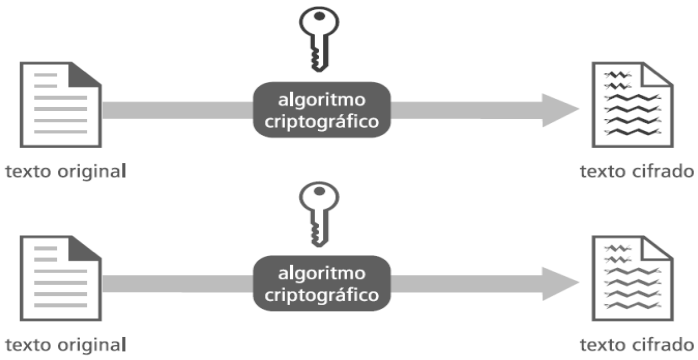

Figura 1. Cifragem de Texto.

A criptografia pode ser definida como o processo de codificação da informação para que somente o emissor e o receptor possam acessá-la, impedindo que uma pessoa não autorizada seja capaz de acessar o seu conteúdo. Os primeiros métodos de criptografia eram realizados usando sempre o mesmo algoritmo de codificação, o que era um problema, pois qualquer receptor que tivesse acesso à informação e tivesse conhecimento desse algoritmo poderia decifrar e interpretar a informação. Para solucionar este problema foram criadas as chaves criptográficas, o emissor poderia utilizar o mesmo algoritmo para vários receptores de uma informação, bastando que cada receptor usasse uma chave diferente. Em caso de perda ou roubo da chave, era apenas necessário substituí-la e o mesmo algoritmo era mantido. Neste contexto, para realizar a decifragem e a leitura da informação, a chave do receptor deverá ser compatível com a chave do emissor.

Para a criptografia moderna, o emprego da chave de criptografia se tornou mais importante do que o próprio algoritmo. Dois tipos de chaves se tornaram vastamente utilizadas: chave simétrica e chave assimétrica ou de chave pública.

2.1.1 Criptografia Simétrica

A criptografia simétrica executa a cifragem e a decifragem de dados utilizando algoritmos que usam a mesma chave, assegurando sigilo na transmissão e armazenagem das informações. Como é utilizada a mesma chave para codificar e decodificar, a chave deve ser compartilhada entre quem efetua a cifragem e quem realiza a decifragem dos dados. O processo da troca de chaves deve ser realizado de forma segura, pois, todos que tiverem acesso à chave poderão decifrar os dados, possibilitando a reprodução ou mesmo a alteração das informações (Vide Figura 2).

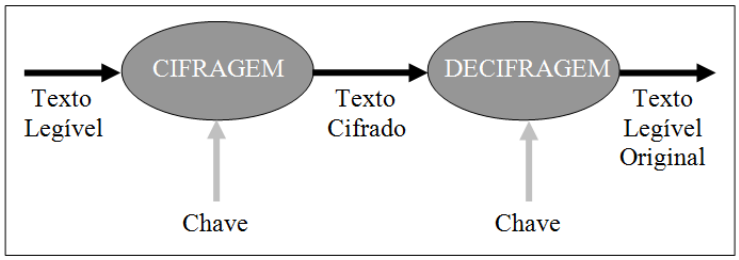

Figura 2. Criptografia Simétrica.

O sistema de criptografia simétrica possui vantagens que ainda a fazem ser usada até hoje, como por exemplo, a velocidade na codificação e decodificação. Ela também é interessante quando a troca de chaves secretas não é considerada um problema, como no armazenamento local de arquivos criptografados.

2.1.2 Criptografia Assimétrica

A criptografia assimétrica ou de chave pública utiliza um par de chaves diferentes que relacionadas matematicamente por intermédio de um algoritmo, possibilita que a informação cifrada por uma seja apenas decifrada pela outra do mesmo par. Tal procedimento é visto através da figura 3.

As duas chaves da criptografia assimétrica são: chave privada e chave pública. Enquanto a chave pública deve ser acessível e disponibilizada a qualquer indivíduo que queira se comunicar com o proprietário da chave privada, por sua vez a chave privada deve ser protegida e mantida em sigilo pelo seu titular que gerou as chaves.

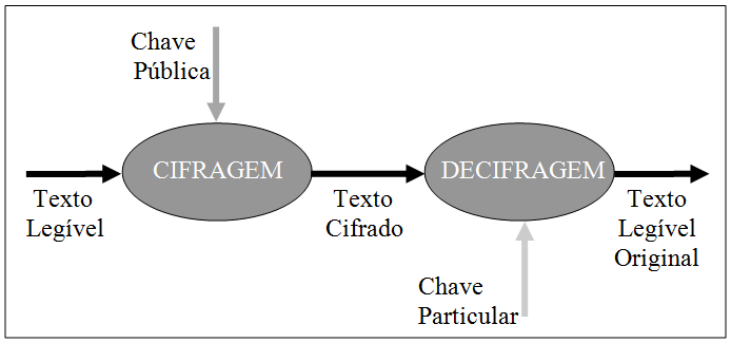

Figura 3. Criptografia Assimétrica.

Esta técnica baseia-se em dois importantes aspectos: confidencialidade e autenticidade. No primeiro consiste em fazer com que a informação esteja acessível apenas a pessoas ou organizações credenciadas. No segundo, em garantir que a informação proceda da origem e modo esperados, de forma que o receptor identifique com clareza.

Em relação à confidencialidade, é importante que o emissor possua a chave pública do destinatário. Por intermédio de algoritmos apropriados, o documento é então cifrado de acordo com esta chave pública. Partindo deste principio, o receptor usará sua correspondente chave privada para a decifragem e consequente obtenção da informação.

2.2 Assinatura Digital

É um método de autenticação que visa garantir a validade legal dos documentos digitais, com isso, o destinatário terá certeza de que a informação que lhe chegou vem da origem esperada, pois, somente esta possui a chave privada que gerou o conteúdo cifrado.

A assinatura digital consiste em dois processos criptográficos: o primeiro sendo uma autenticação através do uso de Assinatura Digital, através do uso de Algoritmos de Criptografia de Chave Pública e a segunda consistir em uma aplicação *hash* que gera um resumo.

A função *hash* retorna um resumo criptográfico da mensagem através de algoritmos complexos que reduzem uma mensagem sempre a um resumo de mesmo

tamanho. Após gerar o *hash*, ele deve ser criptografado através de um sistema de chave pública garantindo a autenticação e a irretratabilidade. O autor da mensagem deve usar sua chave privada para assinar a mensagem e armazenar o *hash* criptografado junto à mensagem original. Para verificar a autenticidade do documento, deve ser gerado um novo resumo a partir da mensagem que está armazenada, e este novo resumo deve ser comparado com a assinatura digital, para isso, é necessário descriptografar a assinatura obtendo o *hash* original. Caso ele seja igual ao *hash* recém gerado, a mensagem está íntegra.

Outro processo criptográfico é o selo cronológico que atesta a referência de tempo à assinatura.

3. Certificado Digital

É um documento eletrônico com assinatura digital que possibilita comprovar a identidade de uma pessoa, uma empresa ou um site, através da associação dessa pessoa ou entidade ao uso de uma chave pública, a fim de que transações on-line e a troca eletrônica de documentos, mensagens e dados, tenham validade jurídica.

3.1 Tipos de Certificados

Esta certificação é um documento eletrônico que pode está armazenado em um computador ou em uma mídia, como um *token* ou *smart* card. Os tokens são dispositivos de mídia removível, somente para leitura. Já os *smartcards* são cartões com chips que armazenam os certificados e são apenas para leitura. Os arquivos eletrônicos contêm os certificados digitais que podem ser salvos em computador específico do proprietário, podendo ser copiado e movido (*Vide* Figura 4).

Figura 4. tokens e smartcards. (e-CPF e e-CNPJ).

Os certificados são diferenciados um dos outros a partir dos aspectos relacionados à sua funcionalidade. Assim, eles são classificados como séries A e S. diante disso, os certificados da série A são o A1, A2, A3 e A4 que são compostos pelos 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.

Já os certificados da série S são o S1, S2, S3 e S4 que são compostos pelos certificados de sigilo, que são usados na codificação de documentos, de bases de dados, de mensagens e de outras informações eletrônicas sigilosas.

Uma característica importante entre os certificados do tipo A1 e S1 é que as chaves privadas ficam armazenadas no próprio computador do usuário e os tipos A2, A3, A4, S2, S3 e S4, as chaves privadas e as informações referentes ao seu certificado ficam armazenadas em um *smart card* ou um *token* (ver Tabela 1). Assim, para acessar essas informações você usará uma senha pessoal determinada no momento da compra.

Tabela 1. Características dos Certificados quanto ao Tipo.

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

Os certificados digitais contêm algumas informações importantes tais como: informações referentes à entidade para o qual o certificado foi emitido (nome, email, CPF/CNPJ, PIS etc.), a chave pública referente à chave privada de posse da entidade especificada no certificado, o período de validade, a localização do "centro de revogação" (uma URL para download da LCR, ou local para uma consulta OCSP) e a(s) assinatura(s) da(s) AC/entidade(s) que afirma que a chave pública contida naquele certificado confere com as informações contidas no mesmo (*Vide* Figura 5).

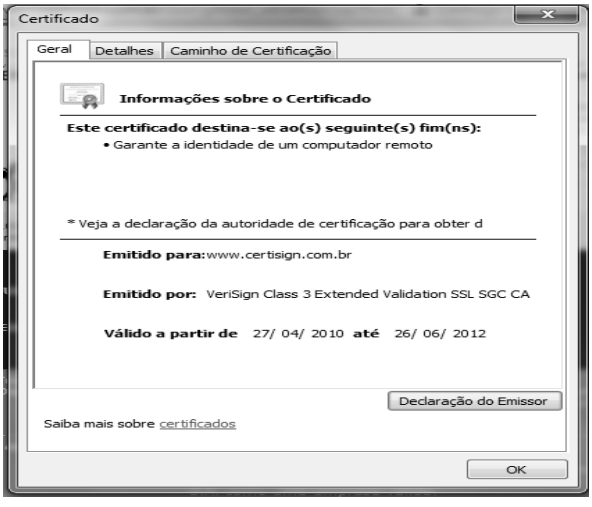

Figura 5. Certificação digital da Certisign (autoridade credenciada).

Uma peculiaridade no Brasil em relação aos certificados é que os mais utilizados são o A1 e A3. O primeiro certificado (A1) possui um menor nível de segurança, pois, é gerado e armazenado no computador do usuário. Assim, os dados são protegidos por uma senha de acesso e somente com essa senha é possível acessar, mover e copiar a chave privada a ele associada. O segundo certificado (A3) possui um nível de segurança

entre médio e alto, pois, ele é gerado e armazenado em um hardware criptográfico que pode ser um cartão inteligente ou um *token*. Desse modo, apenas o detentor da senha de acesso pode utilizar a chave privada, e as informações não podem ser copiadas ou reproduzidas.

Tais certificados digitais são concedidos por uma autoridade certificadora (AC), que é uma entidade considerada confiável pelas partes envolvidas numa comunicação e/ou negociação.

4. ENTIDADES CERTIFICADORAS

A identificação de entidade que emitiu o certificado é obrigatória a fim de comprovar a autenticidade do certificado e para que o mesmo possa ser aceito e utilizado por pessoas, empresas e governos.

4.1 ICP (Infra-Estrutura de Chave Pública)

Uma Infra-estrutura de Chaves Públicas (ICP) é um conjunto formado por várias entidades, padrões técnicos e normas, elaborados para suportar um sistema criptográfico com base em certificados digitais.

A infra-estrutura de chave pública é uma arquitetura de confiabilidade que as empresas podem especificar para suas redes corporativas e políticas de segurança. Ela possibilita transações via internet tão seguras quanto negócios entre pessoas Silva (2004).

4.2 ICP-Brasil

No Brasil existe a ICP-Brasil, que foi criada após a percepção da Presidência da República de que deveria regulamentar as atividades de certificação digital no País. Foi instituída pela Medida Provisória 2.200-2, de 24 de Agosto de 2001, que criou o Comitê Gestor da ICP-Brasil, a Autoridade Certificadora Raiz (AC-Raiz), que é o Instituto Nacional de Tecnologia da Informação (ITI), e as demais entidades que compõem a estrutura da ICP-Brasil. A partir dessa medida, também foram regulamentadas as atividades das entidades integrantes dessa ICP.

O modelo de Infraestrutura adotado pela ICP-Brasil foi o de Certificado com Raiz única, ou seja, é competência do ITI credenciar os demais participantes da cadeia, supervisionar e fazer auditoria dos processos. Essa AC-Raiz é a executora das Políticas de Certificados e das normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil tendo a função de emitir certificados digitais.

A entidade emissora ou autoridades Certificadoras (AC) emitem, suspendem, renovam ou revogam certificados, vinculando pares de chaves criptográficas ao respectivo titular. A AC é o principal componente de uma Infra-Estrutura de Chaves Públicas e é responsável pela emissão dos certificados digitais.

Sob o ponto de vista jurídico, na emissão do certificado devem-se envolver duas entidades: uma Autoridade de Registro (AR) e uma Autoridade Certificadora (AC). O papel da AR é o de requisitar a emissão de certificados digitais da AC, que são transmitidos através de uma conexão segura, que usa um protocolo de transmissão específico para transmitir dados criptografados Gonzaga (2004).

Uma AC tem a função de associar uma identidade a uma chave e "inserir" esses dados em um certificado digital com AC raiz e ACS credenciadas.

Abaixo da AC-Raiz, existem ainda as Autoridades Certificadoras de 1º Nível diretamente ligadas a AC-Raiz e mais abaixo, relacionadas às ACs de 1º Nível, existem, ainda, as Autoridades Certificadoras de 2º Nível. Essas ACs de 1º e 2º Níveis são responsáveis por gerar certificados digitais obedecendo as políticas e normas aplicadas pela AC-Raiz (*Vide* Figura 6).

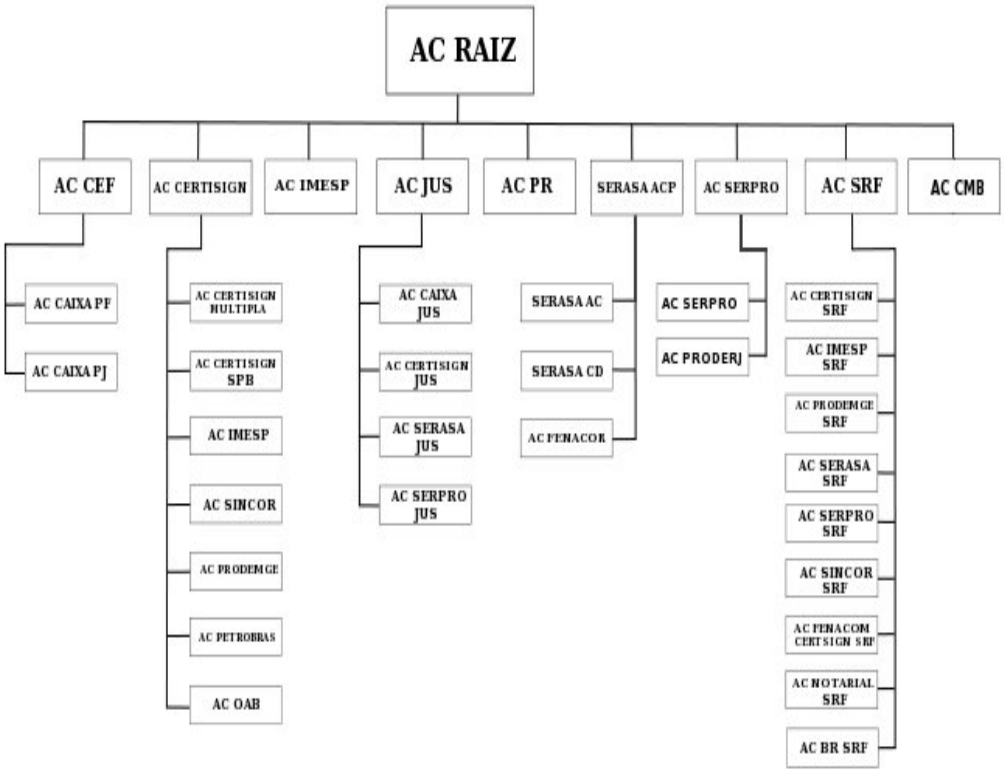

Figura 6. Infra-estrutura de chaves da ICP-Brasil.

4.3 Como Adquirir um Certificado no Brasil

Atualmente conseguir um certificado digital é simples, ou seja, basta efetuar o pedido preenchendo um formulário no site da Autoridade Certificadora com os dados de pessoa física ou jurídica, após isso, são geradas uma senha e um par de chaves. A chave pública gerada é encaminhada à autoridade certificadora e servirá para identificá-lo em todos os processos relacionados ao certificado, durante o período de validade. Faz-se necessário memorizar a senha escolhida, pois, ela será requisitada para instalar o certificado. Após realizar a solicitação, deve-se imprimir 03 cópias do termo de titularidade que é gerado automaticamente na última página do processo. E assim, após esta etapa deve-se escolher uma das opções de pagamento, e de posse do comprovante de pedido/pagamento deve comparecer a um posto da Autoridade de Registro credenciada para efetuar a autenticação presencial. O comparecimento no posto da AR é a única relação física no caminho do certificado e é nesta etapa que será entregue sua chave privada, que é pessoal e intransferível. Agora é só instalar o certificado digital no computador, seguindo as orientações do Agente de Registro.

4.4 Cuidados com o certificado

Ao utilizar um certificado digital será requerida uma senha, a mesma que foi gerada no momento da gravação do certificado. Em caso de perda da senha, não há como recuperá-la ou substituí-la e o certificado estará inválido.

Em caso de perda da mídia armazenadora ou da senha, é necessário realizar algumas atividades, são elas: solicitar a revogação do certificado digital invalidado, mas certifique-se antes que a chave pública anterior não mais está sendo usada; solicitar um novo certificado digital, com encargos por conta do proprietário, seguindo os mesmos procedimentos adotados para aquisição do certificado digital anterior; solicitar a alteração dos acessos, anteriormente vinculados ao certificado digital inutilizado, vinculando-os ao novo certificado digital e atualizar a chave pública eventualmente distribuída, substituindo-a pela nova, pertencente ao novo certificado digital.

5. Conclusão

Com a utilização da certificação digital cada vez mais em evidência e com a crescente evolução dos processos tecnológicos envolvidos, surge a percepção da importância deste mecanismo para garantir segurança na realização das transações eletrônicas, pois a cada dia surgem mais opções de serviços virtuais que se norteiam no uso desta tecnologia.

A projeção de crescimento do uso desta ferramenta de segurança vem reforçar a sua credibilidade e eficácia no combate de casos de crimes on-line. Ao enviar uma mensagem eletrônica, por exemplo, o receptor poderá comprovar que o mesmo foi realmente enviado por determinada empresa ou pessoa, garantindo assim a segurança de seu computador, por sua vez o remetente terá a certeza de que apenas a pessoa a quem foi enviada a mensagem, terá acesso ao conteúdo. Assim, os usuários da internet terão mais segurança ao efetuar compras em sites de comércio eletrônico e os comerciantes poderão realizar transações bancárias com maior tranquilidade.

Visto que o desenvolvimento desse trabalho procurou expor o instrumento certificado digital de modo compreensivo, temos como trabalho futuro detalhar o funcionamento dos certificados usados pelo Governo Federal nos principais órgãos públicos do País, como por exemplo, o projeto da Nota Fiscal Eletrônica (NF-e), Consulta a dados na Receita Federal, o Registro de Identidade Civil – RIC. Além disso, é necessário fazermos uma pesquisa de opinião pública em relação à facilidade ou não trazida por meio destas certificações à sociedade de uma formal geral.

6. Referências

BRASIL, Presidência da República, Casa Civil, Subchefia para Assuntos Jurídicos. MEDIDA PROVISÓRIA Nº2.200-2, DE 24 DE AGOSTO DE 2001. Disponível em: <https://www.planalto.gov.br/ccivil_03/MPV/Antigas_2001/2200-2.htm> Acesso em: 16 junho 2011.

CARTILHA Certificação Digital. São Paulo: Associação dos Registradores Imobiliários de São Paulo, [200-?]. Disponível em: <https://www.oficioeletronico.com.br/Downloads/CartilhaCertificacaoDigital.pdf> Acesso em: 29 junho 2011.

CERTISIGN (A sua identidade na rede). Certificação Digital. Disponível em: <http://www.certisign.com.br/certificacao-digital/por-dentro-da-certificacao-digital>. Acesso em: 8 Ago 2011.

Gonzaga, Diogo C. (2004). Certificação Digital. Disponível em: <http://br-linux.org/tutoriais/002209.html>. Acessado em: 10 de Junho de 2011.

INFOWESTER. Entendendo a certificação digital. Disponível em: <http://www.infowester.com/assincertdigital.php>. Acesso em: 9 de Ago de 2011.

ITI (Instituto Nacional de tecnologia da Informação). O que é Certificação Digital. Disponível em: <http://www.iti.gov.br/twiki/pub/Certificacao/CartilhasCd/brochura01.pdf>. Acesso em: 10 Ago 2011.

Ottoni, Márcia Benedicto. Certificação Digital e Segurança. São Paulo: Certisign, 2005.

Silva, Lino Sarlo da. Public Key Infrastructure – PKI: conheça a infra-estrutura de chaves públicas e a certificação digital. São Paulo: Novatec, 2004.

Silva, Luiz Gustavo Cordeiro da, et al. Certificação Digital: Conceitos e Aplicações. Rio de Janeiro: Editora Ciência Moderna, 2008.