A CERTIFICAÇÃO DIGITAL NA ICP-BRASIL

DIGITAL CERTIFICATION ON THE ICP-BRASIL

CERTIFICACIÓN DIGITAL EN LA ICP-BRASIL

OSEIAS GOMES RIBEIRO[1]

EUSTÁQUIO APARECIDO MARINHO[2]

SAMÁRIS RAMIRO PEREIRA[3]

SUELI APARECIDA LODDI[4]

PAULO SCHROEDER DE SOUZA[5]

Recebido em setembro de 2010. Aceito em novembro de 2010.

---

[1] Graduando em Informática para Gestão em Negócios pela Faculdade de Tecnologia de São Bernardo do Campo, licenciado em Matemática pela Universidade Estadual Paulista.

[2] Graduando em Informática para Gestão em Negócios pela Faculdade de Tecnologia de São Bernardo do Campo, Técnico em Eletrotécnica pela Escola Técnica Federal de São Paulo.

[3] Graduada em Matemática com ênfase em Processamento de Dados e em Tecnologia com ênfase em Técnicas Digitais. Mestre em Informática. Doutoranda em Informática na Saúde pela UNIFESP. Professora da Faculdade de Tecnologia de São Bernardo do Campo.

[4] Graduada em Matemática com ênfase em Processamento de Dados. Mestre em Administração pela Universidade Municipal de São Caetano do Sul. Professora da Faculdade de Tecnologia de São Bernardo do Campo.

[5] Doutor em Engenharia Biomédica. Pós-Doutorando pela Politécnica da Universidade de São Paulo. Diretor da Faculdade de Tecnologia de Santos.

A CERTIFICAÇÃO DIGITAL NA ICP-BRASIL

RESUMO

Com o progresso da Tecnologia da Informação, surgiu a necessidade de se interagir com o mundo digital de maneira segura. Uma solução para esta necessidade é a Certificação Digital, que assegura a autenticidade das informações que transitam pela rede. Entre outras funções, ela é utilizada para transações com o governo brasileiro como na utilização de NF-e, e-CPF e e-CNPJ; no IRPF, IRPJ e na solicitação remota de documentos jurídicos. Nestes casos, há a necessidade de utilização da Infraestrutura de Chaves Públicas Brasileira, a ICP-Brasil. O presente artigo apresenta os principais conceitos da certificação digital, contribuindo assim para uma utilização correta e segura da certificação digital.

PALAVRAS-CHAVE: Assinatura digital. Certificação digital. Chave criptográfica pública. ICP.

DIGITAL CERTIFICATION ON THE ICP-BRASIL

ABSTRACT

There is the need of interaction in the digital world in a safe way with progress in Information Technology. A solution to this need is the digital certificate, which ensures authenticity to information that pass thru the network. Among other functions, it is used for transactions with the Brazilian government as the use of NF-e, e-CPF and e-CNPJ; in IRPF, IRPJ and in the remote request of legal documents. In these cases it is needed to use the Brazilian Public Key Infrastructure, the ICP-Brazil. This paper presents the main concepts in digital certification, contributing to the correct and safe use of this technology.

KEYWORDS: Digital certificate. Digital signature. Public encryption key. PKI.

LA CERTIFICACIÓN DIGITAL EM LA ICP-BRASIL

RESUMEN

Con el avance de la Tecnología de la Información, hay la necesidad de interactuarse con o mundo digital de manera segura. Una solución para esta necesidad es la Certificación Digital, que garantiza la autenticidad de las informaciones que transitan por la red. Entre otras funciones, ella es utilizada para transacciones con el gobierno brasileño como en la utilización de NF-e, e-CPF y e-CNPJ; en el IRPF, IRPJ y en la solicitación remota de documentos jurídicos. En estos casos, hay la necesidad de utilización de la Infraestructura de Claves Públicas Brasileña, la ICP-Brasil. Este artículo presenta los principales conceptos de la certificación digital, contribuyendo así para una utilización correcta y segura de la certificación digital.

PALABRAS-CLAVE: Assinatura digital. Certificação digital. Chave criptográfica pública.

ICP.

1 INTRODUÇÃO

Com o crescimento da demanda em segurança de transações comerciais que ocorrem por intermédio de redes eletrônicas, públicas ou privadas, a certificação digital desponta como tecnologia que fornece confiabilidade e segurança para usuários e que, com outras tecnologias, é utilizada como instrumento para estabelecer um adequado fluxo de informações e regulamentações na comunicação entre empresas e sociedade.

A certificação digital é um conjunto de técnicas e processos que conferem um nível adequado e desejado de segurança possibilitando não somente o controle, no que tange aspectos tecnológicos, mas também administração segura do conteúdo de uma mensagem, da autoria e da data em que foi assinada entre as partes envolvidas. A utilização de um certificado digital apresenta vantagens como (CERTISIGN, 2010):

Controle de acesso a aplicativos e assinatura eletrônica de documentos,através de identificação e comprovação segura da identidade em questão;

Garantia de autenticidade do documento ou mensagem;

Validade jurídica dos documentos assinados impossibilitando o repúdio à autoria e ainda;

Possibilidade de sigilo e privacidade fazendo com que apenas o servidor ou destinatário de uma mensagem interprete corretamente a informação.

Para que a certificação digital garanta integridade, autenticidade, confidencialidade e não-repúdio das informações assinadas, por meio eletrônico, é necessário que uma terceira parte ou uma estrutura de mediação ateste e emita os certificados necessários. No Brasil, essa infraestrutura governamental é a Infraestrutura de Chaves Públicas Brasileira, ICP-Brasil (2010), sendo ela que estabelece o sistema de certificação digital governamental que se relaciona com as empresas (*Government to Business*- G2B) e com o cidadão (*Governmemt to Citizen* - G2C).

O objetivo deste artigo é apresentar os principais conceitos da certificação digital e da gestão da ICP-Brasil, contribuindo para sua utilização correta e segura. A metodologia (LAKATOS e MARCONI, 2005) utilizada foi composta por diversas pesquisas bibliográficas referentes ao tema, constituídas de livros, artigos de periódicos e materiais disponibilizados na Internet, em páginas criteriosamente selecionadas pelos autores quanto ao conteúdo e autoria. Essas pesquisas foram analisadas e sintetizadas considerando a experiência vivenciada pelos autores em mais de vinte e cinco anos de assessoria a empresas nesse tema.

2 ASSINATURA E CERTIFICAÇÃO DIGITAL

Assinatura manuscrita é um sinal gráfico pessoal emitido de próprio punho para firmar um documento indicando sua aprovação e/ou autoria. Assinatura digitalizada é representação gráfica de uma assinatura manuscrita em meio digital (PEREIRA, 2008).

Assinatura digital é a tecnologia que garante eletronicamente a integridade, o não-repúdio e a autenticação dos dados e do signatário. Ela ainda pode, opcionalmente, garantir confidencialidade. Legalmente a aceitação da assinatura digital não é universal, mas sua aceitação tem evoluído velozmente.

Hipoteticamente, enquanto uma assinatura manuscrita é única para cada indivíduo, uma assinatura digital não. Além de estar relacionada a uma entidade emissora, uma assinatura digital se relaciona à transação em questão, sendo única para cada transação realizada pelo emissor e tendo sempre um prazo de validade determinado (PEREIRA, 2008).

Para possibilitar a utilização de assinaturas digitais em transações comerciais e governamentais, foi criada e aperfeiçoada ao longo do tempo, uma Infraestrutura de Chaves Públicas (ICP), envolvendo padronizações, normas, procedimentos, orientações e leis. Envolvem ainda órgãos como Autoridades Registradoras (AR), Autoridades Certificadoras (AC) e outros.

A Certisign (2010) explica aos usuários, entre outros detalhes, que não há necessidade de se processar a assinatura digital da mensagem completa. Para tornar o custo de tempo de processamento da assinatura digital eficiente, ela é gerada a partir do valor de hash[6] da mensagem.

A certificação digital certifica a autenticidade da assinatura digital combinando aspectos tecnológicos e jurídicos. Ela vem sendo utilizada no Brasil para atribuir valor legal a documentos eletrônicos e para garantir sua eficácia probatória (PEREIRA, 2008).

---

[6] Uma função de *hash h* é definida por uma entrada *x* de tamanho arbitrário finito, considerando $|x|$ o tamanho máximo da entrada, a saída $h(x)$ com tamanho fixo de $|h(x)|$ bits, com $|x| >> |h(x)|$. Nas funções de *hash* criptográficas, dado um valor de *hash*, é intratável encontrar-se outra mensagem que origine o mesmo valor de *hash:* se o tamanho em bits do valor de *hash* for *n*, a probabilidade de $h(x)$ ser um valor em específico é de 2^{-n} e a probabilidade de colisão é de $2^{-n/2}$ (PEREIRA, 2008).

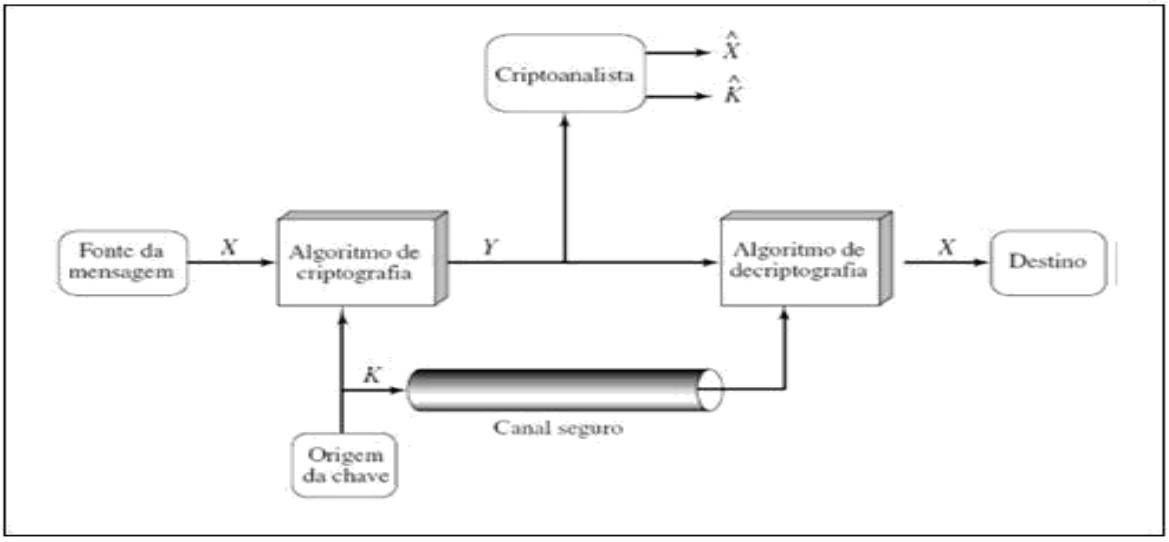

Figura 1 - Modelo de criptografia simétrica. Fonte: STALLINGS (2007)

Os ambientes de infraestruturas de chaves públicas precisam estar sob critérios de segurança rigorosos, desde a AC até o usuário do certificado digital. Nesta visão, uma infraestrutura de chave pública é uma combinação de tecnologia e processos que vinculam a identidade do titular da chave privada sua respectiva chave pública, utilizando a tecnologia assimétrica de criptografia (PEREIRA, 2008).

3 TECNOLOGIA DA CERTIFICAÇÃO DIGITAL: CRIPTOGRAFIA

Como definido por Silva et al. (2008), a "[...] criptografia é a ciência de fazer com que o custo de adquirir uma informação de maneira imprópria sejamaior do que o custo obtido com a informação". Assim, entende-se a importância da criptografia para proteger informações sensíveis ou valiosas, tais como a senha de acesso a uma conta bancária, a fórmula de um produto revolucionário ou uma estratégia militar.

Para o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil – CERT (2010), uma chave criptográfica simétrica, para ser considerada segura, deve ter pelo menos 128 bits, já uma chave pública deve ter pelo menos 1024 bits, sendo que os militares usam 4096 bits, o que requer milhares de anos de ataque de força bruta (esgotamento de todas as possibilidades de uma chave criptográfica) por um computador.

Entende-se como sistema criptográfico, um conjunto de técnicas para embaralhar ou cifrar mensagens de forma que, aparentemente, se tornem ilegíveis e que, posteriormente, se possa obter a

mensagem original por meio do texto embaralhado (STALLINGS, 2007).

No processo de cifragem e decifragem, é utilizada uma sequência de cálculos matemáticos, conhecidos como algoritmo criptográfico, ilustrado na Figura 1. Um algoritmo é a base para que o sistema criptográfico determine como o texto será criptografado, e também é requerida uma chave criptográfica para cifrar um texto original utilizando o algoritmo criptográfico e para recuperar um texto original a partir do texto cifrado.

Para a compreensão da certificação digital, é necessário o conhecimento do conceito de criptografia de chave simétrica e de criptografia de chave pública.

3.1 Criptografia simétrica

A criptografia de chave secreta ou também chamada de chave simétrica utiliza a mesma chave para cifrar ou decifrar uma mensagem. Seu funcionamento é apresentado na Figura 2.

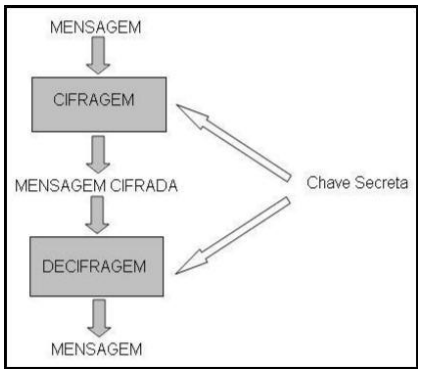

Figura 2 – Cifragem com de Chave Secreta Fonte: Dos autores

Os algoritmos de chave simétrica têm como característica a rapidez na execução. Porém, não permitem assinatura nem certificação digital.

Existe ainda o problema da necessidade de distribuição das chaves, as quais serão utilizadas pelos usuários e, deve ser feita de forma segura. O problema está na dificuldade de enviar a chave gerada para o usuário, pois o canal de comunicação ainda não é seguro.

Outro problema é o uso de chaves secretas diferentes para cada tipo de comunicação e também para cada mensagem, o que faz com que o seu gerenciamento se torne muito complexo (NAKAMURA, 2007).

---

[7]O criptoanalista pode escolher determinada(s) mensagem(ns) e ter acesso ao(s) par(es) (criptograma; mensagem).

3.2 Criptografia de chave pública

Pereira (2009) descreve que a criptografia de chave pública, também chamada de criptografia assimétrica, envolve o uso de 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 a chave pública não é secreta e pode ser distribuída e compartilhada com qualquer pessoa.

Uma chave pública e sua correspondente chave privada possuem uma relação matemática distribuída e compartilhada, distribuída e compartilhada com qualquer pessoa. Uma chave pública e sua correspondente chave privada possuem uma relação matemática, mas é computacionalmente inviável descobrir a chave privada a partir de uma chave pública.

A chave pública e sua chave privada associada são comumente chamadas de par de chaves criptográficas. Devido a sua relação matemática, uma mensagem criptografada com uma chave pública pode ser decifrada com sua chave privada correspondente e uma mensagem que foi criptografada com a chave privada pode ser decifrada com sua chave pública correspondente (processo utilizado na certificação digital).

No entanto, o algoritmo assimétrico é cerca de 60 a 70 vezes mais lento que os algoritmos simétricos, pois a chave privada possui um tamanho em bits maior e um algoritmo mais complexo, portanto um tempo de processamento maior (RSA, 2010). O fluxo principal desse processo é apresentado na Figura 3.

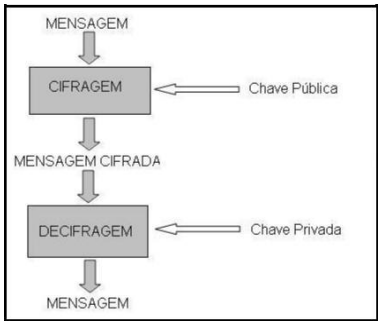

Figura 3 – Cifragem com chave pública (Fonte: Dos autores)

O algoritmo de chaves públicas RSA é o mais amplamente aceito e confiável nas implementações de assinaturas digitais. Esta situação tende a durar, pois sua utilização tem crescido ainda mais desde que expirou a validade da sua patente norte-americana, em 2000 (PEREIRA, 2008).

Na criptografia assimétrica inserida no processo de assinatura digital, é utilizado primeiro a chave privada, pelo emissor da assinatura, o qual estará executando o algoritmo de ciframento, mas com o objetivo de

assinar o documento, e não cifrá-lo. Posteriormente, qualquer usuário que deseje verificar a autenticidade da assinatura digital em questão, irá processar o algoritmo de deciframento, mas com o objetivo de verificar a assinatura digital, e não de decifrar o documento. Portanto, a criptografia assimétrica permite a utilização das chaves nos dois sentidos. O fluxo desse processo é exemplificado na Figura 4.

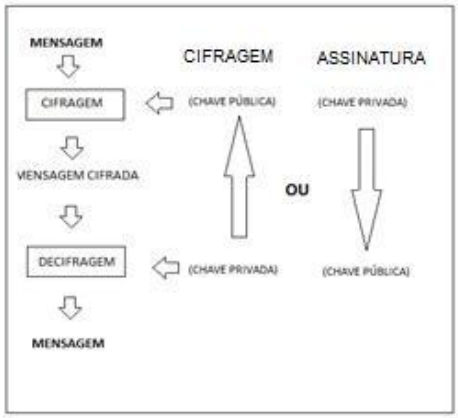

Figura 4 – Cifragem/assinatura com chave pública

(Fonte: Dos autores)

4 INFRAESTRUTURA DE CHAVES PÚBLICAS

Uma Infraestrutura de Chaves Públicas (ICP) regulamenta a certificação de assinaturas digitais, possibilitando um certificado digital com validade jurídica. Ela combina aspectos tecnológicos e jurídicos, para atribuir valor legal a documentos eletrônicos garantindo sua eficácia probatória (não-repúdio) e se aplicando para documentos eletrônicos de diferentes tipos de informação tais como textos, imagens ou vozes.

A ICP-Brasil (ICP-Brasil, 2010) é controlada pelo Instituto Nacional de Tecnologia da Informação, o ITI (ITI, 2010), que é a autoridade certificadora raiz (primeira autoridade da cadeia de certificação brasileira – AC Raiz), uma autarquia federal vinculada à casa Civil da Presidência da República que tem como função credenciar as Autoridades Certificadoras (ACs) e as Autoridades Registradoras (ARs) por meio de supervisão e auditorias. A ICP-Brasil é responsável pelo conjunto de técnicas, práticas e procedimentos a serem implementados pelas organizações, com o objetivo de estabelecer os fundamentos técnicos e metodológicos de um sistema de certificação digital baseado em chaves públicas.

Pelas leis brasileiras em vigor, toda AC deve utilizar-se de chave RSA de comprimento de no mínimo 2048 bits, devendo este valor ser revisto periodicamente, de acordo com as novas definições publicadas pelo CG ICP-Brasil (Comitê Gestor da ICP-Brasil).

Existem diversos tipos de certificados digitais, sendo classificados quanto à necessidade de segurança da assinatura digital e necessidade de sigilo, mas independente do nível de segurança ou de sigilo, a AC deve assegurar que o tamanho das chaves das entidades a ela ligadas seja de no mínimo 512 bits,sendo recomendável o uso de pelo menos 1024 bits (ICP-BRASIL, 2010).

Embora as regras de infraestrutura de chaves públicas não sejam universais, no Brasil, nenhuma AC, nem mesmo a AC-Raiz tem acesso à chave privada da entidade proprietária de um par de chaves públicas. Este par de chaves (pública e privada) deve ser gerado pela entidade usuária, a qual deve zelar por sua chave privada, sendo responsável judicialmente por sua utilização mesmo que por terceiros.

A fim de garantir a segurança da infraestrutura de chaves públicas, há a necessidade de cuidados na distribuição dos pares de chaves (pública e privada), evitando assim ataques como o ataque MITM *(Man-In-The-Middle /* Ataque por Homem ao Meio). Neste tipo de ataque, o invasor interage entre duas partes que estejam se comunicando, sem que nenhuma das partes perceba o que está ocorrendo (PEREIRA, 2008).

Suponha que um adversário obtenha um par de chaves (pública/privada) para utilizar no ataque e que, de alguma forma, ele consiga trocar a chave pública de *A* pela sua. O adversário passa a monitorar a linha de comunicação. Quando um criptograma for enviado para *A*, o adversário intercepta o canal tendo acesso ao criptograma e não deixa que ele chegue ao destinatário *A*. O adversário decifra o criptograma, altera a mensagem conforme sua conveniência e a envia para *A* com a chave pública correta de *A*, de forma que *A* consiga abrir a mensagem. Da mesma forma, quando *A* enviar uma assinatura digital, o adversário intercepta a mensagem enviada e a substitui por outra que ele cria conforme sua conveniência e divulga como se fosse assinada por *A*.

Para evitar esse tipo de ataque, as ACs operam como uma terceira parte confiável, certificando a validade do par de chaves no momento da sua criação. Outra necessidade técnica para a segurança em assinaturas digitais é a utilização de algum esquema de codificação, que processe algum tipo de codificação na mensagem que será assinada, tornando-a pseudoaleatória e

evitando assim, possíveis ataques por mensagem escolhida[7].

5 SEGURANÇA POR MEIO DE CERTIFICAÇÃO DIGITAL

Garantir a segurança com a proteção das informações dos sistemas corporativos deve ser a preocupação constante de uma empresa, visando assegurar que estas não sejam acessadas por terceiros não autorizados ou corrompidas por estarem suscetíveis às ações de vírus provenientes do sistema interno de mensagens ou pela internet, que podem resultar em prejuízos devastadores para a organização. Assim como as empresas, pessoas comuns também prezam pelo sigilo de suas informações pessoais e das armazenadas em seu computador.

Segundo o CERT (2010), foram comunicados cerca de 300.000 ataques à segurança da informação, de janeiro a junho de 2009, e boa parte destes incidentes está ligada a ações de cibercriminosos para capturar dados de internautas, como números de cartão de crédito, senhas bancárias e de informações trocadas através de redes sociais, seja verbalmente ou por escrito em salas de bate-papo e outras redes.

O maior desafio na indústria mundial de software é prover soluções no espaço de tempo mais curto possível, a partir da descoberta de determinada ameaça ou problema. As corporações devem criar um plano que contemplem levantamento dos ativos na empresa, avaliação dos riscos e vulnerabilidades a que estão expostas e, a partir deste, investir na infraestrutura de tecnologia com a aquisição de ferramentas, instalação de soluções e recomendações de uso (STALLINGS, 2007).

A segurança tem valor estratégico participando das decisões de mercado integrada na forma de ofertas de produto e serviços com novas tecnologias, relatórios com informações recentíssimas e privilegiadas e agregando valor a qualquer decisão ou operação estratégica baseada em confidencialidade, autenticidade e/ou integridade. Assim, a segurança da informação demanda diversas aplicações no que se refere à infraestrutura tecnológica (hardware e software) como antivírus, firewall, varredura de vulnerabilidades, Rede Virtual Privada (VPN), criptografia, autenticação e sistemas Antispam. Para alcançar resultados relevantes, a

[7]O criptoanalista pode escolher determinada(s) mensagem(ns) e ter acesso ao(s) par(es) (criptograma; mensagem).

segurança da informação precisa envolver tecnologias, processos e pessoas em um trabalho contínuo e persistente (CERT, 2010).

O certificado digital é a tecnologia que garante a identificação segura de uma mensagem ou transação eletrônica com confidencialidade, integridade e validade jurídica. Cada vez mais a certificação digital estará presente nas diversas esferas do governo contribuindo para a democratização dos serviços públicos, oferecendo redução de tempo, comodidade e principalmente segurança por conta da certificação digital (VOLPI, 2001).

Em segurança da informação, é importante considerar aspectos tecnológicos, metodologias de controle e autorizações de acordo com a necessidade. 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 que estiver sendo utilizada).

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, a 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 (NAKAMURA, 2007).

A tecnologia de certificação digital permitiu a reavaliação dos negócios on-line, pela validação jurídica, assegurando a comunicação no ambiente virtual com privacidade,

segurança e respaldo jurídico, em exemplos como: e-CPF, e-CNPJ e NF-e. Outras aplicações que também utilizam certificação digital são (CERTISIGN, 2010):

- Acompanhamento da declaração de imposto de renda;
- Regularização fiscal na Receita Federal;
- Solicitação remota de documentos jurídicos (ofícios, certidões de escrituras de imóveis, contratos registrados, certidões de nascimento, casamento ou óbito);
- Segurança de acesso em sites institucionais;
- Garantia da autoria e envio de e-mails;
- Utilização de certificados digitais nos tribunais através da criação da Autoridade Certificadora do Judiciário (AC-JUS);
- Sistema de Pagamentos Brasileiros (SPB);
- Programa Universidade para Todos (ProUNI);
- O Instituto Nacional de Seguridade Social (INSS).

A ICP-Brasil é referência em termos de infraestrutura, pois apresenta exigências e controles rígidos e bem implementados como Declaração de Práticas de Certificação, Políticas de Certificado e Políticas de Segurança. A Tabela 1 apresenta alguns desses controles.

Como os conceitos das atividades de uma Autoridade Certificadora estão associados ao conceito de confiança, o processo de auditoria e fiscalização periódica representa um dos instrumentos que facilita a percepção e transmissão de confiança à comunidade de usuários, dado que o objetivo desses processos é verificar a capacidade da AC em atender aos requisitos da ICP-Brasil.

O resultado das auditorias operacionais e fiscalizações são itens fundamentais para a manutenção da condição de credenciada. As auditorias são planejadas, determinando-se o objetivo, frequência e abrangência da auditoria, realizadas periodicamente pela AC Raiz ou por terceiros por ele autorizados, conforme documentos aprovados pelo Comitê Gestor da ICP-Brasil (ITI, 2010; SILVA *et al*., 2008).

Tabela 1 – Principais controles da ICP-Brasil

Controle / Descrição
Declaração de Práticas de Certificação (DPC) Documento que descreve obrigações, responsabilidade e controles de segurança da AC, AR e dos titulares do certificado.

Políticas de Certificado (PC) Define as políticas e tratam das particularidades do tipo específico de certificado.
Políticas de Segurança (PS) Descreve as diretrizes de segurança adotadas pela AC e define o escopo da segurança das entidades em relação a riscos e integridade. A política de segurança é abrangente e contempla requisitos de segurança humana, física, lógica e da tecnologia em recursos criptográficos.

Fonte: Adaptado de Silva et al., (2008)

6 INFRAESTRUTURA DE CHAVES PÚBLICAS (ICP): MODELO BRASILEIRO E AUSTRALIANO

O conhecimento da infraestrutura de certificação digital da Austrália tem sua relevância por apresentar um modelo diferente da infraestrutura do Brasil e ambas são referências mundiais.

O modelo de ICP implantado pelo governo brasileiro pode ser verificado na ICP-Brasil, que é composta por um conjunto de entidades, padrões técnicos e regulamentos, elaborados para suportar um sistema criptográfico com base em certificados digitais, visando proporcionar maior segurança nas transações eletrônicas e incentivar a utilização da Internet como meio de realização de negócios.

As entidades participantes da ICP-Brasil são auditadas previamente ao credenciamento, para verificar se estão aptas a desenvolver suas atividades conforme os regulamentos. A ICP-Brasil oferece diversas garantias aos titulares e usuários de certificados (SILVA et al., 2008):

- O par de chaves criptográfico deve ser gerado sempre pelo próprio titular e sua chave privada de assinatura é de seu exclusivo controle, uso e conhecimento;
- Validade jurídica dos documentos assinados com processo de certificação da ICP-Brasil;
- Utilização de padrões internacionais para os certificados, algoritmos criptográficos e tamanhos de chaves; procedimentos de segurança física, lógica e de pessoal;
- Obrigatoriedade de declaração em repositório público às práticas de segurança utilizadas em todos os seus processos; de contratação de seguro para a cobertura de responsabilidade civil decorrente das atividades e a

validação pessoal dos titulares para a obtenção de certificados;

- Auditorias para a obtenção e manutenção do credenciamento;
- Armazenamento dos dados por no mínimo trinta anos para atender legislações específicas de guarda de documentos.

O governo australiano, por sua vez, implantou o modelo de ICP (chamado de PKI – *Public Key Infrastructure*, neste caso), como um recurso para a realização de serviços on-line, como, por exemplo, num processo de compra ou contratação de produtos e serviços ou a utilização da estrutura pelo Departamento de Impostos. Esta estratégia é implementada através da tecnologia denominada *Gatekeeper*, vista como importante fortalecedor de confiança no processo (SILVA et al., 2008).

Embora não haja legislação que relacione a ICP Australiana ao *Gatekeeper*, este foi implementado e funciona administrativamente regulado pelos contratos entre AGIMO (*Australian Government information Management Office*), departamento de administração e finanças e os provedores de serviço credenciados (SILVA et al., 2008).

Como na infraestrutura brasileira, a relação entre o assinante e a autoridade certificadora é disciplinada por contrato incluindo obrigações, responsabilidades e atribuições da responsabilidade civil dos assinantes. A autoridade certificadora terá seus próprios termos e condições contidas nestes acordos que incorporam, geralmente, as Políticas de Certificado e a Declaração de Práticas de Certificação (SILVA et al., 2008).

As terceiras partes confiáveis[8], no aspecto legal, podem ter que confiar nos parâmetros da justiça comum com respaldo sobre a legislação relativa à negligência, declaração inexata e adulterada ou leis que regem contratos (SILVA et al., 2008).

Ainda conforme Silva et al. (2008), existem nove critérios que são avaliados e certificados por agências do governo de acordo com sua área de atuação e políticas (descentralização de responsabilidade para finalizar o processo) que são:

- Conformidade com a Política de Compras e Contratações do Governo Federal;
- Política da Segurança;
- Segurança Física;
- Avaliação de Tecnologia;

- Administração da Autoridade de Certificação;
- Investigação de Pessoal;
- Políticas da Autoridade de Certificação;
- Contratos e
- Considerações à Privacidade.

7 CONSIDERAÇÕES FINAIS

A necessidade de instrumentos e critérios que permitam a regulamentação e a existência de um adequado fluxo de informações entre Estado, empresas e a sociedade, levaram a adoção da tecnologia da certificação digital, a qual utiliza criptografia e políticas de gestão, como um meio de controle e de autorizações, que fornece confiabilidade e segurança para os usuários do meio digital.

No Brasil, a infraestrutura governamental de Chaves Públicas é a ICP-Brasil (ICP-Brasil, 2010), entendida como um conjunto de técnicas e processos que propiciam mais segurança às comunicações e transações eletrônicas, utilizada para acessar serviços on-line e assinar documentos eletrônicos com a possibilidade de certificação da autenticidade de dados e de entidades, conferindo ainda, a validade jurídica do documento.

A ICP-Brasil é referência em termos de infraestrutura, pois apresenta exigências e controles rígidos e bem implementados, sedimentando sua presença na política tecnológica do governo, definindo suas competências e sua governança, demonstrando sua importância e confiabilidade perante a sociedade.

Apesar de referência, é preciso conhecê-la e entendê-la para utilizá-la da forma correta e, desta forma, desfrutar da segurança e confiabilidade que ela proporciona.

REFERÊNCIAS

CERT. **Centro de estudos, resposta e tratamento de incidentes de segurança no Brasil.** URL: <http://www.cert.br/>. Acesso em 15/09/2010.

CERTISIGN. Site institucional. **Certificação digital.** URL: <http://www.certisign.com.br/certificacao-digital>. Acesso em 03/09/2010.

ICP-Brasil. **Infraestrutura de chaves públicas brasileira.** URL: <http://www.icpbrasil.gov.br/>. Acesso em 03/09/2010.

ITI. Instituto Nacional de Tecnologia da Informação. **Autoridade certificadora brasileira raiz.** URL: <http://www.iti.gov.br/twiki/bin/view/ITI/ Apresentacao>. Acesso em 10/09/2010.

LAKATOS, E. M. e MARCONI, M. A. **Fundamentos de metodologia científica**. 6ª ed. São Paulo: Atlas. 2005.

NAKAMURA, E. T. **Segurança de redes em ambientes cooperativos.** 1ª ed**.** São Paulo: Novatec Editora. 2007.

PEREIRA, S. R. **O sistema criptográfico de chaves públicas RSA**. Dissertação apresentada à Universidade Católica de Santos, UNISANTOS. 2008.

PEREIRA, S. R. **Certificação digital através do algoritmo RSA.** FaSCciTech. Periódico Eletrônico da Fatec São Caetano do Sul. Ano 1. Número 1. 10/2009. URL: <http://www.fatecsaocaetano.edu.br/fascite ch/ed001/>. Acesso em 08/09/2010.

RSA Security Inc. **Laboratórios RSA.** URL: http://www.rsasecurity.com/rsalabs/. Acesso em 20/09/2010.

SILVA, L. G. C.; SILVA, P. C.; BATISTA, E. M.; HOMOLKA, H. O.;AQUINO, I. J. S.; LIMA, M. F. **Certificação digital: conceitos e aplicações, modelos brasileiro e australiano.** 1. ed. São Paulo: Editora Ciência Moderna, 2008.

STALLINGS, W. **Criptografia e segurança de redes.** 4ª edição Ed. Prentice Hall, 2007.

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