UM ESTUDO SOBRE CERTIFICADOS DIGITAIS COMO SOLUÇÃO DE SEGURANÇA DA INFORMAÇÃO

Emerson Henrique Soares Silva

Prof. Ms. Rodrigo Almeida dos Santos

Associação Paraibana de Ensino Renovado - ASPER

Coordenação de Ciência da Computação e Processamento de Dados

E-mail: emerson.hss@gmail.com

rodrigo.almeida@gmail.com

Resumo: *Os Certificados Digitais são tecnologias emergentes no que diz respeito a segurança das informações que circulam pelas redes de computadores e internet. O Certificado Digital funciona como uma carteira de identidade virtual. Um documento eletrônico que contém dados do titular como nome, e-mail, CPF, dois números denominados chave pública e privada, além do nome e da assinatura da AC (Autoridade Certificadora) que o emitiu. Neste estudo serão apresentados os certificados digitais e serão abordados alguns serviços de segurança da informação que a utilização desses certificados oferece, tais como: Integridade da informação, Confidencialidade da informação, Autenticidade da informação e a Não-Repúdiação. Dessa forma, este estudo visa apresentar os certificados digitais e sua importância na área da segurança da informação. Temos também o objetivo de apresentar como os certificados afetam negócios através do aumento na segurança dos serviços públicos e privados que envolvem transações financeiras e de títulos, além de transações com informações sigilosas e confidenciais.*

Palavras-chaves: Segurança da Informação; Certificados Digitais; Infra-estrutura de chave pública; Assinaturas Digitais; ICP-Brasil;

1. Introdução

A informação é um bem valioso e disputado, e a *internet* se tornou um meio de acelerar e movimentar as informações. A internet proporcionou um aumento na agilidade dos processos e na velocidade com que as informações circulam. Mas esse advento tão importante para as comunicações, também vem trazendo muitos benefícios para os negócios e para a administração pública, através da movimentação financeira e de documentos on-line, que, antes, só poderiam ser feitas de forma pessoal, isto é, com presença física. Exemplos disso são o e-CPF e o e-CNPJ, que são certificados digitais credenciados pela Receita Federal do Brasil e são utilizados no acesso ao e-CAC, Centro Virtual de Atendimento ao Contribuinte, que é um serviço oferecido por esse órgão, onde é possível emitir e solicitar documentos que antes teriam que ser solicitados ou emitidos fisicamente nas sedes de RFB ou em órgão habilitados para esse fim. Porém, vulnerabilidades existentes em aplicações nesta grande rede, bem como nos protocolos de comunicações das redes de computadores, permitem a ocorrência de

ataques que podem ser através de invasões, roubo de informações por interceptação, fabricação de informações não verídicas, interrupção de serviços, modificação de informações, etc. Essas ocorrências mantêm o uso da internet bastante tímido para fins de negócios e transação de informações confidenciais.

Esse estudo visa apresentar o uso dos Certificados Digitais como solução de segurança da informação, com o objetivo de demonstrar quais as garantias que essa tecnologia pode oferecer para contribuir ainda mais com a aceleração dos processos e da troca de informações de forma segura através da internet, e apresentar aplicações como a *Assinatura Digital* de documentos eletrônicos, que, utilizando a analogia de Gisele Ribeiro [3], funciona equivalente aos selos e carimbos de cartórios utilizados no reconhecimento de firma de documentos, pois tem o mesmo objetivo de validar documentos.

2. Certificados Digitais

Os certificados digitais surgiram no mercado como produto de segurança por volta de 1999. A proposta é evitar, através do conceito de *criptografia assimétrica* e da possibilidade de assinar digitalmente um documento, alguns problemas clássicos de segurança, garantindo a autenticidade, integridade, confidencialidade e a não-repudiação de informações que transitarão nas redes de computadores.

2.1 O que são os Certificados Digitais?

Os certificados digitais são documentos eletrônicos que identificam uma pessoa, uma instituição, uma máquina ou aplicações na internet [3]. É um arquivo eletrônico que obedece ao padrão X.509. Esse padrão, que está atualmente na versão 3, foi criado pela ITU (*International Telecommunication Union*) e adaptado para internet pelo grupo PKIX da *Internet Engineering Task Force* (IETF).

Um documento X.509 contém a seguinte anatomia:

- Campo de Versão, onde contém a informação da versão do X.509, atualmente na versão 3;
- Campo Número Serial, que pode não ser globalmente único, mas é ao menos no âmbito da autoridade que emitiu o certificado;
- Tipo de algoritmo, campo que contém a informação do tipo de algoritmo criptográfico utilizado pelo emissor do certificado, como também o tipo da função *hash* criptográfica usada no certificado;
- Nome do Titular do certificado, que recebeu o certificado;
- Nome do emitente, autoridade que emitiu ou assinou o certificado;
- Período de Validade, no formato “Não antes de” e “Não depois de”;
- Informações de chave-pública da entidade, algoritmo e a chave;
- Assinatura da autoridade que emitiu;
- Identificador da chave do titular;
- Identificador da chave do emitente;

- e Atributos ou Extensões, que podem ser informações de caráter referente ao objetivo de certificado.

A figura 1 mostra um exemplo de certificado no padrão X.509.

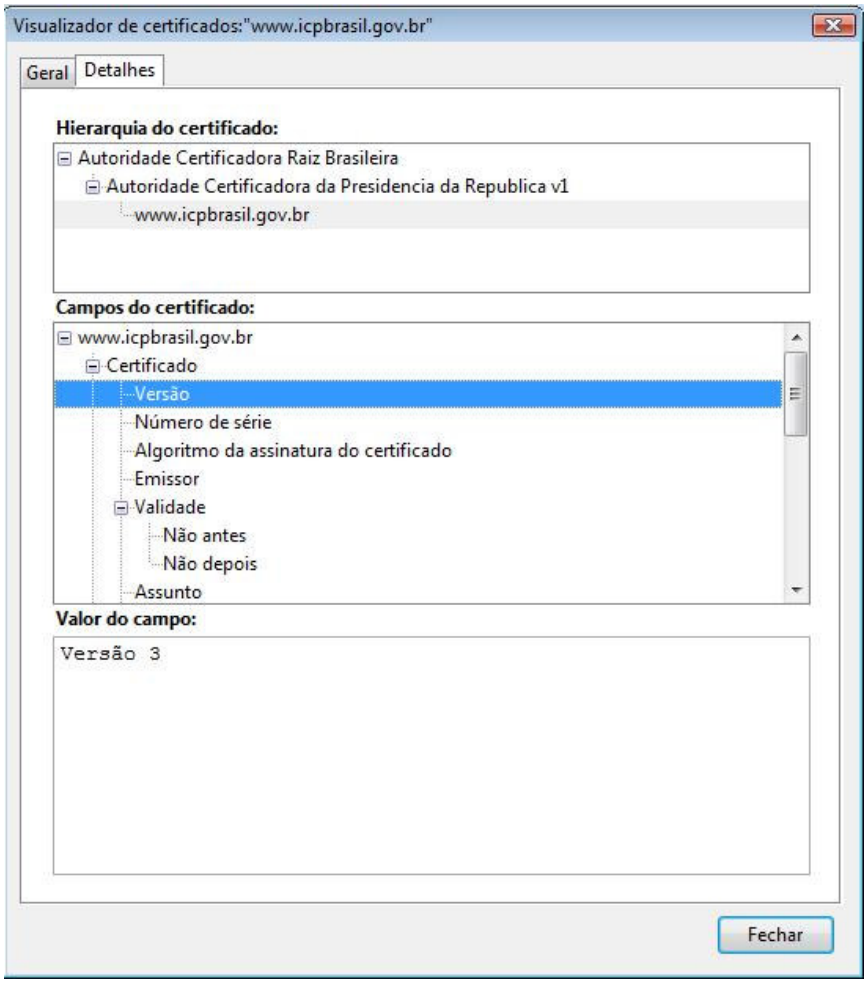

Figura 1 - Exemplo de certificado digital - Padrão X.509

No momento da emissão é relacionado a um certificado digital, um par de chaves criptográficas. Essas chaves são baseadas em algoritmos criptográficos assimétricos. Na *criptografia assimétrica*, as duas chaves, correspondentes ao par, são diferentes, ou seja, $k_p \neq k_e$, onde k_p é a chave pública e k_e é a chave privada. Usando esse algoritmo criptográfico, documentos encriptados com a chave privada k_e do portador do certificado só poderão ser decriptados com a chave pública k_p relacionada ao certificado e vice-versa, ou seja, documentos encriptados com a chave pública k_p do certificado só poderão ser decriptados pelo portador da chave privada k_e do mesmo.

Esses certificados são emitidos por instituições chamadas *Autoridades Certificadoras* (AC) [9]. Essas organizações são responsáveis por relacionar ao certificado no momento emissão, o par de chaves criptográficas, a chave pública e a privada, que são emitidas pelo próprio usuário no momento da aquisição do certificado. As chaves são responsáveis por cifrar documentos para que sejam transportados de forma sigilosa e indecifrável pela rede.

Uma aplicação interessante e bastante usada dos certificados digitais é a *Assinatura Digital* de documentos. A assinatura digital é uma combinação dos conceitos de função *hash* e de chaves pública e privada. A função *hash* é uma técnica de criptografia de uma única via, isto é, uma vez criptografado um documento utilizando uma função *hash*, não é possível obter o documento original a partir do valor gerado pela criptografia, valor conhecido como "valor *hash*". O valor *hash* é de tamanho fixo e gerado a partir de um algoritmo matemático complexo que usa como base os caracteres do documento.

A *Assinatura Digital* funciona da seguinte forma:

"Um usuário possui um documento e a chave pública da pessoa ou entidade para quem ele irá enviar o documento. O usuário utilizará uma função *hash* para criptografar o documento, então obterá um código cifrado de valor fixo. O usuário anexará ao documento o valor *hash* adquirido criptografando-o utilizando a chave pública do destinatário, que ao receber irá decriptar com sua chave privada o anexo do documento e gerar novamente o valor *hash* do documento, comparando-o com o mandado anexo ao documento, se estiver igual terá a certeza que a assinatura é válida. Se o documento for sigiloso o remetente deverá criptografar todo o documento junto com o valor *hash*, pois assim evitará que este seja interceptado." [7]

2.2 Quais critérios de segurança são garantidos pelos Certificados Digitais?

O uso da criptografia assimétrica nos certificados digitais garante a confidencialidade do documento criptografado, já que cifrado ele não será legível por quem não possuir a chave equivalente a que cifrou o documento.

O emissor de um documento o criptografa usando a sua chave privada, que é única e intransferível, isso dará a garantia ao receptor da não-repudiação do documento, ou seja, o receptor terá a certeza de que a chave utilizada para ler o documento é a chave pública do emissor, pois nenhuma outra chave conseguiria decodificar o documento.

A Assinatura Digital garante a integridade e a autenticidade do documento assinado. A comparação do valor *hash* criado pelo emissor do documento com o criado pelo receptor após o recebimento, permite ao receptor saber se o documento é válido, isto é, se permanece íntegro e original.

Para garantir os quatro serviços de segurança citados, a confidencialidade, a integridade, a autenticidade e a não-repúdiação, o seguinte processo pode ser feito entre duas entidades:

"Uma entidade A deseja enviar um documento confidencial a uma entidade B. A entidade A assina digitalmente o documento que será enviado para B gerando o valor *hash* do documento e criptografando este valor com a chave pública de B (K_p^B), o que garante que apenas B que possui a sua chave privada (K_e^B) poderá ter acesso ao conteúdo original. Então A anexa a assinatura cifrada ao documento e criptografa usando a sua chave privada K_e^A (Chave Privada de A). B deve possuir a chave pública de A (K_p^A), pois só assim poderá ler o conteúdo. Isso já garante a autenticidade do documento e a não-repúdiação. Após decriptar o conteúdo com a chave pública de A, B encontrará um pacote cifrado com sua chave pública (K_p^B) e então poderá decriptar com sua chave privada K_e^B, gerar novamente o valor *hash* do documento e comparar com o valor anexo, verificando se o documento possui uma assinatura válida."

Assim demonstramos como os Certificados Digitais podem garantir 4 (quatro) serviços fundamentais de segurança e a origem das informações. Em um futuro muito

próximo, os certificados digitais poderão vir a ser utilizados para controle de acesso em aplicações, como Internet Banking, por exemplo, como já é usado no e-CAC, Centro Virtual de Atendimento ao Contribuinte, que disponibiliza vários serviços da Receita Federal tanto para pessoa física como para pessoa jurídica que possuam o e-CPF ou e-CNPJ, certificados emitidos pelas ACs habilitadas pela SRF (Secretaria da Receita Federal) ou credenciadas pela ICP-Brasil (Infra-estrutura de Chaves Públicas Brasileira), para pessoas físicas e jurídicas, respectivamente. O e-CAC oferece serviços de sigilo fiscal em que só o próprio contribuinte pode ter acesso através do e-CPF ou do e-CNPJ. A ICP-Brasil será detalhada no capítulo 3 deste estudo.

2.3 Tipos de Certificados Digitais

Quanto à tecnologia de armazenamento, os certificados podem ser armazenados em três tipos de mídia: *tokens*, *smartcards* (cartões inteligentes) e *arquivos eletrônicos*. Veja exemplos de *tokens* e os *smartcards* na figura 2. Os *tokens* são dispositivos de mídia removível, apenas para leitura. Os *smartcards* são cartões com chips que armazenam os certificados e também são apenas para leitura. Os *arquivos eletrônicos* contêm os certificados digitais e podem ser salvos em computador específico do seu dono, porém esse pode ser copiado e movido.

Figura 2 - Exemplo de tokens e smartcards. (e-CPF e e-CNPJ fornecidos pela Certisign)

A Infra-estrutura de Chaves Públicas Brasileira classifica os tipos de certificados digitais quanto ao uso e nível de segurança implantada em: Certificados das Séries A e Séries S.

Os certificados da *série A* são o A1, A2, A3 e A4. Essa série 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.

Os certificados da *série S* são o S1, S2, S3 e S4, e essa série 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 de certificados mostrados acima são, ainda, diferenciados quanto ao uso, nível de segurança implantado e pela validade. A tabela 1 abaixo apresenta um pouco da diferença entre esses tipos de certificados.

Tipo de Certificado	Chave Criptográfica			Validade Máxima (anos)
	Tamanho de bits	Processo de Geração	Mídia Armazenadora	
A1 e S1	1024	Software	Arquivo	1
A2 e S2	1024	Software	Smartcard ou token, sem capacidade de geração de chave	2
A3 e S3	1024	Hardware	Smartcard ou token, com capacidade de geração de chave	3
A4 e S4	2048	Hardware	Smartcard ou token, com capacidade de geração de chave	3

Tabela 1 - Tipos de Certificados quanto ao uso, nível de segurança e validade. (*Fonte*: RIBEIRO [3])

Os tipos de certificados mais comuns são o A1 e o A3. O A1 possui um nível de segurança menor e é gerado e armazenado no computador do usuário, e os dados são protegidos por uma senha, em que somente com essa senha é possível acessar, mover e copiar a chave privada associada ao certificado. O A3 possui um nível de segurança de médio a alto, é armazenado em um hardware criptográfico, que pode ser um smartcard ou token, onde os dados não podem ser copiados ou reproduzidos e apenas o detentor da senha pode acessar a chave privada do certificado.

3. ICP (Infra-estrutura de Chave Pública) ou PKI (Public Key Infrastructure)

Uma Infra-estrutura de Chaves Públicas (ICP) ou PKI (Public Key Infrastructure) é um conjunto de entidades, padrões técnicos e regulamentos, elaborados para suportar um sistema criptográfico com base em certificados digitais. [1]

No Brasil existe a ICP-Brasil, já citada anteriormente, 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, 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 [1].

3.1 Estrutura da ICP-Brasil

A ICP-Brasil possui uma Autoridade Certificadora Raiz, que é o ITI. É a primeira autoridade na cadeia de certificação. Essa AC-Raiz é a executora das Políticas de Certificados e das normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil, e não é autorizada a emitir certificados digitais. [9]

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. Essa estrutura é apresentada na figura 3.

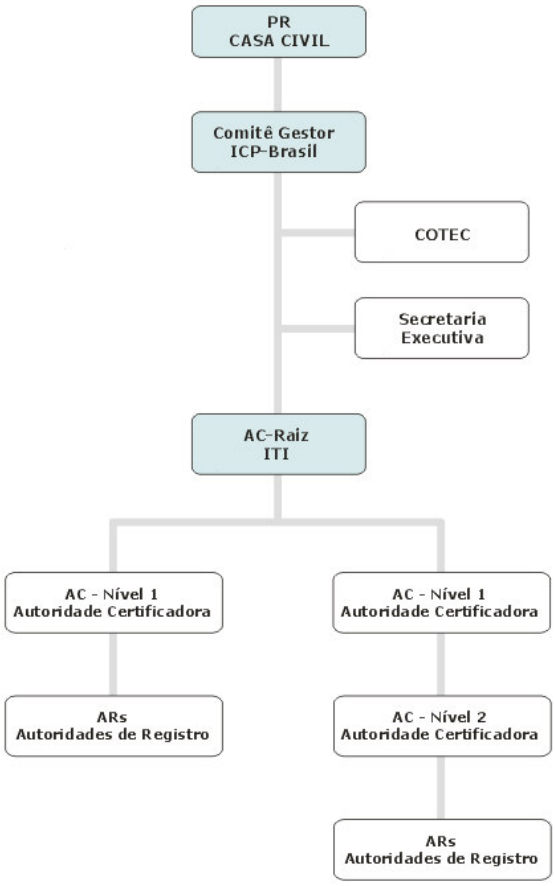

Figura 3 - Organograma da ICP-Brasil (*Fonte*: ICP-Brasil[1])

3.2 Teia de confiança

Uma entidade ao obter um certificado emitido por uma AC entra para uma rede de confiança chamada *teia de confiança*, em que todos confiam na AC-Raiz e esta confia nas ACs de níveis inferiores vinculadas a ela, então todos passam a confiar nessas ACs. Essas ACs de 1º e 2º Níveis certificam apenas as entidades nas quais elas confiam, e por fim todos passarão a confiar nas entidades que possuem certificados da ICP-Brasil.

As Autoridades Certificadoras solicitam, através de Autoridades de Registros (ARs) credenciadas, que a entidade que deseja seu certificado, apresente vários documentos a uma AR para provar sua existência perante o Estado. Ao confirmar que a entidade é realmente quem diz ser, ela estará apta a receber o seu certificado. Esse certificado então será nacionalmente reconhecido, permitindo que a entidade certificada faça uso dele para assinar documentos eletrônicos, realizar negócios pela internet, entre outras diversas coisas, com muito mais segurança.

Algumas Autoridades Certificadoras de 1º e 2º Níveis são apresentadas na figura 4 abaixo.

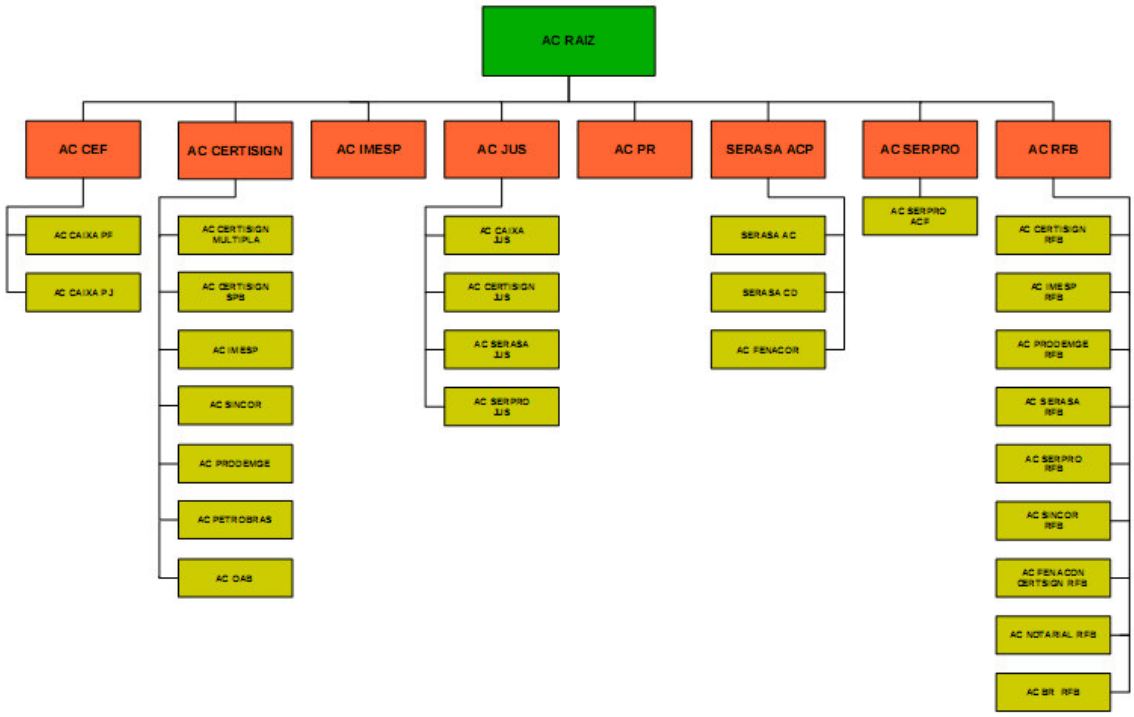

Figura 4 - ICP-Brasil ACs de 1º e 2º Níveis – No topo está a AC-Raiz, no nível abaixo estão as ACs de 1º Nível e mais abaxio estão as ACs de 2º Nível (*Fonte*: ITI[2])

As ACs de 1º Nível atualmente credenciadas na ICP-Brasil são: a AC-CEF (Autoridade Certificadora da Caixa Econômica Federal), AC CERTISIGN, AC IMESP (Autoridade Certificadora da Imprensa Oficial do Estado de São Paulo), AC JUS (Autoridade Certificadora da Justiça), AC PR (Autoridade Certificadora da Presidência da República), AC SERASA, AC SERPRO e AC RFB (AC da Receita Federal do Brasil).

3.3 Obtendo um Certificado Digital

Para obter um certificado digital, basta entrar no site de uma AC, fazer o pedido e comparecer a uma AR credenciada para realizar a autenticação presencial. Esse é o único passo presencial no caminho da certificação digital.

No site da AC, o primeiro passo é preencher um formulário com os dados de pessoa física ou jurídica. Se o certificado desejado for do tipo A3, antes de preencher o formulário é necessário adquirir um dispositivo de armazenamento (*token* ou *smartcard*) e instalar o *driver* do dispositivo no computador. Ao fazer o pedido é gerado o par de chaves (pública e privada) e uma senha. A chave pública será enviada a AC e servirá para identificar o seu dono em todos os processos relacionados ao certificado, durante o período de validade. A senha deve ser memorizada, pois será utilizada para instalar o certificado. Após efetuar a solicitação, é necessário imprimir 3 cópias do termo de titularidade que é gerado automaticamente na ultima página do processo de solicitação.

O próximo passo é escolher a forma de pagamento e, de posse do comprovante de pagamento da solicitação, é hora de se dirigir ao posto da AR credenciada pela AC escolhida levando duas cópias de toda a documentação exigida e as três cópias do termo de titularidade, esse ultimo só deverá ser assinado na presença do Agente Registrador no posto da AR. É nessa etapa que o solicitante de certificado receberá a sua chave privada, que é pessoal e

intransferível. As demais transações serão realizadas on-line. Pronto agora é só instalar o seu certificado digital seguindo as orientações do Agente de Registro. As orientações devem variar de acordo com o tipo de certificado escolhido. [3]

3.4 Cuidados com o Certificado

O certificado digital possui uma senha que não pode ser recuperada ou alterada, por tanto não facilite o acesso a sua senha, e não a perca. Mas se isso acontecer você deve solicitar a revogação do seu certificado, invalidando totalmente o anterior, deve arcar com os encargos para obter um novo certificado, tendo que passar por todos os processos de aquisição, como feito no primeiro certificado adquirido, e deve se preocupar em inutilizar a chave pública referente ao certificado anterior e distribuir uma nova chave pública referente ao seu novo certificado. Também deve, é claro, solicitar a alteração dos acessos aos serviços vinculados ao certificado anterior para que possam ser acessados pelo novo certificado.

4. Alguns exemplos de uso dos certificados digitais

Está ficando cada vez mais comum, você acessar um site que mostre na tela do *browser* uma mensagem solicitando que você examine um certificado, ou mesmo encontrar aplicações que possuem serviços de segurança e acrescentam ao *browser* (navegador *web*) um pequeno cadeado na parte inferior. Geralmente esses sites possuem um certificado digital comum, que é o certificado digital emitido para servidores web. O certificados emitidos para servidores web garantem que o conteúdo do site que é executado no servidor, só possa ser acessado por quem possuir a chave pública do servidor, e o conteúdo passado pelo programa cliente (*web browser*) ao servidor só possa ser acessado exclusivamente pelo servidor, dono da chave privada.

Outra forma de uso dos certificados digitais se dá em webmails. Uma pessoa física que possui um certificado pode utilizá-lo também com um aplicativo cliente de correio eletrônico, desde que esse aplicativo suporte o uso dos certificados. Algumas ACs oferecem soluções com uso de certificação digital para sistemas de correio eletrônico corporativo. A maioria dos provedores de correio eletrônico gratuitos e pagos, ainda não oferece suporte aos certificados digitais no acesso via interface *web*, deixando esse trabalho para as aplicações clientes de correio eletrônico.

Mais uma aplicação para os certificados digitais é o controle de acesso, que substitui a forma mais comum atualmente, com a digitação de usuário e senha, como já é feito no e-CAC.

Além dessas utilizações citadas aqui, existem muitas outras que já estão sendo utilizadas, como também existirão outras, que ainda não foram implementadas e talvez outras que nem foram pensadas.

5. Conclusão

Esse estudo apresentou os certificados digitais como uma solução de segurança da informação capaz de proteger as informações contra problemas de segurança bastante conhecidos, como a interceptação de informações, modificação das mesmas e fabricação de falsas informações. O estudo mostrou que esses certificados oferecem serviços de segurança, como integridade, confidencialidade, autenticidade e não-repudiação de informações, que são garantidos pelo uso de algoritmos criptográficos assimétricos, algoritmos esses que implementam os conceitos de chaves públicas e privadas.

Foi apresentada uma teia de confiança que envolve os portadores de certificados e a ICP-Brasil, que é o centro dessa teia e que garante uma estrutura de confiança para a emissão de certificados digitais.

A partir desse estudo podemos concluir que o uso dessa tecnologia tende a se expandir com o desenvolvimento de aplicações para as iniciativas públicas e privadas, como aplicações bancárias, *e-commerce*, *e-Gov*, etc., focadas na integridade, confidencialidade e autenticidade das informações, em diversas formas de transações realizadas sobre as redes de computadores.

6. Referências

[1] Infra-estrutura de Chave Pública Brasileira - ICP-Brasil. Disponível em: <https://www.icpbrasil.gov.br> Acesso em: 11 nov. 2008.

[2] Instituto Nacional de Tecnologia da Informação - ITI. Disponível em: <http://www.iti.gov.br/twiki/bin/view/Certificacao/CertificadoConceitos> Acesso em: 11 nov. 2008.

[3] RIBEIRO, Gisele. **Como funciona o certificado digital.** HowStuffWorks (ComoTudoFunciona). Disponível em: <http://informatica.hsw.uol.com.br/certificado-digital.htm> Acesso em: 09 nov. 2008.

[4] Certisign. Disponível em: <https://www.certisign.com.br/> Acesso em: 12 nov. 2008.

[5] Movimento Internet Segura. Portal INTERNET SEGURA. Disponível em: <http://www.internetsegura.org > Acesso em: 15 nov. 2008.

[6] MATOS, Manoel. **Ser quem diz ser. Esta é a questão.** Moviento Internet Segura. Portal INTERNET SEGURA. Disponível em: <http://www.internetsegura.org/noticias/22112006.asp> Acesso em: 15 nov. 2008.

[7] ALECRIM, Emerson. **Assinatura Digital e Certificação Digital.** Info Wester. 2005. Disponível em: <http://www.infowester.com/assincertdigital.php> Acesso em: 09 nov. 2008.

[8] JANUÁRIO, Larissa. **Tutorial: Saiba tudo sobre certificação digital.** W News. 2007. Disponível em: <http://wnews.uol.com.br/site/noticias/materia_especial.php?id_secao=17&id_conteudo=264> Acesso em: 09 nov. 2008.

[9] BRASIL, Presidência da República, Casa Civil, Subchefia para Assuntos Jutídicos. **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 nov. 2008.