Comparativo entre estratégias para emissão, gerenciamento e utilização de certificados digitais[16]

Josivan B. Silva, Thiago G. Silva, Elionildo S. Menezes, Lívio L. Ribeiro

Instituto Federal de Educação, Ciência e Tecnologia da Paraíba (IFPB)
Av. 1º de Maio, 720, Jaguaribe, João Pessoa - PB - CEP: 58.015-430

{van.jp01,thiago.gouveia.da.silva}@gmail.com, elionildo@ifpb.edu.br,
livioribeiro@outlook.com

Abstract. *This document provides a comparison between three strategies for issuance, management and use of digital certificates, addressing the advantages and the best application for each strategy. The first strategy is the implementation of proper infrastructure with a self-signed CA, the second presents the creation of an infrastructure with CA affiliated with the Brazilian Public Key Infrastructure (ICP-Brazil) while the third refers to the acquisition of certificates for specialized companies affiliated with ICP-Brazil for use of key people in the organization.*

Resumo. *Este documento traz um comparativo entre três estratégias para emissão, gerenciamento e utilização de certificados digitais, abordando as vantagens e a melhor aplicação para cada estratégia. A primeira estratégia trata da implementação de infraestrutura própria com uma CA auto assinada, a segunda apresenta a criação de uma infraestrutura com CA filiada à Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) enquanto a terceira refere-se à aquisição de certificados de empresas especializadas filiadas à ICP-Brasil para utilização de pessoas chave da organização.*

1 Introdução

O advento da informática e das redes de computadores, em particular a Internet, tornou possível produzir e compartilhar informação de forma muito mais eficiente do que era possível utilizando documentos físicos em papel. Contudo, tais benefícios trouxeram alguns problemas: como garantir a identidade do emissor? Como garantir que a mensagem não foi adulterada? Como garantir que apenas o destinatário será capaz de ler a mensagem? Uma abordagem vastamente utilizada como solução para estes problemas é a criptografia assimétrica, através de certificados digitais e dos protocolos *Transport Layer Security* (TLS) e *Secure Socket Layer* (SSL) (TANENBAUM e WETHERALL, 2011, p.501-502).

A utilização de certificados digitais para estes fins requer, todavia, a implementação de uma PKI (infraestrutura de chaves públicas, do inglês *Public Key Infrastructure*), um sistema distribuído complexo responsável por dar informação suficiente aos usuários para que estes possam decidir, de forma sensata, se devem confiar uns nos outros (MARCHESINI e SMITH, 2005).

Tendo em vista a necessidade de uma PKI e a complexidade de sua implementação, este trabalho discute três estratégias para emissão, gerenciamento e utilização de certificados

[16] Trabalho patrocinado pelo Projeto SIM – Sistema de Informação Municipal

digitais, levando em conta aspectos chave como o custo, a validade jurídica, a infraestrutura necessária e a facilidade de administração de cada implementação.

Por fim, é apresentado um caso de uso onde duas estratégias são combinadas gerando um cenário híbrido capaz de usufruir das vantagens de duas abordagens.

2 Infraestrutura de Chaves Públicas

Na criptografia assimétrica, há a necessidade de verificar se a chave pública de uma entidade (indivíduo, empresa etc.) ao qual deseja se comunicar é legítima. Isso é feito através de um terceiro confiável que verifica a autenticidade da chave. De acordo com Kurose e Ross (2006, p. 540) este terceiro confiável que certifica chaves públicas pertencentes a pessoas, empresas e outras organizações é chamado de autoridade certificadora, ou CA (do inglês, *Certification Authority)*.

A CA certifica as chaves públicas por meio da emissão de certificados digitais. Burnett e Paine (2002, p. 146) definem certificados digitais como um conjunto de dados à prova de falsificação que atesta a associação de uma chave pública a uma entidade. Segundo Kohnfelder (1978 apud STALLINGS, 2008, p. 208), um certificado digital contém, essencialmente, uma chave pública mais informações de identificação do proprietário da chave e o *hash* do certificado assinado pela CA.

O conjunto de autoridade certificadora, entidades de suporte, usuários e processos relacionados ao gerenciamento de certificados compõem a Infraestrutura de Chaves Públicas, denominada PKI (do inglês, *Public Key Infrastructure)*, definida por Shirey, BBN Technologies e GTE (2000, p. 135-136, tradução nossa) na RFC 2828 – *Internet Security Glossary* – Um sistema de CAs (e, opcionalmente, RAs e outros servidores e agentes de suporte) que executam algum conjunto de funções de gerenciamento de certificado, gerenciamento de arquivo, gerenciamento de chaves e gerenciamento de *tokens* para uma comunidade de usuários em uma aplicação de criptografia assimétrica.

2.1 Aspectos jurídicos da certificação digital no âmbito do território brasileiro

Antes da apresentação das estratégias, se faz necessária uma breve discussão acerca dos aspectos legais que norteiam esta prática no Brasil visando esclarecer a validade jurídica da utilização de certificados digitais.

A legislação brasileira regulamentou a emissão e utilização de certificados digitais através da Medida Provisória Nº 2.200-2, de 24 de agosto de 2001, instituindo a infraestrutura de chaves públicas brasileira (ICP-Brasil), conforme o art. 1º, e delegando ao Instituto Nacional de Tecnologia da Informação (ITI), a responsabilidade de exercer o papel de autoridade certificadora raiz da hierarquia brasileira.

> Art. 1º: Fica instituída a Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil, para garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras. (Medida Provisória Nº 2.200-2, de 24 de agosto de 2001).

A validade jurídica dos documentos assinados com certificados digitais também é tratada no texto da Medida Provisória 2.200-2, de acordo com o art. 10, parágrafo primeiro, garante a veracidade dos documentos assinados usando certificados emitidos no âmbito do ICP-Brasil.

> Art. 10, § 1º: As declarações constantes dos documentos em forma eletrônica produzidos com a utilização de processo de certificação disponibilizado pela

> ICP-Brasil presumem-se verdadeiros em relação aos signatários, na forma do art. 131 da Lei nº 3.071, de 1º de janeiro de 1916 - Código Civil. (Medida Provisória Nº 2.200-2, de 24 de agosto de 2001).

Porém, a Medida Provisória ainda afirma que os documentos assinados com certificados que são emitidos por autoridades certificadoras fora da ICP-Brasil são válidos juridicamente, desde que, as entidades envolvidas concordem acerca da validade do documento assinado, conforme o art. 10, parágrafo segundo.

> Art. 10, § 2º: O disposto nesta Medida Provisória não obsta a utilização de outro meio de comprovação da autoria e integridade de documentos em forma eletrônica, inclusive os que utilizem certificados não emitidos pela ICP-Brasil, desde que admitido pelas partes como válido ou aceito pela pessoa a quem for oposto o documento. (Medida Provisória Nº 2.200-2, de 24 de agosto de 2001).

Dessa maneira, se uma das partes não reconhecer e/ou aceitar o certificado emitido por uma autoridade certificadora que não faz parte da ICP-Brasil, judicialmente quebrará os princípios de autenticidade e o não-repúdio, ou seja, poderá negar a sua autoria do documento assinado.

Há muitas empresas no exterior e no Brasil que emitem certificados e não fazem parte da ICP-Brasil, como a Verisign (2012). Nesse caso, para assegurar a validade jurídica dos certificados, deve-se previamente estabelecer um contrato formal entre as partes definindo as condições, formas de uso e emissão desses certificados.

Além destas medidas, o governo ainda toma outras providências através do Decreto Nº 3.996, de 31 de outubro de 2001, onde determina que todos os órgãos da administração pública federal só podem usar certificados da ICP-Brasil, conforme está descrito no parágrafo primeiro do art. 2.

> Art 2, § 1º: Os serviços de certificação digital a serem prestados, credenciados ou contratados pelos órgãos e entidades integrantes da Administração Pública Federal deverão ser providos no âmbito da Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil. (Decreto Nº 3.996, de 31 de outubro de 2001)

Vale ressaltar que um decreto federal não atinge estados e municípios. Porém, por interoperabilidade entre os órgãos da administração pública federal, estadual e municipal, este decreto acaba atingindo-os.

Portanto, o governo brasileiro instituiu um modelo de PKI onde os certificados emitidos dentro desta infraestrutura teriam garantias legais. Além disso, ainda se preocupou em não passar o controle da ICP-Brasil a uma empresa privada, atribuindo para si mesmo o seu controle e administração através do ITI.

3 Estratégias

Segundo Nakamura e Geus (2007), em um ambiente heterogêneo, o gerenciamento de certificados digitais e todas as suas funções torna-se extremamente complexo. Em virtude disso, serão abordadas três estratégias para emissão, gerenciamento e utilização de certificados digitais que atendem a diferentes modelos de negócios.

3.1 PKI com CA auto-assinada

A primeira estratégia abordada, referencia autoridade certificadora auto-assinada, ou seja, que assina seu próprio certificado. Esta CA localiza-se no topo de uma infraestrutura de chaves públicas e, segundo Burnett e Paine (2002, p. 164), essa autoridade certificadora é conhecida como raiz.

Há soluções gratuitas baseadas em software livre que permitem a criação, manutenção e gerenciamento de uma infraestrutura de chaves públicas completa. Entre elas, é possível citar o *OpenSSL*, um conjunto de ferramentas de código aberto que implementa os protocolos *TLS* e *SSL* com uma extensa biblioteca de criptografia (OpenSSL Project, 2009), e o *EJBCA PKI*, uma solução para implementação de uma PKI desenvolvida através da tecnologia Java EE, capaz de criar e administrar CAs, emitir e gerenciar certificados digitais e atuar como servidor *Online Certificate Status Protocol* (OCSP) ou gerar tal de forma independente, (EJBCA TEAM, 2012).

Os certificados emitidos por uma CA auto-assinada seriam juridicamente válidos apenas dentro da organização, pois seus membros estariam de acordo quanto às condições, formas de uso e emissão desses certificados, conforme descrito na seção 2.1. Esta CA não seria reconhecida publicamente, ou seja, por outras organizações como uma CA confiável. Sendo assim, seus certificados são considerados não confiáveis e tratados como possíveis violações à segurança da comunicação.

Um cenário viável para fazer uso desta estratégia seria a utilização de certificados digitais apenas em seus processos internos, como tramitação de documentos e e-mail institucional, sem a necessidade de interoperabilidade com outras organizações e validade jurídica.

3.2 PKI com CA vinculada à ICP-Brasil

Esta estratégia consiste na criação de uma Autoridade Certificadora vinculada à ICP-Brasil. Desse modo, os certificados emitidos seriam reconhecidos dentro e fora da organização, eliminando o problema de certificados não confiáveis descrito na seção 3.1. Porém há regras rigorosas que devem ser seguidas para possibilitar o credenciamento de uma CA à hierarquia brasileira.

As normas e resoluções que regem a atuação e funcionamento da Infraestrutura de Chaves Públicas brasileira são aprovadas pelo Comitê Gestor da ICP-Brasil (ITI, 2012a). Dentre os inúmeros requisitos descritos pelo ITI (2012b), vale destacar:

a) Infraestrutura de rede segura com sala-cofre para instalação dos servidores própria ou contratada através de Prestadores de Serviço de Suporte (PSS);

b) Declaração de Práticas de Certificação (DPC);

c) Política de Segurança (PS);

d) Política de Certificado (PC);

A exigência maior, claro, é sobre os recursos de segurança. Implementar e gerenciar uma infraestrutura de rede segura e robusta é um trabalho árduo e de alto custo. Entretanto, a ICP-Brasil permite o "aluguel" desta infraestrutura através da contratação de Prestadores de Serviço de Suporte (PSS). Empresas como Certisign (2012a) oferecem este tipo de serviço com o argumento de economia e facilidade no gerenciamento de uma Infraestrutura de Chaves Públicas.

Com uma CA vinculada à ICP-Brasil, a organização poderia ainda emitir certificados válidos legalmente para entidades finais que não fazem parte da organização e gerar receita com esta prática. Por exemplo, pessoas físicas poderiam adquirir certificados digitais junto à organização para assinar documentos com valor legal, se autenticar em outros serviços, etc.

3.3 Aquisição de certificados de empresas especializadas

Outra forma de obter certificados digitais é através de empresas especializadas, como a Certisign (2011) e a Serasa Experian (2012), que são vinculadas à ICP-Brasil (ITI, 2012c) e consequentemente emitem certificados com validade jurídica no território nacional.

Nesta estratégia, são adquiridos certificados que ficam de posse de pessoas chaves da organização que os utilizam para assinar transações. Existem dois tipos de certificados para assinatura digital (CAIXA, 2012):

O tipo A1, que é fornecido como um arquivo que contém a chave privada e o certificado do usuário. Possui um período de validade de um ano e, para utilizá-lo, é preciso importá-lo na aplicação com a qual se deseja usar.

O tipo A3, que é fornecido através de um *Token* USB ou *smartcard* e possui validade de dois a três anos. O *Token* é similar a um pendrive, sendo acessado através da interface USB, e o *smartcard* é similar a um cartão de crédito e necessita de um leitor específico. A figura 1 demonstra o *Token* (a), *Smartcard* (b) e o leitor de *Smartcard* (c).

a) **b)** **c)**

Figura 1 – a) Token USB, b) *Smartcard* e c) leitor de *Smartcard* (CERTSIGN, 2012b)

4 Comparativo entre as estratégias

Comparando as três estratégias, a primeira apresenta mais benefícios numa situação em que há apenas a necessidade de garantir o sigilo e autenticidade, como, por exemplo, servidores VPN utilizando certificados para realizar a autenticação e gerar um canal seguro de comunicação.

A segunda estratégia se sobressai quando há uma entidade que necessita emitir seus próprios certificados, mas que tenham valor legal, sendo as empresas especializadas em emissão de certificados digitais o exemplo mais claro.

Já a terceira estratégia se mostra mais vantajosa quando há necessidade de um número limitado de certificados. Um exemplo seria uma organização que possui pessoas que assinam transações financeiras.

O Quadro 1 traz um comparativo entre as três estratégias quanto aos critérios:

- Custo – O investimento em infraestrutura, hardware, software e treinamento deve de ser compatível com os recursos disponíveis pela entidade;
- Validade jurídica – Se a entidade precisa garantir o não-repúdio, é necessário que as assinaturas geradas pelos certificados emitidos sejam válidas legalmente no território brasileiro;
- Necessidade de Infraestrutura própria – A implantação de uma infraestrutura de chaves públicas dentro das instalações da entidade irá aumentar a complexidade da solução e pode inviabilizar a utilização da estratégia;

- Facilidade de administração – O nível de abstração dos processos de gerenciamento de certificados tem impacto direto nos custos com treinamento e manutenção da infraestrutura, quando presente.

Quadro 1 - Comparativo entre estratégias.

	Auto Assinada	**Filiação à ICP-Brasil**	**Aquisição de certificados**
Custo	Baixo	Alto	Baixo
Validade Jurídica	Inválido	Válido	Válido
Infraestrutura própria	Necessária	Necessária	Desnecessária
Facilidade de administração	Média	Baixa	Alta

De acordo com os dados apresentados no Quadro 1, a estratégia de utilizar uma PKI com uma CA auto-assinada envolve um custo baixo, pois não há a exigência de uma infraestrutura diferenciada, sendo possível reutilizar a que já existe. Entretanto, os certificados emitidos não terão validade jurídica no território brasileiro.

A utilização de uma PKI com uma CA filiada à ICP-Brasil envolve um custo alto para a implantação de sua infraestrutura e possivelmente mudanças nas políticas de segurança da entidade, tornando a administração da PKI mais difícil, embora os certificados emitidos tenha validade jurídica.

Já a aquisição de certificados de empresas especializadas torna desnecessária a manutenção de uma infraestrutura própria, delegando a administração da infraestrutura para a empresa emissora do certificado, enquanto garante a validade jurídica dos certificados. Porém, a entidade que adquire os certificados não tem controle sobre a emissão e gerenciamento dos certificados.

5 Modelo híbrido, estudo de caso da Proderj

Além de utilizar apenas um método, existe a possibilidade de se combinar duas estratégias e usufruir dos benefícios de cada uma. Por exemplo, uma organização poderia utilizar a primeira estratégia para garantir o sigilo da comunicação entre suas filiais através de conexões VPN ao mesmo tempo em que utiliza a terceira estratégia para assinar documentos e transações.

Como caso de uso, podemos citar o exemplo da Proderj (2012), em que há a utilização de uma CA filiada à ICP-Brasil que emite certificados para ser utilizados quando é necessário garantir a validade jurídica das informações e a interoperabilidade com outras organizações, e uma CA auto-assinada com a finalidade de substituir os documentos em papel, para solicitação de serviços e demais comunicações internas entre Secretarias e Órgãos do Governo do Estado do Rio de Janeiro diminuindo custos com suprimentos.

6 Considerações Finais

A utilização de certificados digitais proporciona importantes benefícios à organização no âmbito da Segurança da Informação, disponibilizando um meio seguro de autenticação de usuários, não-repúdio, confidencialidade e integridade dos dados.

Ao analisar as estratégias para emissão, gerenciamento e utilização de certificados digitais expostas neste trabalho, é possível concluir que a viabilidade de cada uma está

relacionada à estrutura e operações de cada organização. Por exemplo, para empresas cujas operações estão diretamente relacionadas à segurança da informação e que emitem certificados para entidades finais, é mandatória a criação de uma autoridade certificadora própria filiada à ICP-Brasil, enquanto que para organizações que necessitam de certificados com validade legal no território nacional apenas para assinar transações e garantir o não-repúdio, sem emitir certificados para outras entidades, a aquisição de certificados de empresas especializadas que fazem parte do domínio da ICP-Brasil é a opção mais interessante. Já a utilização de uma CA auto-assinada é adequada para organizações que utilizam certificados para autenticação em sistemas internos da entidade, como criptografia e assinatura de e-mails institucionais.

Algumas organizações se favorecem com uso de uma combinação de duas estratégias, adequando às suas necessidades e modelo de negócio o uso das quais julgam mais apropriadas, como foi exemplificado no estudo de caso apresentado na seção 5 acerca da Proderj, onde em seu caso específico se beneficia com a utilização de uma CA auto-assinada e outra incorporada à hierarquia da ICP-Brasil.

Referências

Brasil. (2001). *Decreto Nº 3.996, de 31 de outubro de 2001* . Acesso em 01 de Agosto de 2012, disponível em Dispõe sobre a prestação de serviços de certificação digital no âmbito da Administração Pública Federal.: http://www.planalto.gov.br/ccivil_03/decreto/2001/D3996.htm

Brasil. (2001). Medida Provisória No 2.200-2, DE 24 DE AGOSTO DE 2001. Acesso em 30 de Julho de 2012, disponível em Institui a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências.: https://www.planalto.gov.br/ccivil_03/MPV/Antigas_2001/2200-2.htm

Burnett, S., & Paine, S. (2002). Criptografia e Segurança - O Guia Oficial RSA (1ª ed.). Rio de Janeiro: Campus.

Certisign. (2011). Certisign. Acesso em 27 de Agosto de 2012, disponível em Certisign: http://www.certisign.com.br/

Certisign. (2012a). MPKI - Certsign. Acesso em 31 de Julho de 2012, disponível em Certisign Certificadora Digital S.A: http://www.certisign.com.br/solucoes-corporativas/produtos/gerenciamento-certificados/mpki

Certsign. (2012b). Compra de Hardware Avulso. Acesso em 28 de Setembro de 2012, disponível em Certsign: http://hotsite.certisign.com.br/hardware-avulso/index.htm

EJBCA Team. (2012). Home. Acesso em 24 de Agosto de 2012, disponível em EJBCA - Open Source PKI Certificate Authority: http://www.ejbca.org

ITI. (2012a). Como Funciona. Acesso em 27 de Setembro de 2012, disponível em ICP-Brasil: http://www.iti.gov.br/index.php/icp-brasil/como-funciona

ITI. (2012b). Credenciamento das Entidades Integrantes da ICP-Brasil - DOC-ICP-03 - versão 4.6. Acesso em 27 de Setembro de 2012, disponível em Infraestrutura de Chaves Públicas Brasileira: http://www.iti.gov.br/images/icp-brasil/Normas%20ICP-Brasil/Documentos%20principais/DOC-ICP-03_Credenciamento_das_Entidades_Integrantes_da_%20ICPBrasil_Versao_4.6.pdf

ITI. (2012c). Estrutura. Acesso em 27 de Setembro de 2012, disponível em ICP-Brasil: http://www.iti.gov.br/index.php/icp-brasil/estrutura

Kurose, J. F. & Ross, K. W. (2006). Redes de computadores e a Internet: uma abordagem top-down (3ª ed.). São Paulo: Pearson Addison Wesley.

Marchesini, J. & Smith, S. (2005). Modeling Public Key Infrastructure in the RealWorld. Public Key Infrastructure, Second European PKI Workshop: Research and Applications, pp. 118-134.

Nakamura, E. T. & Geus, P. L. (2007). Segurança de Redes em Ambientes Cooperativos. São Paulo: Novatec Editora.

OpenSSL Project. (2009). Welcome to the OpenSSL Project. Acesso em 24 de Agosto de 2012, disponível em OpenSSL: http://www.openssl.org/

Proderj. (2012). Serviços para Clientes. Acesso em 27 de Agosto de 2012, disponível em Proderj: http://www.proderj.rj.gov.br/icp.asp

Serasa Experian. (2012). Serasa Experian. Acesso em 27 de Agosto de 2012, disponível em Serasa Experian: http://www.serasaexperian.com.br/

Shirey, R., BBN Technologies, & GTE. (2000). Internet Security Glossary. Acesso em 31 de Julho de 2012, disponível em Request for Comments: 2828: http://www.ietf.org/rfc/rfc2828.txt

Stallings, W. (2008). Criptografia e segurança de redes (4ª Ediçao ed.). São Paulo: Pearson Pretince Hall.

Symantec Corporation. (2012). SSL Certificates Powered by Symantec. Acesso em 1 de Outubro de 2012, disponível em Verisign: http://www.verisign.com/

Tanenbaum, A. S. & Wetherall, D. (2011). Redes de Computadores (5ª ed.). São Paulo: Pearson Prentice.