

Infra-estrutura de Chave Pública (ICP)

Luiz Cezar Quaquio*

RESUMO: O artigo descreve a infra-estrutura de chave pública usando certificados digitais baseados em chave pública e como é a infra-estrutura brasileira de chave pública. Explica, ainda, o que é, como e quando usar certificado digital e a opinião do autor sobre o futuro dessa tecnologia.

PALAVRAS-CHAVE: Chave pública, Chave Privada, Certificado digital.

1 INTRODUÇÃO

Para se realizar eletronicamente transações ou negócios com segurança, assinados digitalmente e podendo gerar, se necessário, recibos digitais, tornando as partes envolvidas responsáveis pelas transações ou comunicações que participam, é necessário estabelecer uma conexão segura entre elas, trocando suas respectivas chaves públicas, que terão sua autenticidade atestada por um *Certificado Digital*. Em outras palavras, o certificado digital garantirá que uma chave pública é verdadeira e que pertence realmente a quem ela diz pertencer.

Existem outras funcionalidades em que o certificado digital também pode ser empregado, como por exemplo:

- ▶ Criar túneis para *Virtual Private Networks* (VPN);
- ▶ Criptografar documentos;
- ▶ Enviar e-mails para pessoas autorizadas;
- ▶ Criar controles automatizados de acesso;

Mas, para autenticar, homologar, auditar e fiscalizar o certificado digital, é necessário uma estrutura que seja uma espécie de “cartório virtual”, começando pela Autoridade Certificadora Raiz (AC Raiz), que é o principal nó de confiança para todos os outros abaixo dele - podem ser outras AC subordinadas, que devem possuir uma cópia da chave pública da AC Raiz, e/ou Autoridades de Registro (AR) para ajudá-las, já que é necessário ir fisicamente a uma AR e provar, com documentação, que você é realmente quem diz ser ou que é o dono de uma empresa, criando assim uma ICP.

A sigla ICP significa *Infra-estrutura de Chaves Públicas*, e pode ser formada por um órgão ou iniciativa pública ou privada que irá definir um conjunto de padrões, técnicos e práticos, e regulamentos com o objetivo de suportar um sistema criptográfico com base em

* Analista de Segurança da Informação, formado em Ciência da Computação, pela UNIP.

certificados digitais, os quais são baseados em chaves públicas e privadas. Ou seja, a ICP é responsável pela geração e gestão de uma chave pública e privada e pela emissão de um certificado digital associada a esse par de chaves.

A figura 1 ilustra como é a estrutura básica de uma ICP, mostrando os diferentes níveis de hierarquia que formam uma cadeia de confiança. Quando uma AC gera um certificado digital, todas as outras ACs confiam nele.

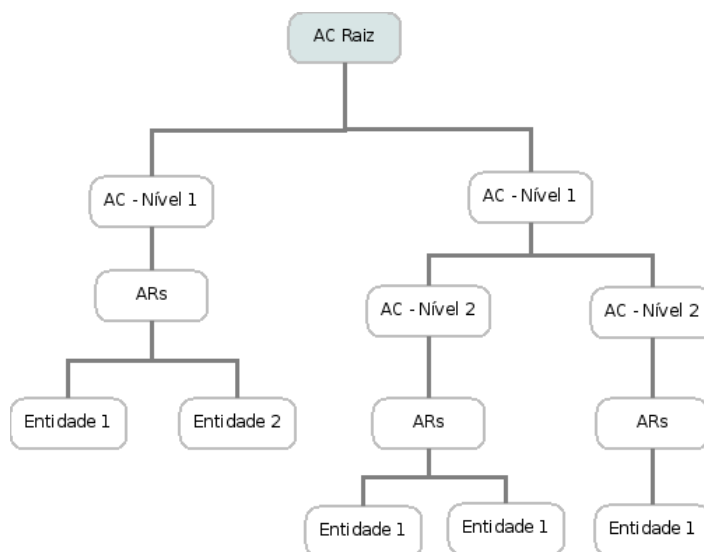


Figura 1 – Infra-estrutura de Chaves Públicas

No Brasil, a infra-estrutura de chaves públicas existente é chamada de ICP-Brasil, e foi definida pela Medida Provisória N°. 2.200-2, de 24 de Agosto de 2001. A partir dessa MP, foram elaborados os regulamentos que regem as atividades das entidades integrantes da ICP-Brasil: as Resoluções do Comitê Gestor da ICP-Brasil, as Instruções Normativas e outros documentos, que podem ser consultados em legislação no decreto 3.872.

O Comitê Gestor da ICP-Brasil (CG-ICP) é nomeado pela Presidência da República, com o objetivo de seguir e garantir as medidas necessárias para seu funcionamento. No decreto 3.872, de 18 de Julho de 2001, o artigo 3º estabelece suas competências, e o artigo 2º, a sua composição.

O suporte técnico e a assistência dada para o CG-ICP é feita pela Comissão Técnica Executiva (COTEC), conforme descrição do artigo 4º, e também pela Secretaria Executiva, cuja função é descrita no artigo 7º.

O Instituto Nacional de Tecnologia da Informação (ITI) é a AC Raiz da ICP-Brasil, responsável por fazer o credenciamento, a fiscalização, a supervisão e a auditoria de toda a

cadeia, para certificar-se que as AC e AR estão seguindo os processos e as políticas de certificação vigentes.

A figura 2, referenciada em <https://www.icpbrasil.gov.br/apresentacao/estrutura>, ilustra como é atualmente a ICP-Brasil e seus níveis hierárquicos de confiança.

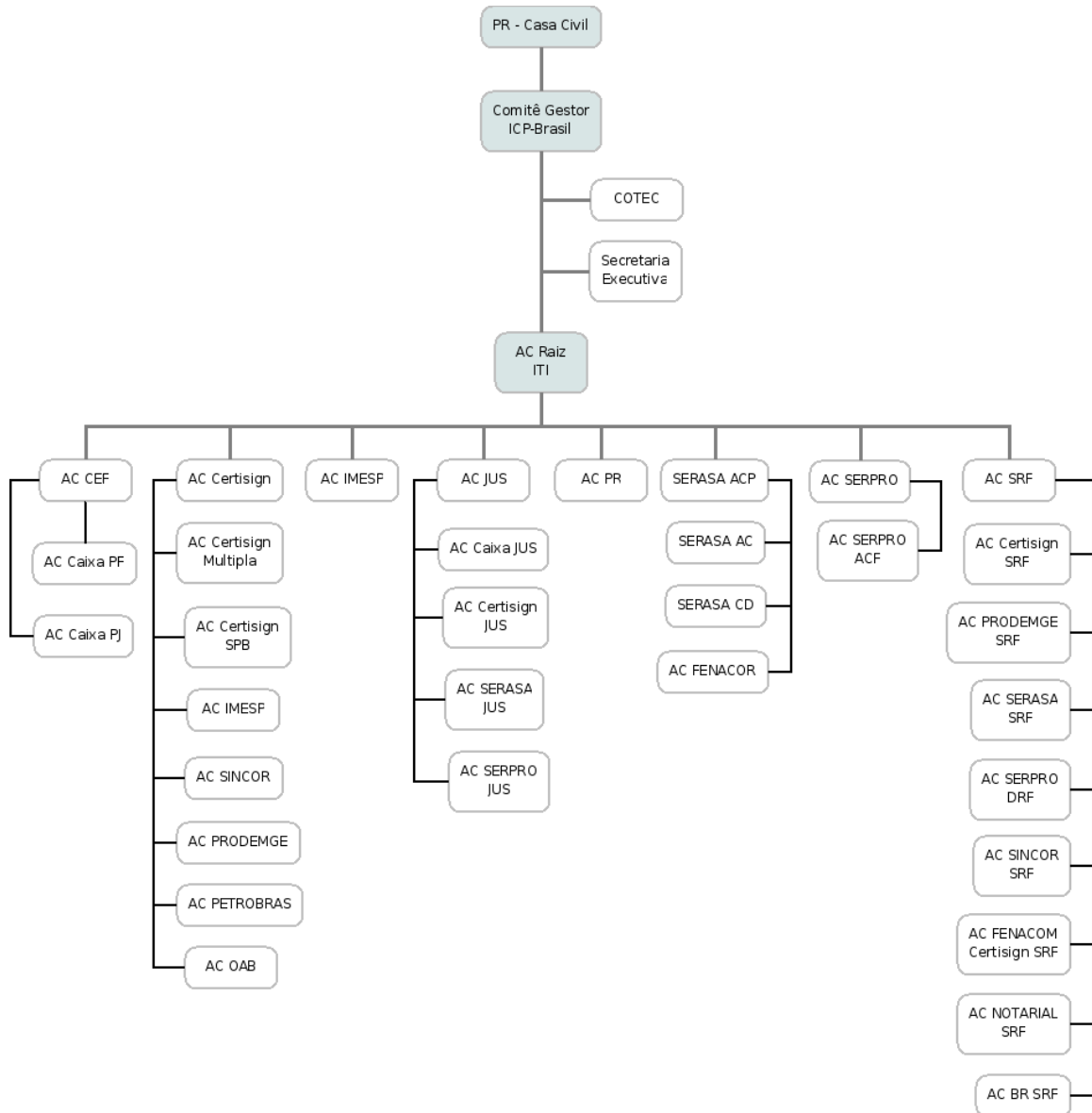


Figura 2 – ICP-Brasil

Qualquer organização pode ser uma AC e fazer parte da ICP-Brasil; para isso, basta se adequar às práticas, processos, regulamentos e políticas exigidos pela infra-estrutura de chave pública brasileira, que estão descritos na resolução nº. 40, de 18 de abril de 2006, feita pelo CG, e requisitar o seu devido registro junto à AC Raiz. Assim que essa nova AC se incorpora à ICP-Brasil, os certificados emitidos por ela valem em todo o território nacional e têm validade jurídica.

A obtenção de um certificado digital pode ser feito por qualquer pessoa jurídica ou física, bastando apresentar fisicamente a documentação necessária a uma AR, que passará esses dados para a AC à qual é subordinada. Esta gerará um certificado no padrão X.509, com o nome, o e-mail, o CPF/CNPJ e a chave pública do seu titular, além do nome e da assinatura da Autoridade Certificadora emissora, período de validade e número de série do certificado digital.

No caso de a chave privada relacionada a um certificado digital ser comprometida, ou no caso de haver mudança nos dados do seu titular, o certificado digital poderá ser revogado. As AC possuem uma lista de todos os certificados digitais revogados ou cancelados, chamada de Lista de Certificados Revogados (LCR). Outra forma de verificar da validade de um certificado digital é fazer uma consulta à AC, por meio do *Online Certificate Status Protocol* (OCSP).

Para os usuários, o certificado digital (CD) funciona da seguinte maneira: os navegadores atuais (como Internet Explorer, Firefox, Ópera, dentre outros) possuem uma lista de AC confiáveis pré-instalados. Quando o usuário acessa um *website* que usa certificação digital, o navegador verifica se a AC emissora do mesmo está na relação das AC confiáveis. Em caso positivo, verifica se o nome obtido na URL está de acordo com o que consta no CD. Se isso for confirmado, será estabelecida, então, uma conexão segura através do protocolo HTTPS, na porta 443. No caso de a AC não constar na lista dos confiáveis, o navegador dará a opção de o usuário confiar permanentemente, temporariamente ou não confiar na mesma.

Existem vários tipos de certificado digital. Vejamos a tabela abaixo retirada de <http://informatica.hsw.uol.com.br/certificado-digital4.htm>:

Tabela 1 – Tipos de certificado digital

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

Para verificar a integridade e a autenticidade das informações contidas em uma assinatura digital de documentos eletrônicos, e-mails, VPNs e identidades na Internet, são

usados os tipos A1, A2, A3 e A4. Os tipos S1, S2, S3 e S4 são para certificados de sigilo, ou seja, são para codificar mensagens, documentos e/ou outras informações eletrônicas que são sigilosas.

Os certificados mais comuns são o A1, que é gerado e armazenado no disco rígido do titular, e o A3, que é gerado e armazenado em um token ou cartão inteligente. Ambos têm o manuseio da chave privada protegida por uma senha, que é bloqueada após n tentativas erradas.

2 CONSIDERAÇÕES FINAIS

As transações e negócios on-line estão cada vez mais presentes em nossas vidas. Com o conseqüente crescimento, redução de custos e versatilidade dessa “identidade virtual” chamada Certificado Digital, esse, com certeza, será o método mais utilizado para garantir a confidencialidade, a integridade e o não-repúdio dos dados trafegados pela Internet.

REFERÊNCIAS BIBLIOGRÁFICAS

CERTISIGN. ICP-Brasil. Disponível em: <<https://www.certisign.com.br/companhia/icp-brasil>>. Acesso em: 12 dez 2008.

HOW STUFF WORKS. Disponível em: <http://informatica.hsw.uol.com.br/certificado-digital.htm>. Acesso em: 17 dez 2008.

ICP-Brasil, Disponível em: <<https://www.icpbrasil.gov.br/apresentacao>>. Acesso em: 12 dez. 2008.

WIKIPEDIA. Certificado Digital: Versão Português. Disponível em: <http://pt.wikipedia.org/wiki/Certificado_digital>. Acesso em: 12 dez 2008.

WIKIPEDIA. ICP: Versão Português. Disponível em: <http://pt.wikipedia.org/wiki/Infra-estrutura_de_Chaves_Publicas> Acesso em: 12 dez 2008.