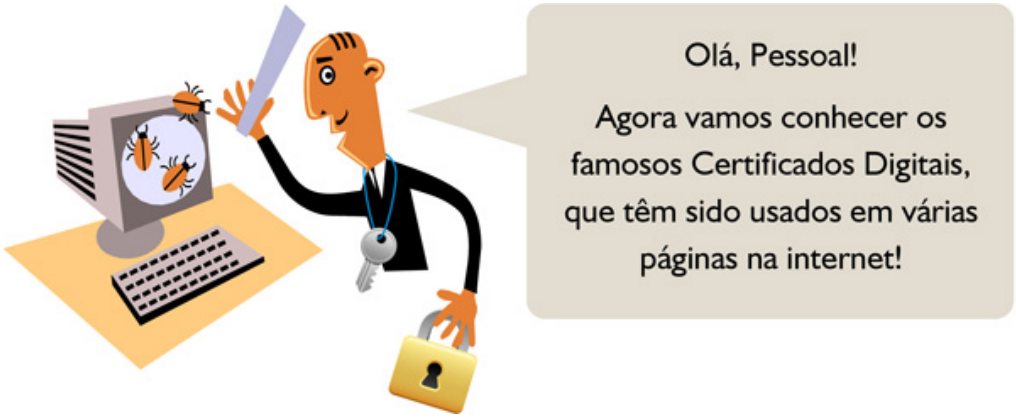
Segurança em Redes

Aula 06 - Certificados Digitais

Apresentação



Nesta aula, você vai estudar mais detalhadamente os certificados digitais, os detalhes de como eles são emitidos, para que servem e como o Brasil tem usado esse mecanismo de segurança.

Vídeo 01 - Apresentação

Objetivos

Ao final desta aula, você será capaz de:

- Saber para que servem os certificados digitais.
- Conhecer o conteúdo de certificados digitais.
- Saber o que são e o que fazem as autoridades certificadoras.
- Distinguir os elementos que fazem parte da ICP-Brasil.

Conceito de Certificado Digital

Um certificado digital é um arquivo que contém informações sobre o seu proprietário (pessoa, empresa, site, programa de computador etc.), tais como nome do proprietário, chave pública do proprietário, validade do certificado, entre outras informações que você verá ainda nesta aula.

Para que servem os certificados digitais?

Servem para comprovar a identidade de uma pessoa, empresa, site, programa de computador etc.

Quem emite os certificados digitais?

Tecnicamente, você mesmo pode emitir seus certificados digitais, contudo, para que ele seja reconhecido publicamente, deve ser emitido por uma autoridade certificadora (CA – *Certificate Authority*).

Certificados digitais são usados com muita frequência em sites, mesmo sem você perceber, neste caso, servem para confirmar a sua autenticidade. Um exemplo do uso de certificados digitais acontece quando você entra no site de um banco. O site identifica-se através de um certificado digital, que pode ser visto clicando em um cadeado na interface do seu navegador. Ao clicar no cadeado, você pode confirmar que aquele site é realmente do banco. Isso também permite que as informações que fluem entre o site do banco e seu computador sejam protegidas.

Os certificados têm sido amplamente usados no comércio eletrônico, em compras virtuais, transações bancárias e em serviços governamentais. O governo decidiu implantar certificação digital para agilizar as transações, reduzir a burocracia e melhorar a satisfação dos usuários.

Um certificado digital associa uma chave pública de uma “entidade” a um ou mais atributos relacionados com sua identidade, assegurando, portanto, que a chave pública pertence à entidade identificada e que ela possui a chave privada correspondente. Assim, um certificado digital garante que a chave pública do seu

titular é confiável. Os certificados digitais possibilitam, dentre outras coisas: o uso da criptografia e assinatura digital; controlar o acesso aos recursos; codificar privilégios de autorização.

Tipicamente, de posse de um certificado digital, seu titular deve enviá-lo aos destinatários de suas mensagens, que, para validá-lo, devem contatar a CA emissora do certificado. Dessa forma, os referidos destinatários podem passar a confiar na chave pública do titular. As mensagens a serem enviadas pelo titular do certificado podem ser assinadas digitalmente com sua chave privada e validadas pelo destinatário com a chave pública do emissor.

Porém, como a chave pública pode ser do conhecimento de terceiros, pode não haver sigilo na comunicação nesse sentido (do titular para o destinatário). Em um programa de e-mail, pode-se habilitar a Assinatura Digital e as mensagens passarão a ser enviadas com a assinatura do emissor da mensagem em anexo. A mensagem, nesse caso, não é criptografada, mas são enviadas informações de controle através das quais o receptor da mensagem consegue verificar a identidade de quem enviou a mensagem, em conjunto com a entidade emissora do certificado digital.

Vídeo 02 - Certificados Digitais

Atividade 01

1. Os certificados digitais podem ser emitidos por qualquer pessoa? Por quê?

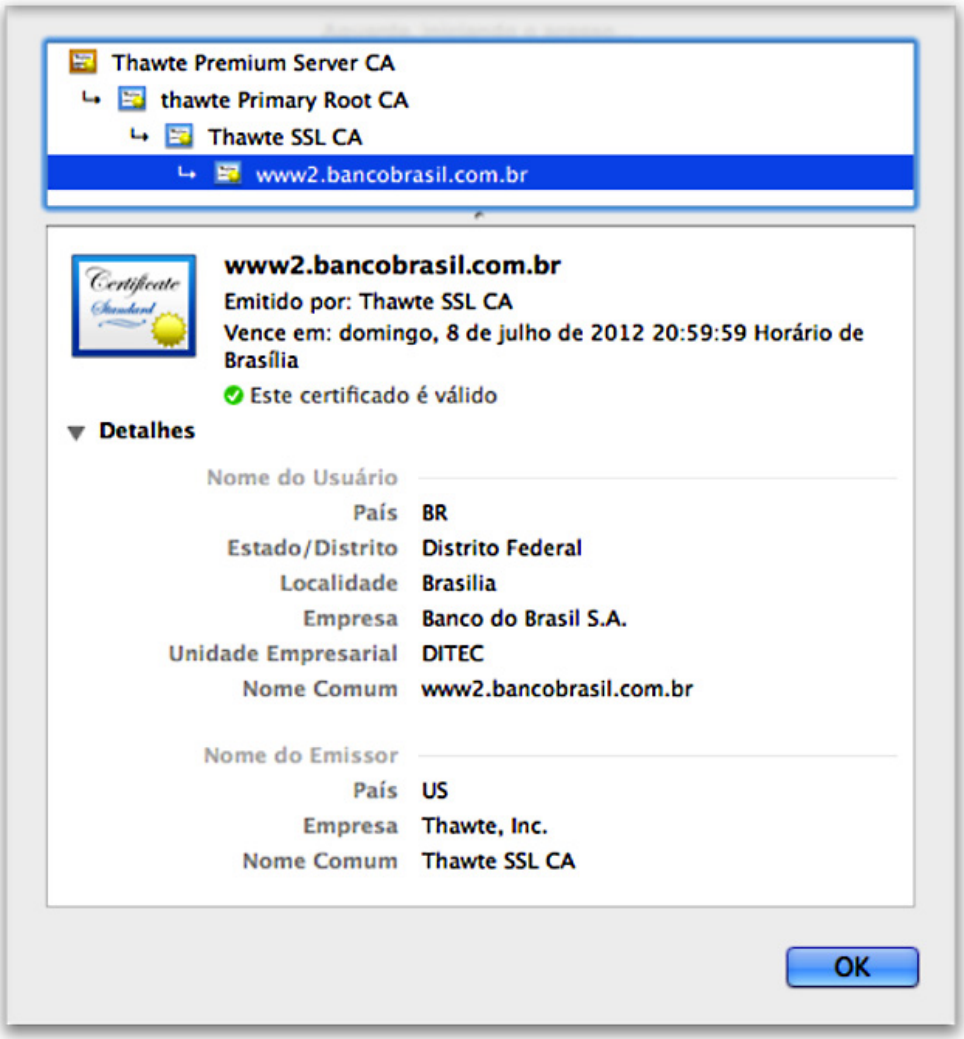
Você deve estar se perguntando: o que contém um certificado digital? Na verdade, ele pode conter várias informações, sendo as essenciais:

- número de série do certificado;
- chave pública do proprietário do certificado;
- validade da chave pública;

- identificação da autoridade certificadora que emitiu o certificado;
- assinatura digital da autoridade certificadora.

Dependendo do certificado, nome, e-mails, URL etc., também podem estar contidos nele. Conforme já dito, um exemplo de certificado digital é bastante comum como os usados em sites de bancos, comércio eletrônico etc. A **Figura 1** mostra informações sobre o certificado digital utilizado pelo site do Banco do Brasil. Nele, podemos ver uma série de informações sobre a o proprietário (www2.bancobrasil.com.br) e autoridade certificadora que emitiu o certificado (Thawte).

Figura 01 - Exemplo de certificado digital utilizado em sites.



Atividade 02

1. Qual a importância de um certificado digital conter várias informações sobre seu proprietário e ser assinado digitalmente pela autoridade certificadora?

Padronização de Formatos de Certificados

Considerando que há propostas de vários formatos para certificados digitais, já houve várias tentativas de padronização, e uma das iniciativas mais significantes é a recomendação X.509 da *International Telecommunication Union-Telecomunication Standardization Sector* (ITU-T) e ISO/*International Electrotechnical Commission* (IEC), publicada pela primeira vez em 1988 como parte do padrão para serviço de diretório X.500. A **Figura 2** ilustra o formato de certificados X.509. Seus campos básicos incluem:

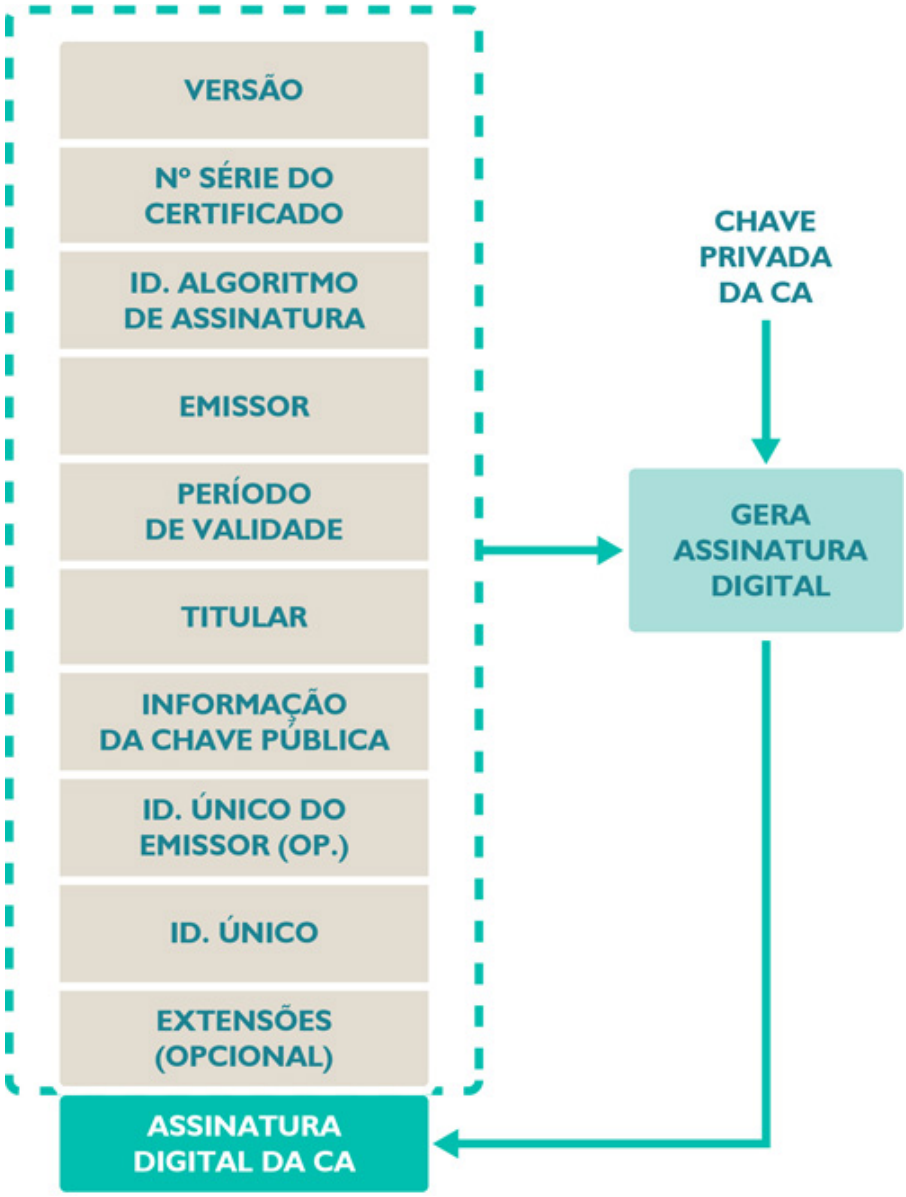
1. **Versão do formato do certificado** indicador do número da versão X.509. Pode assumir os valores 1, 2, ou 3.
2. **Número de série do certificado** um identificador numérico inteiro único para o certificado.
3. **Identificador do algoritmo de assinatura** identificador do algoritmo de assinatura digital usado pela CA para assinar digitalmente o certificado.
4. **Nome do emissor** nome identificador da CA que emitiu o certificado.
5. **Período de validade** datas e, opcionalmente, hora de início e de expiração do certificado.
6. **Nome do titular** especifica o nome da entidade proprietária da chave privada correspondente à chave pública identificada no certificado. Uma mesma entidade pode ser titular com o mesmo nome de mais de um certificado. Porém, uma CA não pode emitir mais de um certificado com o mesmo nome de titular para entidades diferentes.
7. **Informação da chave pública** contém a chave pública pertencente ao titular do certificado, como também o algoritmo usado na sua geração e a

função *hash* com a qual a chave pública deve ser usada.

8. **Identificador único do emissor** campo opcional para permitir o reúso de nomes do emissor.

9. **Identificador único do titular** campo opcional para permitir o reúso de nomes.

Figura 02 - Formato do Certificado Digital X.509 v3.



10. **Extensões** a versão 3 da recomendação X.509 adicionou novos campos ao certificado básico chamados “extensões”. Esses campos são opcionais; portanto, um certificado pode ter zero ou mais campos de extensão. A principal função das extensões é permitir que novos campos sejam adicionados sem modificar o certificado. As extensões permitem associar informações adicionais sobre titulares, chaves públicas, gerenciamento da

hierarquia de certificação e gerenciamento da distribuição da lista de revogação de certificados. Assim, comunidades e organizações podem definir seus próprios campos de extensões para atender às suas necessidades. Por exemplo, um ambiente financeiro pode precisar estender um certificado para codificar dados sobre o cartão de crédito do proprietário, tais como o número do cartão e limite de crédito (FEGHHI; WILLIAMS, 1999). Cada extensão consiste em três campos: Tipo, Valor e Grau de Importância (BATARFI, 2003). Você verá agora esses três campos.

Tipo: contém o identificador do objeto que fornece informação de tipo e semântica para o conteúdo do campo "valor" (por exemplo, string, data etc.).

Valor: contém os dados presentes na extensão, os quais são descritos pela extensão tipo.

Grau de Importância: indica se o valor associado à determinada extensão é crítico ou não. Quando o *flag* indica uma extensão crítica, qualquer aplicação que processar o certificado precisa processar o valor da extensão associada imediatamente; se a aplicação não pode processar uma extensão crítica porque não reconheceu o tipo de extensão, ela deve rejeitar o certificado.

Autoridade Certificadora

Uma autoridade certificadora (CA) é uma entidade que emite, ou seja, envia certificados digitais para seus titulares. A sua CA pode ser a empresa na qual você trabalha ou uma entidade que você paga para emitir o seu certificado digital. A **Figura 3** apresenta um modelo de operação de uma CA (FEGHHI; WILLIAMS, 2010).

As CAs oferecem vários serviços, entre eles:

1. autenticação de chaves públicas;
2. listagem de revogação de certificados;
3. assinatura digital de certificados.

Figura 03 - Modelo de operação de uma CA.

Vídeo 03 - Autoridades Certificadoras

Lista de Revogação de Certificados

Um certificado digital tem um período de validade durante o qual ele é confiável. Após esse período, ele torna-se inválido e não é mais confiável. Durante seu período de validade, a CA que o emitiu mantém e fornece informação sobre o status do

mesmo. O status “revogado” indica que a validade do certificado foi prematuramente encerrada e, portanto, não é mais confiável. Uma autoridade certificadora pode revogar um certificado por razões como:

- Comprometimento da chave privada do titular.
- Comprometimento da chave privada da autoridade certificadora, o que significa que todos os certificados por ela emitidos são não confiáveis e devem ser revogados.
- Mudanças nas informações relativas ao titular do certificado.
- Violação da política de segurança da autoridade certificadora pelo assinante.

A CA deve divulgar uma lista de revogação de certificados (*CRL – Certificate Revocation List*). Essa lista é uma estrutura de dados digitalmente assinada pela CA emissora desses certificados, na qual contém:

- A data e a hora de sua publicação.
- O nome da CA emissora.
- O número de série dos certificados revogados que ainda não expiraram.

Para poder confiar em um certificado, a aplicação deve verificar se o número de série do mesmo não consta na lista de revogação de certificados. Para tal, vários métodos diferentes podem ser empregados. A lista de revogação de certificados pode ser consultada pela aplicação acessando a CA e fazendo o download da lista. Neste caso, a aplicação deverá conhecer a próxima data de atualização da lista para fazer novo download da mesma. Outra forma de divulgação da lista é o seu envio pela CA para as aplicações, tão logo um certificado seja revogado. Isso pode acarretar carga excessiva na rede, além de não se ter certeza de que as informações não vão ser apagadas por um intruso quando estiverem em trânsito. A forma mais prática de verificação da revogação de um determinado certificado é o envio pela aplicação de uma solicitação do status de revogação desse certificado à CA.

Uma solicitação de revogação pode ser originada pelo titular do certificado ou por uma autoridade local de registro. A CA deve validar a origem e autenticidade de uma solicitação de revogação antes de revogar um certificado.

A ITU-T e a ISO/IEC desenvolveram na recomendação X.509, um padrão de formato da lista de revogação de certificados. A **Figura 4** mostra o formato da lista de revogação de certificados estabelecido na versão 2, incluindo os campos básicos predefinidos, e zero ou mais campos de extensões de entrada. Os campos básicos do formato da lista de revogação de certificados estabelecidos na versão 2 são os mesmos da versão 1 e estão listados a seguir (FEGHHI, 1999).

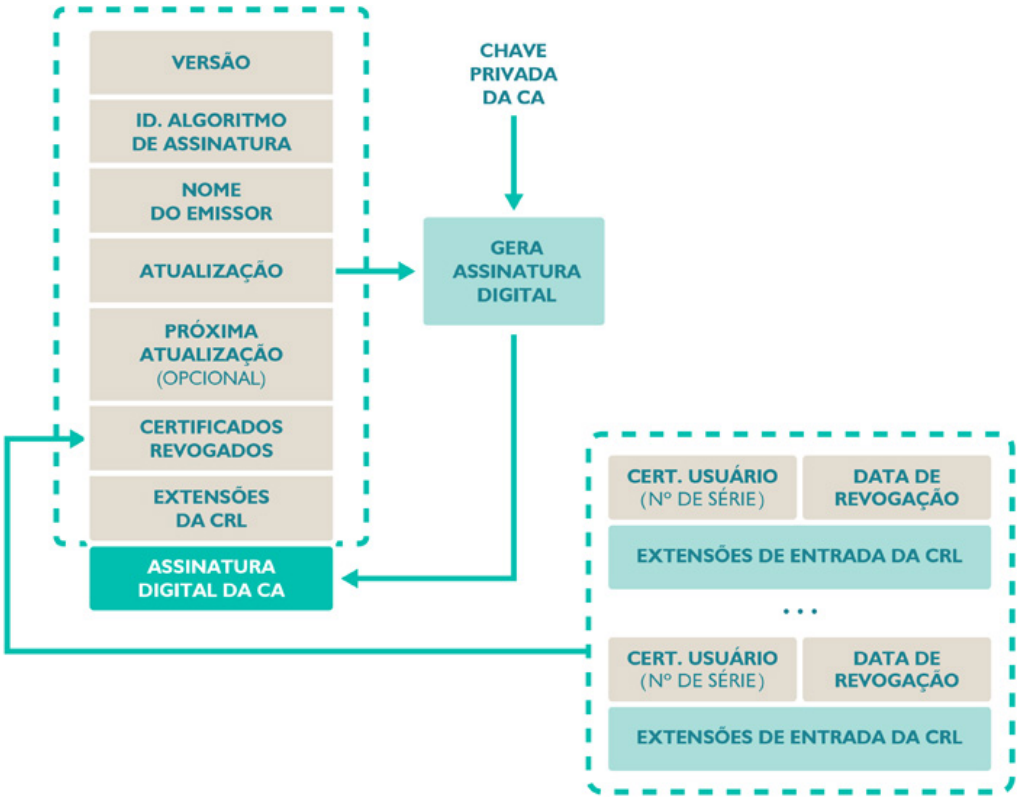
Versão: deve especificar a versão 2 se algum campo de extensão estiver presente, e omitido se não existirem campos de extensão.

Assinatura: contém o identificador do algoritmo usado para assinar a lista de revogação de certificados.

Nome do emissor: nome da entidade que emitiu e assinou a lista de revogação de certificados.

Atualização: indica a data e hora de emissão da lista de revogação de certificados. Pode ser omitido se a próxima atualização for conhecida por todos os sistemas. Uma atualização pode ser emitida antes da data indicada, mas não depois desta data.

Figura 04 - Formato da lista de revogação de certificados X.509, versão 2.



Como mostrado na **Figura 4**, o campo certificados revogados é composto por um conjunto de dados de certificados revogados. Assim, cada certificado revogado é especificado através de três subcampos: certificado do usuário (contendo seu número de série); data de revogação e extensões de entrada da lista de revogação de certificados. Esses três subcampos reúnem as informações necessárias para especificar totalmente os certificados revogados e as suas datas de revogação.

ICP – Brasil

A ICP-Brasil (Infraestrutura de Chaves Públicas – Brasil) foi criada pela MP 2200-2/2001. Com ela, foi estabelecida a validade legal de documentos assinados digitalmente, utilizando-se certificados digitais emitidos dentro da sua cadeia de certificação. Na ICP-Brasil são usados certificados X.509 V3.

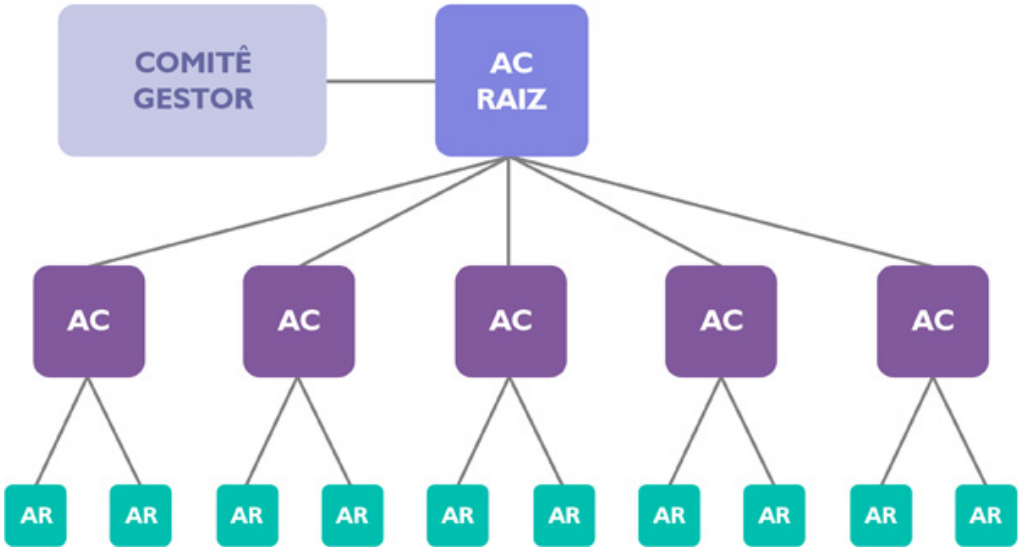
Segundo o portal da justiça federal (2010, extraído da Internet), a "ICP-Brasil fiscaliza e audita o processo de emissão de certificados digitais das autoridades certificadoras integrantes a fim de garantir total confiabilidade do processo de

certificação. Desta forma, dá respaldo à presunção legal de integridade, autenticidade e não repúdio dos arquivos assinados digitalmente.”

A ICP-Brasil é uma estrutura composta por autoridades certificadoras que, através de um conjunto de normas técnicas e procedimentos, dão suporte ao uso de certificados digitais, possibilitando assegurar autenticidade de um usuário ou documento de mídia eletrônica.

A ICP-Brasil segue uma estrutura hierárquica ilustrada na Figura 5. Nela, podemos observar a existência de diversas entidades; cada uma tem uma função definida. A seguir são relacionadas cada uma dessas entidades e suas principais funções na ICP-Brasil.

Figura 05 - Hierarquia ICP-Brasil.



O **comitê gestor** tem a função de atuar na formulação e controle da execução das políticas públicas relacionadas à ICP-Brasil, inclusive nos aspectos de normatização e nos procedimentos administrativos, técnicos, jurídicos e de segurança.

A **autoridade certificadora raiz (AC - raiz)** é a entidade que credencia, realiza auditorias e fiscaliza as autoridades certificadoras, autoridades de registro e demais entidades habilitadas na ICP – Brasil. Compete a ela expedir, emitir, distribuir, revogar e gerenciar os certificados das autoridades certificadoras de nível imediatamente abaixo dela, além de verificar se as mesmas estão atuando em conformidade com as normas técnicas estabelecidas pelo comitê gestor.

A **autoridade certificadora (AC)** é a entidade que emite, renova ou revoga certificados digitais de outras AC ou de titulares finais. Além disso, emite e publica a LCR (**lista de certificados revogados**). Um certificado digital só deve ser emitido por uma AC após a verificação dos dados do usuário a partir de autoridades de registro (AR).

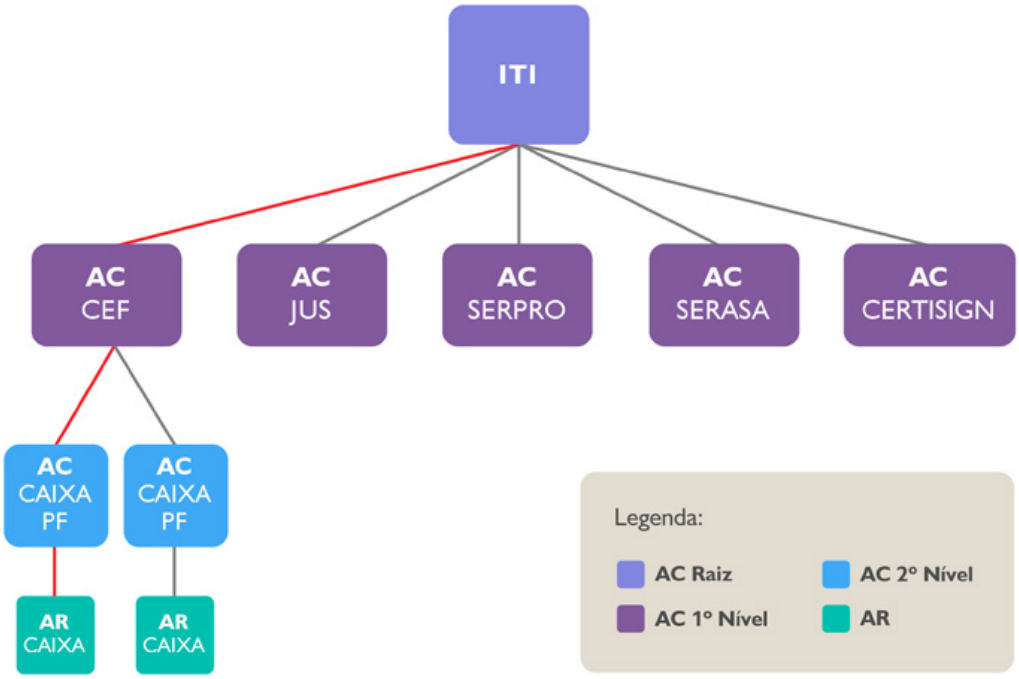
As **autoridades de registro** (AR) são entidades que têm por objetivo o recebimento, validação, encaminhamento de solicitações de emissão ou revogação de certificados digitais ligados às AC. Uma autoridade de registro tem a obrigação de verificar pessoalmente a identidade e os dados do requisitante do certificado digital, a fim de garantir a autenticidade das informações fornecidas.

Mostrando como essa estrutura abstrata é instanciada, no Brasil, o Instituto Nacional de Tecnologia da Informação (ITI) é a autoridade certificadora raiz, que tem como responsabilidade credenciar e supervisionar as demais AC e fazer auditoria dos processos. Abaixo do ITI existem várias AC, denominadas AC de 1º Nível, como:

- AC-CEF (Caixa Econômica Federal);
- AC-JUS (autoridade certificadora da Justiça);
- AC-SERPRO;
- AC-SERASA, dentre outros.

Cada uma das AC de 1º nível tem sua própria finalidade. A AC-CEF emite, por exemplo, certificados referentes ao FGTS e à Previdência Social. A Figura 6 mostra o caminho para emissão de certificados digitais de pessoa física.

Figura 06 - Caminho para emissão de Certificado Digital de Pessoa Física junto à AC-CEF.



Vídeo 04 - ICP – Brasil

Curiosidade!

Como se faz para se obter um certificado digital?

1. O interessado gera uma requisição e anexa a alguns documentos como cópia do RG, CPF ou CNPJ e comprovante de residência (essa requisição pode ser feita na página Web da autoridade certificadora, via uma autoridade de registro). Por exemplo, se o interessado quiser solicitar um certificado digital junto à AC-CEF, ele deve preencher o formulário de solicitação que está disponível no endereço <http://www.certificado.caixa.gov.br/>.

2. O interessado deve se dirigir pessoalmente a AR, levando os documentos solicitados. No nosso exemplo da AC-CEF, ele deve comparecer a uma das agências credenciadas da CAIXA, apresentando os documentos solicitados. O endereço <http://www.certificado.caixa.gov.br/> também fornece a lista das agências credenciadas.

Na AR, os agentes de registro conferem os dados e, se tudo estiver correto, enviam a requisição do certificado para a autoridade

Atividade 03

1. Qual a importância de existirem diversas AC dentro da ICP-Brasil?

Certificados da Receita Federal

O e-CPF e o e-CNPJ são os certificados digitais ligados à Receita Federal. O e-CPF, por exemplo, foi criado com o objetivo de identificar a pessoa física na internet.

Os e-CPFs são cartões inteligentes (*smart cards*) que incluem um tipo de hardware com um microprocessador e memória capaz de armazenar vários tipos de informações e processá-las. A partir dessas informações, é possível gerar uma chave e mantê-la no dispositivo, permitindo, assim, que as operações criptográficas possam ser realizadas dentro do próprio dispositivo. A Figura 7 mostra o e-CPF. Ele é semelhante a um cartão de crédito convencional. Feito de plástico semirrígido, possui o nome e o CPF do titular, e um chip, que contém os dados do titular e a chave privada a ele associada.

Figura 07 - e-CPF

Fonte: http://www.iti.gov.br/twiki/pub/Certificacao/CartilhasCd/brochura01.pdf Acesso em: 26 mar. 2012

Hoje em dia, várias atividades econômicas, sociais e culturais estão sendo feitas via internet. O uso da certificação digital é essencial para garantir segurança e comprovar a identidade dos mais diversos tipos de entidades. Certificados digitais são amplamente utilizados em operações como comércio eletrônico, transações bancárias, serviços governamentais, dentre outras.

Leitura Complementar

Leia mais sobre a ICP-Brasil em: <http://www.iti.gov.br/twiki/bin/view/Certificacao/EstruturaIcp>

Atividade 04

Pesquise

1. Você sabia que no Brasil existe outra infraestrutura de chaves públicas voltada, exclusivamente, para ensino e pesquisa? Pesquise em: <http://www.rnp.br/servicos/icpedu.html>

Resumo

Nesta aula, você estudou os certificados digitais, conheceu suas finalidades e quem os emite. Você aprendeu seu formato e aprendeu, também, que há algumas tentativas de padronização desse formato. Você viu quem são as autoridades certificadoras e que elas podem revogar algum certificado digital, assim como os motivos pelos quais elas podem fazer isso. Conheceu a Infraestrutura de Chaves Públicas do Brasil (ICP-Brasil) e as entidades que têm alguma função dentro dela. E, por fim, conheceu o e-CPF, que possui um certificado digital emitido pela Receita Federal.

Autoavaliação

1. Quais são as principais informações existentes em um certificado digital?
2. Por que o mecanismo de assinatura digital, estudado na aula anterior, é essencial na geração de certificados digitais?
3. Qual a função das AR dentro da ICP-Brasil?

4. Marque V ou F, sendo V para verdadeiro e F para falso.

    a. ( ) Um certificado, mesmo revogado, permanece confiável.

    b. ( ) A AC-Raiz da ICP-Brasil emite certificados digitais para usuários finais.

    c. ( ) O sistema bancário utiliza amplamente certificados digitais.

    d. ( ) Certificados digitais sempre têm um prazo de validade.

    e. ( ) O X.509 é um padrão que não é utilizado pela ICP-Brasil

Referências

BATARFI, O. Certificate Validation in Untrusted Domains. **Lecture Notes in Computer Science (LNCS)**, v. 2889, p. 1057 – 1068, 2003.

BATISTA, C. S. V. **Um Serviço de certificação digital para plataformas de Middleware**. 2004. Dissertação (Mestrado em Sistemas e Computação) – Universidade Federal do Rio Grande do Norte, Natal, 2004.

FEGHHI, J.; FEGHHI, J.; WILLIAMS, P. **Digital certificates**: applied internet security. New York: Addison Wesley, 1999.

INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO – ITI. **Estrutura da ICP-Brasil**. Disponível em: <http://www.iti.gov.br/twiki/bin/view/Certificacao/Estruturalcp>. Acesso em: 3 set. 2010.

ITU-T. **Rec. X.509 ISO/IEC 9595-8**. The Directory: Public-key and Attribute Certificate Frameworks, May 2001.

STALLINGS, W. **Cryptography and network security**: principles and practice. 5th. ed. New York: Prentice Hall, 2010. 744 p.