Certificação Digital
Assinatura Eletrônica

Prof. Paulo Barbosa
duvidas@paulobarbosa.com.br

Observações Importantes

- Esse material pode ser denominado "Notas de Aulas". Ele **não é autodidático**, não o utilize como fonte única de consulta para estudos para pré-concurso.
- Use-o apenas como complemento das minhas aulas. Ele **não é auto-explicativo.**
- **Não se encontra em sua versão final.**
- **Versão – 16/04/2012**
  - **www.paulobarbosa.com.br/informatica/**

Boa Sorte e continuem estudando.
Prof. Paulo Barbosa

O QUE É CERTIFICAÇÃO DIGITAL?

A Certificação Digital é um conjunto de técnicas e processos que propiciam mais segurança às comunicações e transações eletrônicas, permitindo também a guarda segura de documentos.

Utilizando-se da Certificação Digital, é possível, por exemplo, evitar que hackers interceptem ou adulterem as comunicações realizadas via Internet.

Certificado Digital

O certificado digital é um **documento eletrônico** que garante **proteção às transações online e a troca virtual de documentos, mensagens e dados**, com validade jurídica.

Com este dispositivo, os sistemas de informação podem validar e reforçar os mecanismos de **segurança online**, utilizando a tecnologia para garantir a privacidade e confirmar a autenticidade das informações dos usuários, empresas e instituições na rede.

Com a certificação digital é possível, por exemplo, realizar transações bancárias com mais segurança. A instituição bancária possui certificado para autenticar-se junto ao cliente, assegurando que todas as transações estão sendo enviadas para o servidor do banco. Já o cliente, realizando operações via banco online, também tem uma chave de acesso que comprova sua identidade perante o banco.

Também é possível saber, com certeza, quem foi o autor de uma transação ou de uma mensagem, ou, ainda, manter dados confidenciais protegidos contra a leitura por pessoas não autorizadas. Embora seja baseada em conceitos matemáticos altamente sofisticados, ela pode ser utilizada facilmente. A maioria dos sistemas de correio eletrônico e navegadores estão preparados para orientar os usuários, de forma didática, a realizar as principais operações com Certificação Digital.

A Certificação Digital baseia-se na existência de Certificados Digitais, que são "documentos de identificação" eletrônicos. Eles são emitidos por uma Autoridade Certificadora, que é uma entidade considerada confiável pelas partes envolvidas numa comunicação e/ou negociação.

Esses certificados podem ser emitidos para pessoas físicas ou jurídicas, equipamentos ou aplicações, chamados de "titulares de certificados".

PROPRIEDADES DA ASSINATURA DIGITAL

- **autenticidade** – o receptor deve poder confirmar que a assinatura foi feita pelo emissor;
- **integridade** – qualquer alteração da mensagem faz com que a assinatura não corresponda mais ao documento;
- **não repúdio ou irretratabilidade** – o emissor não pode negar a autenticidade da mensagem.

POR QUE USAR CERTIFICAÇÃO DIGITAL

A busca por eficácia e eficiência na administração pública passa, cada vez mais, pela automação de processos com o uso intensivo de computadores e de redes de dados. A rapidez e a flexibilidade que as redes imprimiram às comunicações estão revolucionando a forma como as empresas e governos trabalham e realizam negócios.

Os Municípios arrecadam diariamente impostos e taxas, ou seja, uma grande quantidade de documentos que devem ser processados e armazenados de forma segura e inviolável.

A Certificação Digital permite que essas informações transitem pela Internet, agilizando o processo não só de arrecadação, mas também de contabilização e guarda dos documentos.

Esse é apenas um exemplo de como a Certificação Digital pode facilitar a vida das prefeituras e dos cidadãos dos Municípios. Veja outras informações sobre essa técnica e as suas possibilidades de uso.

Segmentos da economia que utilizam a certificação em suas atividades:

Receita Federal do Brasil ;
Área financeira e contábil;
Poder Judiciário;
Saúde;
Educação.

Benefícios da certificação digital:

- ✓Economia de tempo e redução de custos;
- ✓Desburocratização de processos;
- ✓Validade jurídica nos documentos eletrônicos;
- ✓Possibilidade de eliminação de papéis;
- ✓Autenticação na Internet com segurança.

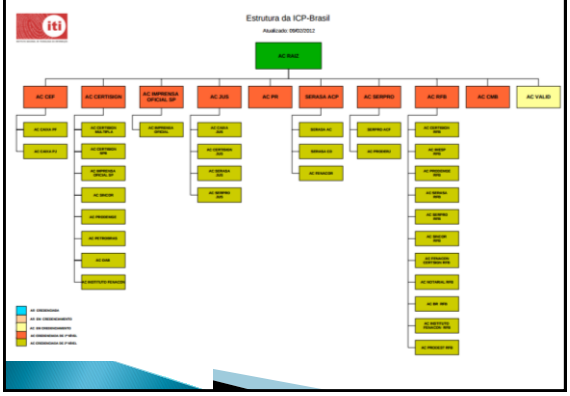
CERTIFICADOS DA ICP-BRASIL

Muitas Autoridades Certificadoras diferentes podem oferecer certificados digitais. Nem todas, porém, estão credenciadas na Infra-Estrutura de Chaves Públicas Brasileira, a ICP-Brasil.

A ICP-Brasil, criada a partir da Medida Provisória 2.200-2, de 24.10.2001, é um conjunto de entidades prestadoras de serviços ordenadas em conformidade com as diretrizes e normas técnicas estabelecidas por um Comitê Gestor. Somente as transações realizadas com processo de certificação envolvendo certificados emitidos por autoridades credenciadas na ICP-Brasil presumem-se verdadeiras em relação aos signatários, dando validade jurídica aos documentos assinados digitalmente. Uma das principais características da ICP-Brasil é sua estrutura hierárquica. No topo da estrutura, encontra-se a Autoridade Certificadora Raiz e, abaixo dela, estão as diversas entidades.

O contrato de adesão é subordinado a um processo de credenciamento, no qual são analisadas a capacidade jurídica, econômico-financeira, fiscal e técnica de cada entidade.

Também é exigida a contratação de seguro de responsabilidade civil e a realização de auditorias prévias e anuais. Tudo isso tem o objetivo de garantir a segurança do processo, desde a identificação dos titulares até a emissão dos certificados, trazendo, assim, confiabilidade a toda estrutura e aos atos praticados em seu âmbito.



Garantia de sigilo e privacidade

Quando você visita um site "seguro" da web, o seu computador recebe o certificado contendo a chave pública desse site, o que é suficiente para criar um túnel criptográfico, tornando os dados incompreensíveis durante o tráfego, sendo possível apenas ao servidor web recuperar a informação original.

Controle de acesso a aplicativos

O servidor web pode solicitar ao usuário que apresente um certificado digital, em vez de digitar usuário e senha. Os usuários não poderão colocar em perigo a aplicação pela falta de cuidado no uso e armazenamento da senha.

Assinatura de formulários e impossibilidade de repúdio

Os usuários poderão assinar os formulários que submetem preenchidos pela web da mesma maneira que fariam pessoalmente em um balcão de atendimento.

Garantia de sigilo e privacidade

O sistema de correio eletrônico utilizado para troca de mensagens através da Internet não possui recursos nativos para impedir a violação da correspondência eletrônica. Com o uso de certificados digitais, você pode selar a sua correspondência em um envelope digital criptográfico' e certificar-se de que apenas o destinatário será capaz de compreender seu conteúdo.

Identificação do remetente

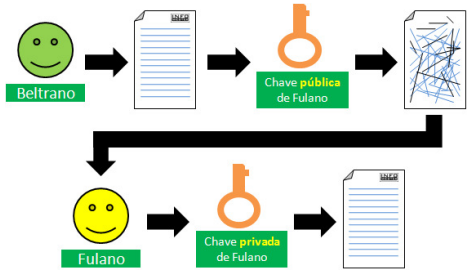
Não existirá mais dúvidas sobre a origem de uma mensagem, pois será possível certificar-se da identidade do emissor.

Assinatura de mensagens e impossibilidade de repúdio

As mensagens de correio eletrônico, ou qualquer documento digital, passam a valer como documento assinado, com validade jurídica, dispensando-se o uso de papel.

Versão eletrônica do CPF e do CNPJ. Permite realizar operações de pessoas físicas e jurídicas que necessitem de certificado digital, com a Receita Federal e Conectividade Social. É armazenado em dispositivo portátil e tem validade de 1 a 3 anos.

Assinatura digital



Passo 1: Alice envia sua chave pública para Bob

sso 2: Bob cifra a mensagem com a ave pública de Alice e envia para ce, que recebe e decifra o texto lizando sua chave privada

CAIXA

- A partir deste ponto.
- Segue uma "apostila" da própria CEF sobre Certificado Digital

O que é certificado digital?

funciona como uma espécie de carteira de identidade virtual que permite a identificação segura do autor de uma mensagem ou transação em rede de computadores. Um documento eletrônico que possui Certificação Digital tem garantia de autenticidade de origem e autoria, de integridade de conteúdo, de confidencialidade e de irretratabilidade, ou seja, de que a transação, depois de efetuada, não pode ser negada por nenhuma das partes. A certificação digital é um tipo de tecnologia de identificação que permite que transações eletrônicas dos mais diversos tipos sejam feitas de forma a evitar que adulterações, interceptações ou outros tipos de fraude ocorram. Um certificado digital contém os dados de seu titular como nome, data de nascimento, chave pública, nome e assinatura da Autoridade Certificadora que o emitiu, podendo ainda conter dados complementares como CPF, título de eleitor, RG, etc.

Qual a diferença entre os certificados A1 e A3 da Caixa?

- Tipo A1: Pode ser armazenado nas mídias Disquete, token, cartão ou pen drive e possui a validade de 1 ano.
- Tipo A3: Pode ser armazenado em Cartão Inteligente (Smartcard) ou token e possui validade de 03 anos.

Por que eu preciso de um certificado digital?

Nas operações bancárias, em compras via Internet e em outros serviços virtuais, a segurança continua sendo grande preocupação. O controle de acesso através de uma simples senha não é mais adequado. Controlar o acesso por meio de algo que só você conhece e possui, como o certificado digital, é muito mais seguro. Mais e mais companhias que fazem negócios na Internet estão acordando para esta realidade e requerendo o uso de certificados digitais para seus clientes. Todavia, não são apenas os clientes no mundo eletrônico que irão precisar de certificados digitais. As máquinas que viabilizam o comércio eletrônico na Internet precisam de certificados digitais também. A presença de um certificado digital atesta a integridade do negócio, fornecendo aos consumidores virtuais a garantia que estão tratando com um negócio legítimo.

Como solicitar o certificado?

Faça a sua Solicitação por meio do preenchimento do Formulário de Solicitação no site da caixa e compareça à uma das agências habilitadas da CAIXA, apresentando os documentos (originais e cópias) necessários para a emissão do certificado. Obs: Não é permitida a representação do titular por meio de procuração.

Esse é o procedimento da CEF, mas pode-se solicitar em quaquer A.C. credenciada pela ICP-Brasil.

É obrigatória a presença do cliente para emissão do certificado?

Sim. O certificado só é emitido com a presença física do titular quando for pessoa física e do(s) representante(s) legal (is) constante (s) no ato constitutivo da empresa e do responsável pelo o uso do certificado quando for pessoa jurídica.

Qual a documentação necessária para obter um certificado digital?

- Comprovante de residência emitido há no máximo 90 dias, em que constem o nome do titular, data de emissão e CEP (contas de água, luz, telefone, extratos bancários ou contrato de aluguel).

O que é a senha PIN?

- É a senha utilizada diariamente pelo usuário, a qual dá acesso ao certificado digital armazenado no cartão. Esta senha deve conter de 6 a 15 caracteres alfanuméricos (letras e números) e deve existir pelo menos uma letra maiúscula, uma minúscula e um número

O que é a senha PUK?

- O PUK (Personal Unblock Key) é um código utilizado para desbloquear seu PIN em caso de perda ou bloqueio. O PUK de seu cartão é composto por números e/ou letras, com 6 a 15 caracteres e pode ser alterado a qualquer momento por meio do software Gestão da mídia.

Esqueci as senhas PIN e PUK. O que fazer?

- No caso de esquecimento das senhas PIN e PUK, o certificado deve ser revogado. Não há possibilidade de recuperação das senhas PIN e PUK.

Quais os tipos de mídias utilizadas para armazenar o certificado?

- Token e smartcard – armazenam os certificados tipo A1 e A3
- Disquete e pen drive – armazenam os certificados tipo A1

Quantas vezes são possíveis renovar o certificado?

- Os certificados de pessoa física e pessoa jurídica podem ser renovados uma única vez. O certificado de aplicação ou equipamento servidor não pode ser renovado.

Fontes

- www.caixa.com.br
- www.iti.gov.br
- pt.wikipedia.org
- www.serasa.com.br
- www.correios.com.br