

CERTIFICAÇÃO DIGITAL

A internet facilitando nossa vida

As exigências e as pressões crescentes da vida moderna, o caos urbano, os congestionamentos e as filas levam à busca por mais praticidade pelas pessoas. Milhares de pessoas fazem suas compras sem sair de casa, aproveitando as promoções de lojas, que oferecem descontos especiais para quem compra pela internet.

Hoje em dia já é possível obter uma série de documentos, como certidões da Receita Federal, sem enfrentar nenhuma fila.

E esses novos serviços disponibilizados garantem a segurança das transações feitas por meio da internet, utilizando o mecanismo da certificação digital, que permite que as informações transitem de forma rápida, garantindo a integridade, a autenticidade, o sigilo e a irretratabilidade das transações.

A identidade digital

No mundo eletrônico, uma das grandes preocupações é a autenticidade, ou seja, saber com quem estamos nos relacionando. Uma das formas mais seguras é por meio do certificado digital.

O certificado digital pode ser traduzido como uma identidade digital – assim como o seu RG - e uma assinatura gerada com a utilização do certificado digital – padrão ICP-Brasil - pode ser comparada a sua assinatura de próprio punho, mas de forma eletrônica, com validade jurídica.

O que é um certificado digital

Certificado digital é um arquivo eletrônico que identifica as pessoas. Como qualquer documento, ele contém informações importantes sobre o seu portador, como por exemplo, nome, data de nascimento e CPF. É uma identidade eletrônica baseada na tecnologia de criptografia de chave pública (cálculos matemáticos complexos), sendo uma das formas mais eficientes de reconhecimento de uma pessoa ou entidade na internet. Um certificado digital é emitido por uma autoridade certificadora.

A certificação digital baseia-se em uma criptografia assimétrica, que é uma forma de produzir um código secreto através do uso de um par de chaves diferentes

entre si, que se relacionam matematicamente por meio de um algoritmo, de forma que o texto codificado por uma chave, apenas seja decifrado pela outra, do mesmo par.

As duas chaves envolvidas na criptografia assimétrica são denominadas chave pública e chave privada.

A chave pública, junto com dados de identificação, é gravada no certificado digital que pode ser repassado pelo seu titular a qualquer pessoa ou entidade com quem ele se relacione no mundo eletrônico. O certificado digital garante que aquela chave pública pertence ao titular do certificado.

Para cada chave pública, existe uma única chave privada que pode fechar esta combinação, que é feita utilizando cálculos matemáticos poderosos e que inviabiliza a sua descoberta. Portanto, a chave privada é de uso exclusivo do titular.

Além de ser um mecanismo de identificação seguro, a pessoa pode assinar arquivos ou documentos eletrônicos com a utilização de seu certificado digital, gerando uma assinatura eletrônica que possui os mesmos efeitos legais que aquela que é feita em um documento em papel.

Uso da certificação digital

A popularização do certificado digital - a identidade digital - permitirá a disponibilização de muitos serviços, que atualmente necessitam da presença física do cidadão, por meio da internet, evitando que as pessoas se desloquem de um ponto para outro transportando grandes volumes de papéis e enfrentem filas para resolver problemas com órgãos públicos, realizar negócios junto aos bancos etc.

Encontram-se disponibilizadas atualmente inúmeras aplicações que utilizam a tecnologia de certificação digital por instituições públicas nas diversas esferas de governo. Como exemplo, podemos citar, dentre os serviços disponibilizados pela Receita Federal do Brasil, a obtenção de cópia de sua declaração de IR dos últimos cinco anos, além do extrato com informações sobre o processamento da declaração.

Uma amostra do que está por vir é, por exemplo, a cópia autenticada da certidão de casamento? Fácil! Acesse o site do cartório e imprima. No futuro, quem sabe, poderemos dizer adeus às filas.

Como obter um certificado digital

O processo de emissão de um certificado digital é bem próximo ao de uma carteira de identidade: existe uma estrutura do governo federal responsável, chamada

ICP-Brasil, que autoriza empresas a emitirem certificados digitais seguros para as pessoas. Essas empresas são chamadas autoridades certificadoras.

Para entregar o certificado a uma pessoa e garantir que ela é realmente o seu titular, existe uma entidade chamada autoridade de registro, empresas autorizadas pelas autoridades certificadoras a realizar tal procedimento.

A pessoa ou empresa que desejar utilizar um certificado deve procurar uma autoridade certificadora ou autoridade de registro para a emissão do mesmo. Isto pode ser feito por meio da internet, acessando seus sites.

Todos os documentos autenticados com essa identidade digital têm validade jurídica, pois a Medida Provisória 2.200-2, de 24 de agosto de 2001, reconhece que todos os documentos emitidos ou assinados, em forma eletrônica, pela estrutura de certificação da ICP-Brasil, possuem a mesma validade e veracidade que os documentos assinados em papel, com firma reconhecida.

Para obter todas as vantagens que um certificado digital pode proporcionar, a pessoa ou empresa precisa apenas de um único certificado emitido na cadeia a ICP-Brasil. Esse único certificado poderá ser utilizado nas diversas aplicações disponibilizadas pelas diversas empresas/órgãos.

O certificado é armazenado no cartão inteligente (*smartcard*) protegido por uma senha de acesso, também conhecida como PIN, atribuída pelo próprio titular do certificado. Assim, em caso de perda não há perigo de outra pessoa usá-lo.

Esta senha é diferente das outras, tais como as que os clientes têm com os bancos, por exemplo, porque ela só existe no cartão do certificado e a pessoa usa a mesma senha em todas as vezes em que o uso do certificado digital é permitido. Assim, fica mais fácil, pois só é preciso decorar uma senha.

O Comitê Gestor da ICP-Brasil é quem regulamenta o funcionamento das autoridades certificadoras e das autoridades de registro. O Instituto Nacional de Tecnologia da Informação (ITI) é o responsável por fazer cumprir a regulamentação.

Você pode encontrar todas as informações que precisa e uma lista das Autoridades certificadoras e de registro no site do ITI www.iti.gov.br.

Tipos de Certificado Digital

Existem diversos tipos de certificados digitais disponíveis para utilização no âmbito da ICP-Brasil. Um tipo de certificado digital que pode ser usado tanto para acessar sites de bancos, permitir o uso do site da Receita Federal e assinar contratos é o e-CPF.

O e-CPF pode ser armazenado em um cartão parecido com o seu cartão de banco. Esse cartão tem um chip, onde fica guardado de forma segura o e-CPF do titular.

Dicas de Segurança

O certificado digital é pessoal e intransferível e o titular deve adotar os procedimentos de segurança, visando impedir o acesso de terceiros.

A senha pessoal (PIN) é de uso e conhecimento exclusivo do titular, que deve observar alguns pontos importantes:

- Manter o sigilo da senha pessoal, não a revelando a terceiros
- Trocar periodicamente a senha pessoal
- Memorizar a senha pessoal e não escrever em nenhum lugar

Glossário

Assinatura digital: assinatura eletrônica que permite aferir, com segurança, a autenticidade e a integridade de um documento eletrônico mediante a utilização do certificado digital, através da combinação matemática de algoritmos criptográficos.

Autoridade Certificadora: entidade autorizada pela ICP-Brasil a emitir certificados digitais de acordo com as práticas definidas na Declaração de Práticas de Certificação (DPC). É comumente conhecida por sua abreviatura AC.

Autoridade de Registro: é responsável pela identificação presencial da pessoa. Cadastra e encaminha as solicitações de certificados às autoridades certificadoras e é comumente conhecida por sua abreviatura AR.

Criptografia de Chaves Públicas: tipo de criptografia que usa um par de chaves criptográficas matematicamente relacionadas. As chaves públicas podem ficar disponíveis para qualquer um que queira cifrar informações para o dono da chave privada ou para verificação de uma assinatura digital criada com a chave privada correspondente. A chave privada é mantida em segredo pelo seu dono e pode decifrar informações ou gerar assinaturas digitais.

DPC – Declaração de Práticas de Certificação: documento que contém as práticas e atividades que uma AC implementa para emitir certificados. É a declaração da entidade certificadora a respeito dos detalhes do seu sistema de credenciamento e as

práticas e políticas que fundamentam a emissão de certificados e outros serviços relacionados.

ICP-Brasil - Infra-Estrutura de Chaves Públicas Brasileira: arquitetura, organização, técnicas, práticas e procedimentos que suportam, em conjunto, a implementação e a operação de um sistema de certificação baseado em criptografia de chaves públicas. Determina as políticas da certificação digital no Brasil.

Fontes de Informação:

Febraban – Federação Brasileira de Bancos (www.febraban.org.br)

ICP Brasil – Infra-Estrutura de Chaves Públicas Brasileira (www.icpbrasil.gov.br)

ITI - Instituto Nacional de Tecnologia da Informação (www.iti.gov.br)

RFB - Secretaria da Receita Federal do Brasil (www.receita.fazenda.gov.br)