

O que é certificado digital?

O certificado digital é um documento eletrônico assinado digitalmente por uma autoridade certificadora, e que contém diversos dados sobre o emissor e o seu titular. A função precípua do certificado digital é a de vincular uma pessoa ou uma entidade a uma chave pública.

Para adquirir um certificado digital, o interessado deve dirigir-se a uma Autoridade de Registro, onde será identificado mediante a apresentação de documentos pessoais (dentre outros: cédula de identidade ou passaporte, se estrangeiro; CPF; título de eleitor; comprovante de residência e PIS/PASEP, se for o caso). É importante salientar que é indispensável a presença física do futuro titular do certificado, uma vez que este documento eletrônico será a sua "carteira de identidade" no mundo virtual.

A emissão de certificado para pessoa jurídica requer a apresentação dos seguintes documentos: registro comercial, no caso de empresa individual; ato constitutivo, estatuto ou contrato social; CNPJ e documentos pessoais da pessoa física responsável.

As principais informações que constam em um certificado digital são: chave pública do titular; nome e endereço de e-mail; período de validade do certificado; nome da AC que emitiu o certificado; número de série do certificado digital; assinatura digital da AC.

O que é assinatura digital?

A assinatura digital é uma modalidade de assinatura eletrônica, resultado de uma operação matemática que utiliza algoritmos de criptografia assimétrica e permite aferir, com segurança, a origem e a integridade do documento.

A assinatura digital fica de tal modo vinculada ao documento eletrônico "subscrito" que, ante a menor alteração neste, a assinatura se torna inválida. A técnica permite não só verificar a autoria do documento, como estabelece também uma "imutabilidade lógica" de seu conteúdo, pois qualquer alteração do documento, como por exemplo a inserção de mais um espaço entre duas palavras, invalida a assinatura.

Necessário distinguir assinatura digital da assinatura digitalizada. A assinatura digitalizada é a reprodução da assinatura autógrafa como imagem por um equipamento tipo scanner. Ela não garante a autoria e integridade do documento eletrônico, porquanto não existe uma associação inequívoca entre o subscritor e o texto digitalizado, uma vez que ela pode ser facilmente copiada e inserida em outro documento.

Os atributos da assinatura digital são:

- a) ser única para cada documento, mesmo que seja o mesmo signatário;
- b) comprovar a autoria do documento eletrônico;
- c) possibilitar a verificação da integridade do documento, ou seja, sempre que houver qualquer alteração, o destinatário terá como percebê-la;
- d) assegurar ao destinatário o "não repúdio" do documento eletrônico, uma vez que, a princípio, o emitente é a única pessoa que tem acesso à chave privada que gerou a assinatura.

A assinatura digital garante ao destinatário que o documento não foi alterado ao ser enviado (integridade) e ainda comprova a autoria do emitente (autenticidade), enfim, confere maior grau de segurança, pois os documentos eletrônicos não assinados digitalmente têm as características de alterabilidade e fácil falsificação.

Como uso Identificações Digitais?

Quando você recebe mensagens assinadas digitalmente, pode verificar a Identificação Digital do signatário para determinar se não ocorreu nenhuma falsificação ou adulteração. Você também pode usar uma Identificação Digital para se identificar perante servidores seguros, como servidores da Web baseados em associação. Geralmente, depois de obter uma Identificação Digital, você pode configurar seu aplicativo de correio eletrônico ou navegação na Web com funções de segurança para usar a Identificação Digital automaticamente.

Qual o Ciclo de Vida de um Certificado?

Todo Certificado será objeto de uma Solicitação, uma Validação após comprovação do pagamento da sua respectiva taxa, uma Emissão, o Uso durante o seu Período de Validade e uma Renovação ou uma Revogação.

Quando e como Renovar um Certificado Digital?

Os Titulares de Certificado serão comunicados da necessidade da renovação. As solicitações de renovação de certificados, que implica na Geração de novo par de chaves antes da expiração do atual.

O responsável pelo Certificado, notificará a Autoridade Certificadora enviando a Solicitação de Revogação para que esta promova a revogação do Certificado Digital emitido, sempre que ocorrer um dos seguintes eventos:

- a) Houver mudança em qualquer informação contida no Certificado Digital;
- b) Em caso de suspeita ou evidência de comprometimento de chaves privadas ou senhas assim como da mídia de armazenamento;

- c) A pedido formal do Titular do Certificado Digital, quando não houver mais interesse na utilização do Certificado Digital;

Quem emite um Certificado Digital?

Um Certificado Digital ou Identificação Digital, é emitida por uma Autoridade de Certificação (AC) e é assinada com a Chave Privada desta AC. Uma Identificação Digital normalmente contém:

- A Chave Pública do proprietário
- O nome do proprietário
- A data de vencimento da Chave Pública
- Nome do emissor (a AC que emitiu a Identificação Digital)
- O número de série da Identificação Digital
- A assinatura digital do emissor

Onde adquirir certificados digitais ICP-Brasil?

O Instituto Nacional de Tecnologia da Informação (ITI), autarquia federal vinculada à Casa Civil da Presidência da República, é a Autoridade Certificadora Raiz da Infra-estrutura de Chaves Públicas Brasileiras (ICP-Brasil) e é o órgão que credencia empresas a fornecer certificados padrão ICP-Brasil. Consulte o site do ITI (www.iti.gov.br) para informações de cadeias certificadoras.