Entendendo a Certificação Digital

Introdução

Há tempos que as pessoas utilizam assinaturas à caneta, carimbos, selos, entre outros recursos, para comprovar a autenticidade de documentos, expressar concordância com determinados procedimentos, declarar responsabilidades, etc. Hoje, muitas dessas atividades podem ser feitas através da internet. Mas, como garantir autenticidade, expressar concordância ou declarar responsabilidade no "mundo eletrônico"? É aí que entra em cena a **certificação digital** e conceitos relacionados, como assinatura digital. Nas próximas linhas você verá uma explicação com os principais pontos que envolvem esses recursos.

O que é certificação digital?

A internet permite que indivíduos, empresas, governos e outras entidades realizem uma série de procedimentos e transações de maneira rápida e precisa. Graças a isso, é possível fechar negócios, emitir ou receber documentos, acessar ou disponibilizar informações sigilosas, economizar dinheiro evitando processos burocráticos, entre outros. No entanto, da mesma forma que os computadores oferecem meios para tudo isso, podem também ser usados por fraudadores, o que significa que tais operações, quando realizadas por vias eletrônicas, precisam ser confiáveis e seguras. A certificação digital é capaz de atender à essa necessidade.

A certificação digital é um tipo de tecnologia de identificação que permite que transações eletrônicas dos mais diversos tipos sejam feitas considerando sua integridade, sua autenticidade e sua confidencialidade, de forma a evitar que adulterações, interceptações ou outros tipos de fraude ocorram.

Como funciona a certificação digital?

A certificação digital funciona com base em um documento eletrônico chamado **certificado digital** e em um recurso denominado **assinatura digital**. É conveniente compreender primeiro este último, para melhor compreensão.

O que é Assinatura digital?

Imagine-se na seguinte situação: você está em uma viagem de negócios e precisa enviar documentos sigilosos à matriz de sua empresa. Dada a distância, o jeito mais rápido de fazer isso é utilizando a internet.

No entanto, se você optasse por enviar esses documentos em papel, certamente os assinaria à caneta para comprovar a autenticidade e a sua responsabilidade sobre eles. Além disso, provavelmente utilizaria um serviço de entrega de sua confiança e o instruiria a deixar os documentos apenas com a pessoa ou o setor de destino.

Mas, como colocar em prática essas medidas quando se usa documentos eletrônicos? Digitalizar sua assinatura através de um scanner não é uma boa ideia, afinal, qualquer pessoa pode alterá-la em programas de edição de imagem. Enviar os documentos sem qualquer proteção via e-mail também tem seus riscos, já que alguém pode interceptá-los. O jeito então é utilizar uma assinatura digital.

A assinatura digital é um mecanismo eletrônico que faz uso de criptografia, mais precisamente, de *chaves criptográficas*. Desde já, o InfoWester recomenda que você leia este artigo sobre criptografia para entender melhor esse conceito.

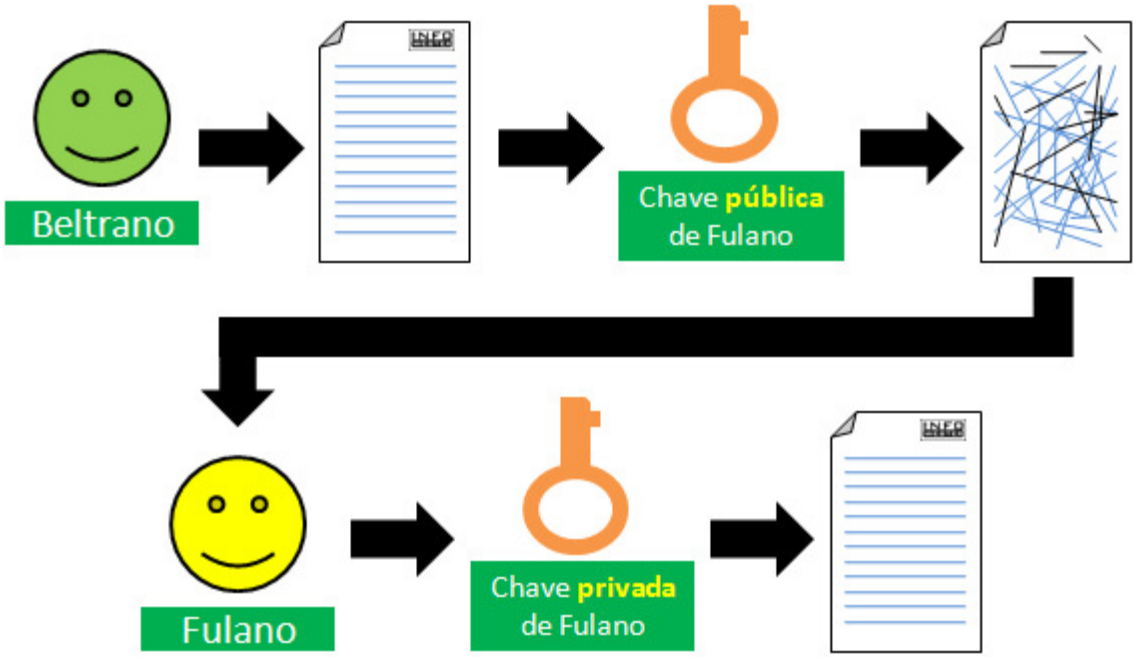
Chaves criptográficas são, em poucas palavras, um conjunto de bits baseado em um determinado algoritmo capaz de cifrar e decifrar informações. Para isso, pode-se usar *chaves simétricas* ou *chaves assimétricas*, estas últimas também conhecidas como *chaves públicas*.

Chaves simétricas são mais simples, pois com elas o emissor e o receptor utilizam a mesma chave para, respectivamente, cifrar e decifrar uma informação.

As chaves assimétricas, por sua vez, trabalham com duas chaves: a *chave privada* e a *chave pública*. Nesse esquema, uma pessoa ou uma organização deve utilizar uma chave de codificação e disponibilizá-la a quem for mandar informações a ela. Essa é a chave pública. Uma outra chave deve ser usada pelo receptor da informação para o processo de decodificação. Essa é a chave privada, que é sigilosa e individual. Ambas as chaves são geradas de forma conjunta, portanto, uma está associada a outra.

Note que esse método é bastante seguro, pois somente o detentor da chave privada conseguirá desfazer a cifragem realizada com a respectiva chave pública. Com chaves simétricas, os riscos são maiores, já que uma única chave é utilizada para cifragem e decifragem, aumentando consideravelmente as possibilidades de extravio ou fraudes. É por esta razão que chaves públicas são utilizadas em assinaturas digitais.

Em sua essência, o funcionamento das assinaturas digitais ocorre da seguinte forma: é necessário que o emissor tenha um documento eletrônico e a chave pública do destinatário. Através de algoritmos apropriados, o documento é então cifrado de acordo com esta chave pública. O receptor usará então sua chave privada correspondente para decifrar o documento. Se qualquer bit deste for alterado, a assinatura será deformada, invalidando o arquivo.



Na verdade, o processo de assinatura digital de documentos eletrônicos usa um conceito conhecido como *função hashing*. Como o uso de algoritmos de chaves públicas nas assinaturas digitais pode causar muita demora em um processo de decifragem, a função hashing se mostra como a solução ideal. Seu funcionamento ocorre da seguinte forma: o algoritmo da função hashing faz com que todo o documento a ser assinado seja analisado e, com base nisso, um valor de tamanho fixo é gerado. Trata-se do *valor hash* ou *resumo criptográfico*.

Com isso, o emissor usa sua chave privada e a chave pública do receptor para assinar digitalmente o documento. Se este sofrer qualquer alteração, por menor que seja, seu valor hash será diferente. Como consequência, o receptor receberá um documento inválido, já que sua chave só conseguirá lidar com o arquivo com o valor hash original.

O que é Certificado Digital?

Agora que você já sabe que o é assinatura digital, fica mais fácil compreender o certificado digital. Basicamente, trata-se de um documento eletrônico com assinatura digital que contém dados como nome do utilizador (que pode ser uma pessoa, uma empresa, uma instituição, etc), entidade emissora (você saberá mais sobre isso adiante), prazo de validade e chave pública. Com o certificado digital, a parte interessada obtém a certeza de estar se relacionando com a pessoa ou com a entidade desejada.

Um exemplo de uso de certificados digitais vem dos bancos. Quando uma pessoa acessa sua conta corrente pela internet, certificados digitais são usados para garantir ao cliente que ele está realizando operações financeiras com o seu banco. Se o usuário clicar no ícone correspondente no navegador de internet, poderá obter mais detalhes do certificado. Se algum problema ocorrer com o certificado - prazo de validade vencido, por exemplo -, o navegador alertará o usuário.

É importante frisar que a transmissão de certificados digitais deve ser feita através de conexões seguras, como as que usam o protocolo *Secure Socket Layer* (SSL), que é próprio para o envio de informações criptografadas.

Obtendo certificados digitais

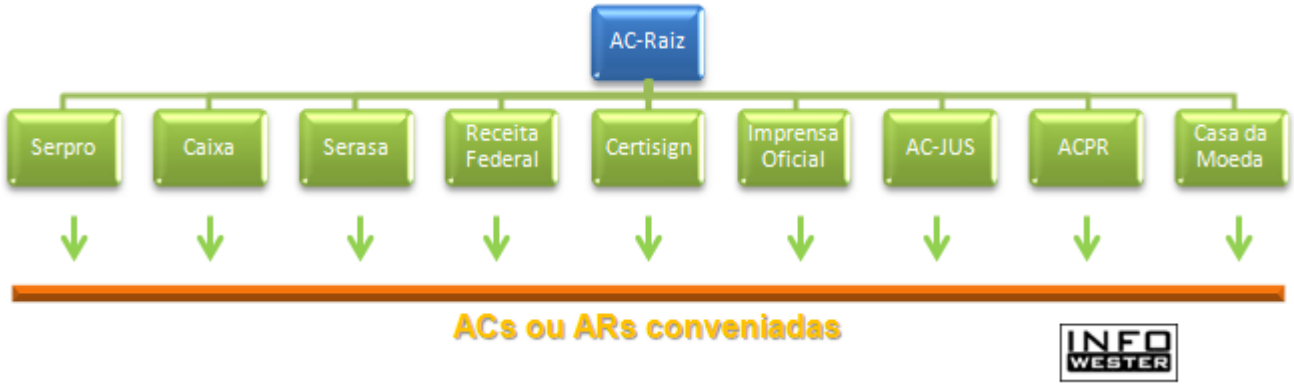
Para que possa ser aceito e utilizado por pessoas, empresas e governos, os certificados digitais precisam ser emitidos por entidades apropriadas. Sendo assim, o primeiro passo é procurar uma *Autoridade Certificadora* (AC) ou uma *Autoridade de Registro* (AR) para obter um certificado digital. Uma AC tem a função de associar uma identidade a uma chave e "inserir" esses dados em um certificado digital. Para tanto, o solicitante deve fornecer documentos que comprovem sua identificação. Já uma AR tem uma função intermediária, já ela pode solicitar certificados digitais a uma AC, mas não pode emitir esse documento diretamente.

É conveniente que cada nação conte com uma *Infra-estrutura de Chaves Públicas* (ICP) ou, em inglês, *Public Key Infrastructure* (PKI), isto é, um conjunto de políticas, técnicas e procedimentos para que a certificação digital tenha amparo legal e forneça benefícios reais à sua população. O Brasil conta com a **ICP-Brasil** para essa finalidade.

A ICP-Brasil trabalha com uma hierarquia onde a *AC-Raiz*, isto é, a instituição que gera as chaves das ACs e que regulamenta as atividades de cada uma, é o Instituto Nacional de Tecnologia da Informação (ITI). A ICP-Brasil tem, considerando a data de atualização deste artigo no InfoWester, nove ACs credenciadas:

- Serpro;
- Caixa Econômica Federal;
- Serasa;
- Receita Federal;
- Certisign;
- Imprensa Oficial;
- AC-JUS (Autoridade Certificadora da Justiça);
- ACPR (Autoridade Certificadora da Presidência da República);
- Casa da Moeda do Brasil.

São essas instituições que devem ser procuradas por quem deseja obter certificado digital legalmente reconhecido no Brasil. Note que cada uma dessas entidades pode ter critérios distintos para a emissão de certificados, o que inclusive resulta em preços diferentes, portanto, é conveniente ao interessado saber qual AC é mais adequada às suas atividades. Repare também que essas entidades podem ter ACs "secundárias" ou ARs ligadas a elas.



Tipos de certificados da ICP-Brasil

A ICP-Brasil oferece duas categorias de certificados digitais: *A* e *S*, sendo que cada uma se divide em quatro tipos: A1, A2, A3 e A4; S1, S2, S3 e S4. A categoria A é direcionada para fins de identificação e autenticação, enquanto que o tipo S é direcionado a atividades sigilosas. Vejas as características que tornam as versões de ambas as categorias diferentes entre si:

A1 e S1: geração das chaves é feita por software; chaves de tamanho mínimo de 1024 bits; armazenamento em dispositivo de armazenamento (como um HD); validade máxima de um ano;

A2 e S2: geração das chaves é feita por software; chaves de tamanho mínimo de 1024 bits; armazenamento em cartão inteligente (com chip) ou token (dispositivo semelhante a um pendrive); validade máxima de dois anos;

A3 e S3: geração das chaves é feita por hardware; chaves de tamanho mínimo de 1024 bits; armazenamento em cartão inteligente ou token; validade máxima de três anos;

A4 e S4: geração das chaves é feita por hardware; chaves de tamanho mínimo de 2048 bits; armazenamento em cartão inteligente ou token; validade máxima de três anos.

Os certificados A1 e A3 são os mais utilizados, sendo que o primeiro é geralmente armazenado no computador do solicitante, enquanto que o segundo é guardado em cartões inteligentes (*smartcards*) ou tokens protegidos por senha.

e-CPF e e-CNPJ

Falar de certificação digital no Brasil frequentemente remete a duas importantes iniciativas: o **e-CPF** e o **e-CNPJ**. O primeiro é, essencialmente, um certificado digital direcionado a pessoas físicas, sendo uma espécie de extensão do CPF (Cadastro de Pessoa Física), enquanto que o segundo é um certificado digital que se destina a empresas ou entidades, de igual forma, sendo um tipo de extensão do CNPJ (Cadastro Nacional da Pessoa Jurídica).

Ao adquirir um e-CPF, uma pessoa tem acesso pela internet a diversos serviços da Receita Federal, muitos dos quais até então disponíveis apenas em postos de atendimento da instituição. É possível, por exemplo, transmitir declarações de imposto de renda de maneira mais segura, consultar detalhes das declarações, pesquisar situação fiscal, corrigir erros de pagamentos, entre outros. No caso do e-CNPJ, os benefícios são semelhantes.

O e-CPF e o e-CNPJ estão disponíveis nos tipos A1 e A3. As imagens abaixo, obtidas no site da Receita Federal, mostram os modelos dos cartões inteligentes (tipo A3) para esses certificados:

É importante destacar que o e-CPF e o e-CNPJ não são gratuitos. Sua aquisição deve ser feita em entidades conveniadas à Receita Federal, como Certisign e Serasa. Os preços não são padronizados, variando de acordo com a empresa e com o tipo de certificado (A1 ou A3).

Finalizando

Antes do encerramento deste artigo, eis uma observação: você viu neste texto que é graças à ICP-Brasil que as certificações digitais no país são amplamente aceitas e utilizadas, especialmente do ponto de vista legal. No entanto, vale frisar que qualquer instituição pode criar sua própria ICP, independente de seu porte. Por exemplo, se uma empresa criou uma política de uso de certificados digitais unicamente para a troca de informações entre a matriz e sua filiais, não necessita solicitar tais certificados a uma AC controlada pela ICP-Brasil. A própria empresa pode criar sua ICP e fazer, por exemplo, com que um departamento das filiais atue como AC ou AR, solicitando ou emitindo certificados para seus funcionários.

No mais, se você quiser conhecer mais detalhes sobre certificação digital no Brasil, acesse o site do ITI:

- **www.iti.gov.br**.

Nele, é possível conseguir acesso a documentos sobre legislação, procedimentos, resoluções, entre outros, assim como obter notícias e orientações sobre o assunto.

Escrito por Emerson Alecrim - Publicado em 30/04/2009 - Atualizado em 27/02/2010