

O QUE É CERTIFICAÇÃO DIGITAL?

Os computadores e a Internet são largamente utilizados para o processamento de dados e para a troca de mensagens e documentos entre cidadãos, governo e empresas. No entanto, estas transações eletrônicas necessitam da adoção de mecanismos de **segurança** capazes de garantir **autenticidade**, **confidencialidade** e **integridade às informações eletrônicas**. A certificação digital é a tecnologia que provê estes mecanismos.

No cerne da certificação digital está o certificado digital, um documento eletrônico que contém o nome, um número público exclusivo denominado chave pública e muitos outros dados que mostram quem somos para as pessoas e para os sistemas de informação. A chave pública serve para validar uma assinatura realizada em documentos eletrônicos.

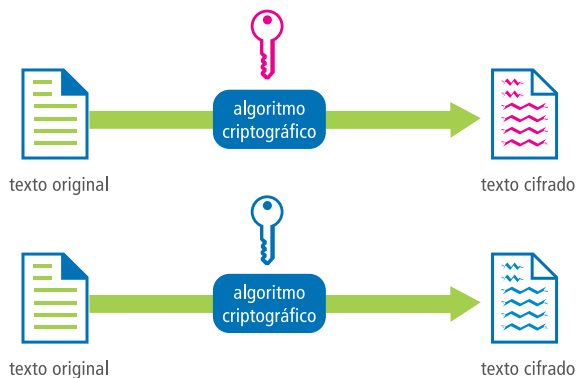
A certificação digital tem trazido **inúmeros benefícios** para os cidadãos e para as instituições que a adotam. Com a certificação digital é possível utilizar a Internet como meio de comunicação alternativo para a disponibilização de diversos serviços com uma maior agilidade, facilidade de acesso e substancial redução de custos. A tecnologia da certificação digital foi desenvolvida graças aos avanços da criptografia nos últimos 30 anos.



CRIPTOGRAFIA

A palavra criptografia tem origem grega e significa a **arte de escrever em códigos** de forma a esconder a informação na forma de um texto incompreensível. A informação codificada é chamada de texto cifrado. O processo de codificação ou ocultação é chamado de **cifragem**, e o processo inverso, ou seja, obter a informação original a partir do texto cifrado, chama-se **decifragem**.

A cifragem e a decifragem são realizadas por programas de computador chamados de cifradores e decifradores. Um programa cifrador ou decifrador, além de receber a informação a ser cifrada ou decifrada, recebe um número chave que é utilizado para definir como o programa irá se comportar. Os cifradores e decifradores se comportam de maneira diferente para cada valor da chave. Sem o conhecimento da chave correta não é possível decifrar um dado texto cifrado. Assim, para manter uma informação secreta, basta cifrar a informação e manter em sigilo a chave.





Atualmente existem dois tipos de criptografia: a simétrica e a de chave pública. A criptografia simétrica realiza a cifragem e a decifragem de uma informação através de algoritmos que utilizam a mesma chave, garantindo sigilo na transmissão e armazenamento de dados. Como a mesma chave deve ser utilizada na cifragem e na decifragem, a chave deve ser compartilhada entre quem cifra e quem decifra os dados. O processo de compartilhar uma chave é conhecido como **troca de chaves**. A troca de chaves deve ser feita de forma segura, uma vez que todos que conhecem a chave podem decifrar a informação cifrada ou mesmo reproduzir uma informação cifrada.

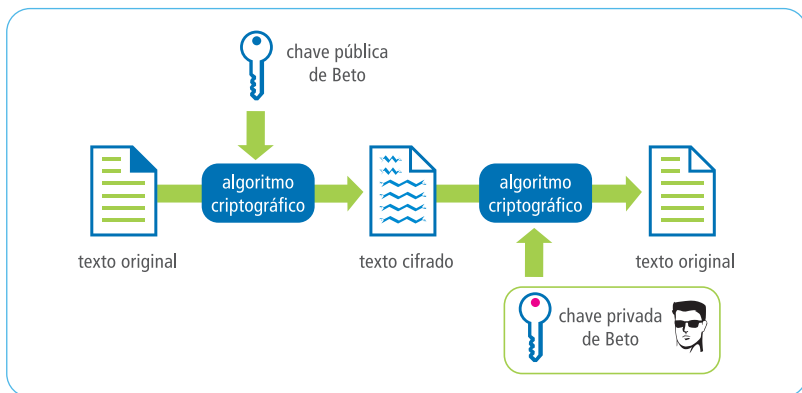
Os algoritmos de chave pública operam com duas chaves distintas: chave privada e chave pública. Essas chaves são geradas simultaneamente e são relacionadas entre si, o que possibilita que a operação executada por uma seja revertida pela outra. A chave privada deve ser mantida em sigilo e protegida por quem gerou as chaves. A chave pública é disponibilizada e tornada acessível a qualquer indivíduo que deseje se comunicar com o proprietário da chave privada correspondente.

ALGORITMOS CRIPTOGRÁFICOS DE CHAVE PÚBLICA

Os algoritmos criptográficos de chave pública permitem garantir tanto a confidencialidade quanto a autenticidade das informações por eles protegidas.

CONFIDENCIALIDADE

O emissor que deseja enviar uma informação sigilosa deve utilizar a chave pública do destinatário para cifrar a informação. Para isto é importante que o destinatário disponibilize sua chave pública, utilizando, por exemplo, diretórios públicos acessíveis pela Internet.

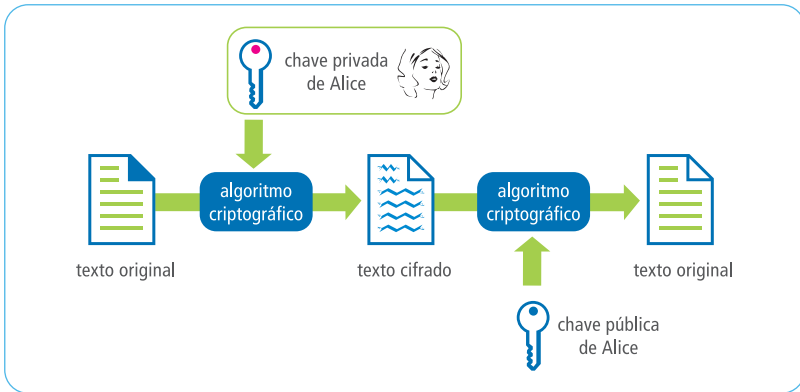


Sigilo utilizando criptografia assimétrica

O sigilo é garantido, já que somente o destinatário que possui a chave privada conseguirá desfazer a operação de cifragem, ou seja, decifrar e recuperar as informações originais. Por exemplo, para Alice compartilhar uma informação de forma secreta com Beto, ela deve cifrar a informação usando a chave pública de Beto. Somente Beto pode decifrar a informação pois somente Beto possui a chave privada correspondente.

AUTENTICIDADE

No processo de autenticação, as chaves são aplicadas no sentido inverso ao da confidencialidade. O autor de um documento utiliza sua chave privada para cifrá-lo de modo a garantir a autoria em um documento ou a identificação em uma transação. Esse resultado só é obtido porque a chave privada é conhecida exclusivamente por seu proprietário.



Autenticidade utilizando criptografia assimétrica

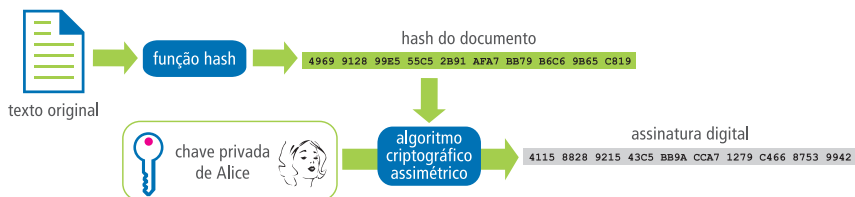
Assim, se Alice cifrar uma informação com sua chave privada e enviar para Beto, ele poderá decifrar esta informação pois tem acesso à chave pública de Alice. Além disto, qualquer pessoa poderá decifrar a informação, uma vez que todos conhecem a chave pública de Alice. Por outro lado, o fato de ser necessário o uso da chave privada de Alice para produzir o texto cifrado caracteriza uma operação que somente Alice tem condições de realizar.



ASSINATURA DIGITAL

O mesmo método de autenticação dos algoritmos de criptografia de chave pública operando em conjunto com uma função resumo, também conhecido como função de hash, é chamada de **assinatura digital**.

O resumo criptográfico é o resultado retornado por uma função de hash. Este pode ser comparado a uma impressão digital, pois cada documento possui um valor único de resumo e até mesmo uma pequena alteração no documento, como a inserção de um espaço em branco, resulta em um resumo completamente diferente.

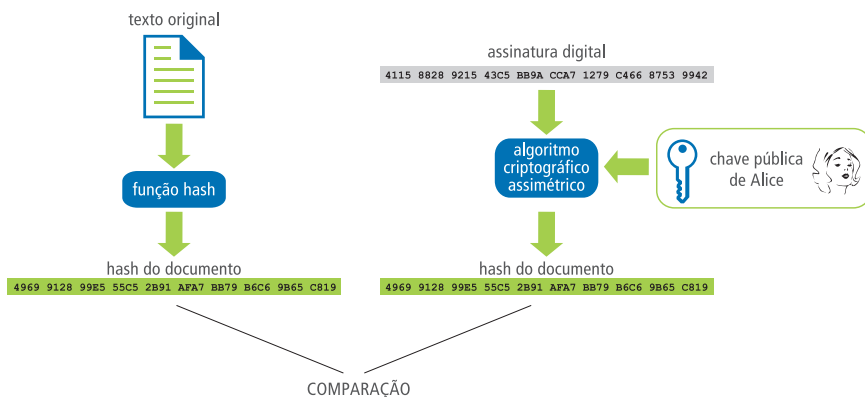


Assinatura digital utilizando algoritmos de chave pública

A vantagem da utilização de resumos criptográficos no processo de autenticação é o aumento de desempenho, pois os algoritmos de criptografia assimétrica são muito lentos. A submissão de resumos criptográficos ao processo de cifragem com a chave privada reduz o tempo de operação para gerar uma assinatura por serem os resumos, em geral, muito menores que o documento em si. Assim, consomem um tempo baixo e uniforme, independente do tamanho do documento a ser assinado.



Na assinatura digital, o documento não sofre qualquer alteração e o hash cifrado com a chave privada é anexado ao documento.



Conferência da assinatura digital

Para comprovar uma assinatura digital é necessário inicialmente realizar duas operações: calcular o resumo criptográfico do documento e decifrar a assinatura com a chave pública do signatário. Se forem iguais, a assinatura está correta, o que significa que foi gerada pela chave privada corresponde à chave pública utilizada na verificação e que o documento está íntegro. Caso sejam diferentes, a assinatura está incorreta, o que significa que pode ter havido alterações no documento ou na assinatura pública.



DOCUMENTO EM PAPEL X DOCUMENTO ELETRÔNICO

A semelhança da assinatura digital e da assinatura manuscrita restringe-se ao princípio de atribuição de autoria a um documento. Na manuscrita, as assinaturas seguem um padrão, sendo semelhantes entre si e possuindo características pessoais e biométricas de cada indivíduo. Ela é feita sobre algo tangível, o papel, responsável pela vinculação da informação impressa à assinatura. A veracidade da assinatura manuscrita é feita por uma comparação visual a uma assinatura verdadeira tal como aquela do documento de identidade oficial.

ASSINATURA MANUSCRITA

Nos documentos eletrônicos não existe um modo simples para relacionar o documento com a assinatura. Ambos são compostos apenas pela representação eletrônica de dados, ou seja, por uma seqüência de bits (0s e 1s), que necessitam de um computador para a sua visualização e conferência. Na assinatura digital, a assinatura gerada é diferente para cada documento, pois está relacionada ao resumo do documento.

ASSINATURA DIGITAL

Apesar das diferenças, a técnica de assinatura digital é uma forma eficaz de garantir autoria de documentos eletrônicos. Em agosto de 2001, a Medida Provisória 2.200 garantiu a validade jurídica de documentos eletrônicos e a utilização de certificados digitais para atribuir autenticidade e integridade aos documentos. Este fato tornou a assinatura digital um instrumento válido juridicamente.

O texto acima demonstra que o provimento de autenticação em documentos eletrônicos é viável tecnicamente, mas ainda restam duas questões fundamentais: como conseguir as chaves públicas? Como garantir a identidade do proprietário do par de chaves? A resposta a ambas as questões é o certificado digital.

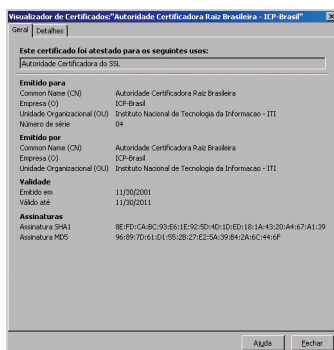


CERTIFICADO DIGITAL

O certificado digital é um documento eletrônico assinado digitalmente e cumpre a função de associar uma pessoa ou entidade a uma chave pública. As informações públicas contidas num certificado digital são o que possibilita colocá-lo em repositórios públicos.

Um **Certificado Digital** normalmente apresenta as seguintes informações:

- nome da pessoa ou entidade a ser associada à chave pública
- período de validade do certificado
- chave pública
- nome e assinatura da entidade que assinou o certificado
- número de série.



Certificado Digital da Autoridade Certificadora Raiz Brasileira – ICP Brasil

Um exemplo comum do uso de certificados digitais é o serviço bancário provido via Internet. Os bancos possuem certificado para autenticar-se perante o cliente, assegurando

do que o acesso está realmente ocorrendo com o servidor do banco. E o cliente, ao solicitar um serviço, como por exemplo, acesso ao saldo da conta corrente, pode utilizar o seu certificado para autenticar-se perante o banco.

Serviços governamentais também têm sido implantados para suportar transações eletrônicas utilizando certificação digital, visando proporcionar aos cidadãos benefícios como agilidade nas transações, redução da burocracia, redução de custos, satisfação do usuário, entre outros. Alguns destes casos de uso são:

GOVERNO FEDERAL: o Presidente da República e Ministros têm utilizado certificados digitais na tramitação eletrônica de documentos oficiais, que serão publicados no Diário Oficial da União. Um sistema faz o controle do fluxo dos documentos de forma automática, desde a origem dos mesmos até sua publicação e arquivamento.

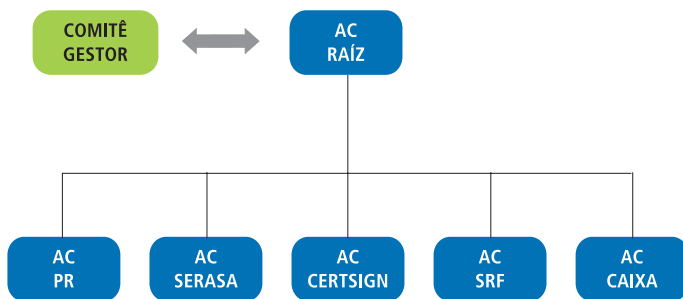
ESTADO DE PERNAMBUCO: primeiro estado brasileiro a utilizar a Certificação Digital. A Secretaria de Fazenda de Pernambuco disponibilizou um conjunto de serviços pela Internet com base na certificação digital que proporcionou diversos benefícios como: entrega de diversos documentos em uma única remessa; redução drástica no volume de erros de cálculo involuntários; apuração automática dos impostos; minimização de substituições de documentos e redução de custos de escrituração e armazenamento de livros fiscais obrigatórios.

IMPRESSA OFICIAL DO ESTADO DE SÃO PAULO: implantou certificação digital de ponta a ponta em seu sistema que automatiza o ciclo de publicações na Internet, permitindo a eliminação das ligações interurbanas e dos constantes congestionamentos telefônicos em horários de pico, uma vez que se utiliza a Internet com garantias de sigilo e privacidade, além da obtenção de garantia de autoria por parte do autor das matérias.




POR QUE CONFIAR EM UM CERTIFICADO DIGITAL?

Entre os campos obrigatórios do certificado digital encontra-se a identificação e a assinatura da entidade que o emitiu, os quais permitem verificar a autenticidade e a integridade do certificado. A entidade emissora é chamada de Autoridade Certificadora ou simplesmente AC. A AC é o principal componente de uma Infra-Estrutura de Chaves Públicas e é responsável pela emissão dos certificados digitais. O usuário de um certificado digital precisa confiar na AC.



A escolha de confiar em uma AC é similar ao que ocorre em transações convencionais, que não se utilizam do meio eletrônico. Por exemplo, uma empresa que vende parcelado aceita determinados documentos para identificar o comprador antes de efetuar a transação. Estes documentos normalmente são emitidos pela Secretaria de Segurança de Pública e pela Secretaria da Receita Federal, como o RG e o CPF. Existe, aí, uma relação de confiança já estabelecida com esses órgãos. Da mesma forma, os usuários podem escolher uma AC à qual desejam confiar a emissão de seus certificados digitais.



Para a emissão dos certificados, as ACs possuem deveres e obrigações que são descritos em um documento chamado de Declaração de Práticas de Certificação – DPC. A DPC deve ser pública, para permitir que as pessoas possam saber como foi emitido o certificado digital. Entre as atividades de uma AC, a mais importante é verificar a identidade da pessoa ou da entidade antes da emissão do certificado digital. O certificado digital emitido deve conter informações confiáveis que permitam a verificação da identidade do seu titular.

Por estes motivos, quanto melhor definidos e mais abrangentes os procedimentos adotados por uma AC, maior sua confiabilidade. No Brasil, o Comitê Gestor da ICP-Brasil é o órgão governamental que especifica os procedimentos que devem ser adotados pelas ACs. Uma AC que se submete às resoluções do Comitê Gestor pode ser credenciada e com isso fazer parte da ICP-Brasil. O cumprimento dos procedimentos é auditado e fiscalizado, envolvendo, por exemplo, exame de documentos, de instalações técnicas e dos sistemas envolvidos no serviço de certificação, bem como seu próprio pessoal. A não concordância com as regras acarreta em aplicações de penalidades, que podem ser inclusive o descredenciamento. As ACs credenciadas são incorporadas à estrutura hierárquica da ICP-Brasil e representam a garantia de atendimento dos critérios estabelecidos em prol da segurança de suas chaves privadas.



RESPONSABILIDADES

A certificação digital traz diversas facilidades, porém seu uso não torna as transações realizadas isenta de responsabilidades. Ao mesmo tempo que o uso da chave privada autentica uma transação ou um documento, ela confere o atributo de não-repúdio à operação, ou seja, o usuário não pode negar posteriormente a realização daquela transação. Por isto, é importante que o usuário tenha condições de proteger de forma adequada a sua chave privada.

Existem dispositivos que incrementam a proteção das chaves, como os cartões inteligentes (smart cards). Eles se assemelham – em formato e tamanho – a um cartão de crédito convencional. Os smart cards são um tipo de hardware criptográfico dotado de um microprocessador com memória capaz de armazenar e processar diversos tipos de informações. Com eles é possível gerar as chaves e mantê-las dentro de um ambiente seguro, uma vez que as operações criptográficas podem ser realizadas dentro do próprio dispositivo.



Alguns usuários preferem manter suas chaves privadas no próprio computador. Neste caso, são necessárias algumas medidas preventivas para minimizar a possibilidade de se comprometer a sua chave privada:

- caso o software de geração do par de chaves ofereça a opção de proteção do acesso à chave privada através de senha, essa opção deve ser ativada, pois assim há a garantia de que, na ocorrência do furto da chave privada, a mesma esteja cifrada;
- não compartilhar com ninguém a senha de acesso à chave privada;
- não utilizar como senha dados pessoais, palavras que existam em dicionários ou somente números, pois são senhas facilmente descobertas. Procurar uma senha longa, com caracteres mistos, maiúsculos e minúsculos, números e pontuação;
- em ambiente acessível a várias pessoas, como em um escritório, usar produtos de controle de acesso ou recursos de proteção ao sistema operacional, como uma senha de sistema ou protetor de tela protegido por senha;
- manter atualizado o sistema operacional e os aplicativos, pois versões mais recentes contêm correções que levam em consideração as vulnerabilidades mais atuais;
- não instalar o certificado com a chave privada em computadores de uso público.

Em caso de suspeita de comprometimento da chave privada, seja por uma invasão sofrida no computador ou pelo surgimento de operações associadas ao uso da chave que não sejam de conhecimento do seu proprietário, a revogação do certificado deve ser solicitada o mais rapidamente possível à AC responsável pela sua emissão. Além disso, é necessário estar alerta às recomendações da DPC quanto aos procedimentos necessários a revogação do certificado.



VALIDADE

O certificado digital, diferentemente dos documentos utilizados usualmente para identificação pessoal como CPF e RG, possui um período de validade. Só é possível assinar um documento enquanto o certificado é válido. É possível, no entanto, conferir as assinaturas realizadas mesmo após o certificado expirar.

O certificado digital pode ser revogado antes do período definido para expirar. As solicitações de revogação devem ser encaminhadas à AC que emitiu o certificado ou para quem foi designada essa tarefa. As justificativas podem ser por diversos fatores como comprometimento da chave privada, alterações de dados do certificado ou qualquer outro motivo.

A AC, ao receber e analisar o pedido, adiciona o número de série do certificado a um documento assinado chamado Lista de Certificados Revogados (LCR) e a publica. O local de publicação das LCRs está declarado na DPC da AC que emitiu o certificado, e em muitos casos o próprio certificado possui um campo com apontador para um endereço WEB que contém o arquivo com a LCR. As LCRs são publicadas de acordo com a periodicidade que cada AC definir. Essas listas são públicas e podem ser consultadas a qualquer momento para verificar se um certificado permanece válido ou não.

Após a revogação ou expiração do certificado, todas as assinaturas realizadas com este certificado tornam-se inválidas, mas as assinaturas realizadas antes da revogação do certificado continuam válidas se houver uma forma de garantir que esta operação foi realizada durante o período de validade do certificado. Mas como obter essa característica? Existem técnicas para atribuir a indicação de tempo a um documento, chamadas carimbo de tempo. Estes carimbos adicionam uma data e hora à assinatura, permitindo determinar quando o documento foi assinado.



Linha do tempo do certificado e assinatura digital

O usuário pode solicitar a renovação do certificado para a AC após a perda de validade deste. Na solicitação, o usuário pode manter os dados do certificado e até mesmo o par de chaves, se a chave privada não tiver sido comprometida. Mas, por que não emitir os certificados sem data final de validade? Porque a cada renovação da validade do certificado renova-se também a relação de confiança entre seu titular e a AC.

Essa renovação pode ser necessária para a substituição da chave privada por uma outra tecnologicamente mais avançada ou devido a possíveis mudanças ocorridas nos dados do usuário. Essas alterações têm como objetivo tornar mais robusta a segurança em relação às técnicas de certificação e às informações contidas no certificado.