Assinatura Digital de Documentos Eletrônicos no Brasil: Conceitos Básicos e Infraestrutura

Apresentação

A utilização de documentos em papel, com aposição de assinaturas manuscritas ou impressões digitais, constitui prática que atravessa gerações. As civilizações aprenderam, por força da tradição, a conferir status de confiança aos documentos assim firmados. Os recentes avanços da tecnologia da informação e comunicação, contudo, produziram instrumentos adequados à modernização destes procedimentos. Novidades tecnológicas na gestão e segurança de documentos eletrônicos vêm lançando uma nova perspectiva sobre o tema, gerando debates, projetos e iniciativas variadas.

No Brasil, a criação da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), através da Medida Provisória 2.200-2/2001, representou um marco histórico para a nação ao conferir eficácia probante aos documentos eletrônicos assinados digitalmente. Como resultado, a substituição de documentos físicos por equivalentes eletrônicos vem ganhando atenção crescente no país. Diversas iniciativas governamentais - como a Lei nº 11.419, de 19 de dezembro de 2006, que trata da informatização do processo judicial, e a Lei nº 11.382, de 6 de dezembro de 2006, que trata de alienação judicial pela internet (leilão de bens penhorados) - já requerem o uso de certificação digital e fomentam a adoção dessas novas tecnologias.

Entretanto, toda a legislação e tecnologia do mundo são insuficientes para se usufruir de seus benefícios se houver escassez de um componente fundamental: a informação.

O que é um certificado digital? O que é assinatura digital? O que é carimbo do tempo? Estas são apenas algumas das perguntas encontradas neste material, com respostas didáticas e objetivas.

Desejamos a você uma boa leitura e esperamos que esta iniciativa contribua para uma expansão ainda maior do uso de documentos eletrônicos seguros no nosso país.

Sumário

Sumário

O que é um certificado digital?

Um certificado digital é um documento de identidade eletrônico que tem o objetivo de identificar uma pessoa, empresa ou sistema computacional no mundo dos computadores ou da internet.

Um certificado digital possui informações sobre a entidade para a qual foi emitido (no caso de uma pessoa, possui o seu nome, CPF etc.). Além destes dados, contém uma sequência de código conhecida como chave pública.

Associada ao certificado digital, existe uma segunda sequência de código, esta secreta, denominada de chave privada. Esta chave é armazenada em local físico protegido, de preferência um smartcard ou token. Por ser exclusiva, é utilizada para gerar assinaturas digitais que não podem ser imitadas.

A chave pública é utilizada para certificar-se de que um determinado arquivo foi assinado pelo detentor da chave privada daquele certificado.

Certificados digitais são utilizados para diversos fins, tais como assinaturas de documentos eletrônicos, autenticação perante sistemas e sigilo de informações, entre outros.

O que é preciso para se obter um certificado digital?

Primeiramente, o interessado em um certificado digital precisa gerar uma requisição e juntar alguns documentos, tais como cópia do seu RG, CPF e comprovante de residência. Esta requisição é normalmente feita pelo próprio interessado na página web de uma Autoridade Certificadora e encaminhada, via internet, a uma Autoridade de Registro (AR). Posteriormente, o interessado deve se dirigir pessoalmente à AR, levando consigo os documentos solicitados. Na AR, os agentes de registro conferem os dados e, se tudo estiver correto, enviam a requisição do certificado para a Autoridade Certificadora, responsável por sua emissão.

voltar ao sumário

O que é uma Autoridade de Registro?

Uma Autoridade de Registro (AR) é uma entidade que verifica os dados do solicitante de um certificado digital. Assim como uma AC, as AR precisam ser credenciadas e periodicamente auditadas pela AC-Raiz. Além da conferência dos dados, a AR tem a obrigação de verificar pessoalmente a identidade do titular. Isso é feito por funcionários da AR especialmente treinados para este fim, conhecidos como agentes de registro. Os agentes de registro, após conferirem os dados diante do titular, encaminham à Autoridade Certificadora a requisição do certificado. Após a emissão do certificado pela AC, o certificado é entregue ao solicitante pelos próprios agentes de registro ou através de uma consulta a uma página web. De posse de certificado, o titular pode assinar documentos eletrônicos.

voltar ao sumário

O que é uma Autoridade Certificadora?

Uma autoridade certificadora é uma entidade que emite certificados digitais. No Brasil, a autoridade certificadora (AC) precisa ser credenciada e periodicamente auditada pela Autoridade Certificadora Raiz (AC-Raiz). Um certificado digital só é emitido pela AC após a conferência dos dados do usuário, que é feita por Autoridades de Registro (AR).

O que é a Autoridade Certificadora Raiz?

É a entidade certificadora de mais alto nível do sistema de certificação digital. É nela que todos confiamos e é a partir dela que é criada toda a rede de confiança de todos os certificados emitidos no âmbito da ICP-Brasil. Todas as entidades integrantes da ICP-Brasil precisam de autorização da AC-Raiz para funcionar.

O que é uma Infraestrutura de Chaves Públicas (ICP)?

É um conjunto de normas, procedimentos e serviços computacionais que permitem a emissão e a utilização confiável de certificados digitais.

O que é a ICP-Brasil?

A Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) é um conjunto de normas, padrões, procedimentos e entidades que têm por objetivo manter, no Brasil, uma estrutura segura para a emissão de certificados digitais. A ICP-Brasil é governada por um Comitê Gestor (CG), formado por representantes do governo e da sociedade civil, e por uma Comissão Técnica (Cotec), que tem por objetivo auxiliar os membros do Comitê Gestor. Além dessas duas comissões, faz parte da ICP-Brasil o Instituto Nacional de Tecnologia da Informação (ITI), responsável por implementar a AC-Raiz e de credenciar e auditar todas as entidades integrantes da infraestrutura. Atualmente, podem ser credenciadas na ICP-Brasil autoridades certificadoras (AC), autoridades de registro (AR), autoridades de carimbo do tempo (ACT), prestadores de serviço de suporte (PSS) e auditores independentes.

O que é um documento eletrônico seguro?

É um documento eletrônico assinado digitalmente por um signatário com um certificado digital emitido por autoridade certificadora credenciada pela ICP-Brasil. O documento eletrônico seguro e sua assinatura não podem ser modificados sem que essas modificações sejam detectadas pelo destinatário do documento. Um documento eletrônico seguro é equivalente a um documento que teve sua firma reconhecida por um cartório.

O que é assinatura digital?

Uma assinatura digital é o conjunto de dados que são gerados a partir do processo de assinatura de um arquivo. A partir da assinatura digital, é possível verificar a integridade e a autoria de um documento eletrônico. Os dados de uma assinatura digital podem estar anexos ao documento eletrônico ou em outro arquivo externo.

Como é produzida e validada uma assinatura digital?

Para assinar ou verificar a integridade e autoria de um documento eletrônico são usadas respectivamente a chave privada e as informações contidas do certificado digital do signatário.

A chave para assinar, conhecida como chave privada, é mantida secreta e armazenada em local físico protegido, de preferência um smartcard ou token.

A chave para verificar a assinatura, denominada chave pública, é disponibilizada no próprio documento a todos os destinatários (pessoas e sistemas) que precisam verificar a assinatura.

Assim, na prática, utiliza-se, para assinar o documento, um software assinador e o smartcard; e para verificar a assinatura desse documento, um software validador e a chave pública do certificado digital do signatário, inclusa no documento eletrônico.

Para impedir que alguém de posse do smartcard do signatário possa assinar documentos em seu nome, uma senha é utilizada. Essa senha é conhecida como número de identificação pessoal ou, em Inglês, Personal Identification Number (PIN). Sempre que o signatário precisar assinar um documento, o sistema de assinatura solicitará o PIN do smartcard. Com o PIN, o sistema de assinatura pode invocar o smartcard para gerar a assinatura de um documento. O smartcard deve ser de uso exclusivo do signatário e nunca cedido a terceiros.

voltar ao sumário

O que é carimbo do tempo?

É uma informação de data e hora segura aplicada a uma assinatura digital. Assim, o carimbo do tempo serve como evidência de que a assinatura de um documento eletrônico era válida naquela data e hora.

Qual a vantagem de se aplicar um carimbo do tempo nas assinaturas digitais?

A presença de um carimbo de tempo prorroga a vida da assinatura de um documento eletrônico, uma vez que é possível verificá-la com base na data em que a assinatura foi produzida.

Uma assinatura sem um carimbo só permanece válida enquanto o certificado do signatário é válido. No entanto, com a aposição de um carimbo à assinatura, mesmo que o certificado do assinante deixe de ser válido após a assinatura do documento - seja por revogação ou expiração -, a verificação da assinatura é feita com base na data e hora em que foi produzida. Com o carimbo, a assinatura mantém-se válida enquanto o carimbo é válido. Neste sentido, devem ser periodicamente adicionados novos carimbos à assinatura se for necessário preservá-la por longo prazo.

De que forma o carimbo do tempo garante a data e hora correta da assinatura?

Na prática, um carimbo de tempo é um documento eletrônico assinado que contém o hash de sua respectiva assinatura e a data e hora de sua geração. Os carimbos de tempo são gerados por um sistema computacional confiável, o Sistema de Carimbo do Tempo (SCT). O relógio do SCT garante a data e hora correta, pois é sincronizado pelo Sistema de Auditoria e Sincronismo (SAS) da Autoridade Certificadora Raiz.

O que preciso fazer para aplicar um carimbo do tempo nas minhas assinaturas? Preciso de um certificado digital especial?

Alguns softwares assinadores permitem que, ao realizar a assinatura, seja invocado um SCT para a emissão de um carimbo do tempo no documento. Isso é feito de forma transparente para os signatários, e não é necessário um certificado digital especial para isso.

Sou obrigado a usar carimbo do tempo nas assinaturas digitais? O que acontece se eu optar por não o utilizar?

O uso de um carimbo do tempo não é obrigatório. No entanto, sempre que for preciso manter a assinatura digital válida por um período de tempo maior que aquele estipulado para o certificado digital do signatário, ou mesmo para evitar que a assinatura deixe de ser válida pelo ato de sua revogação, é necessário incluir na assinatura um carimbo do tempo.

Na prática, em qualquer documento que precise manter seu valor probante por períodos superiores a alguns dias, é imperativa a inclusão de carimbos do tempo na assinatura. Uma assinatura sem um carimbo deixa de ser válida se o certificado do signatário deixar de ser válido. Isso acontece se o certificado do signatário expirar ou se qualquer certificado da cadeia de certificação, incluindo o do signatário, for revogado. As assinaturas digitais sem um carimbo de tempo são conhecidas como assinaturas de curto prazo ou de uso restrito.

O que é o Padrão Brasileiro de Assinatura Digital?

É um conjunto de regras publicadas no Diário Oficial da União no dia 13 de janeiro de 2009 que garantem a produção de assinaturas digitais confiáveis, sua preservação a longo prazo e a interoperabilidade entre todos os sistemas computacionais que a adotam.

As assinaturas produzidas em conformidade com o padrão podem ser entendidas e verificadas pelos mais diversos sistemas de informação de instituições públicas e privadas. Assim, um documento assinado respeitando o padrão brasileiro de assinatura digital poderá ser
enviado ou recebido com a garantia de que a assinatura vai ser entendida pelas partes.

O que é o Padrão Brasileiro de Carimbo do Tempo?

É um conjunto de regras que permitem a emissão de carimbos do tempo confiáveis.

O tempo adicionado ao carimbo é rastreável até o relógio atômico da AC-Raiz Brasileira, mantido pelo Instituto Nacional de Tecnologia da Informação (ITI). Carimbos emitidos segundo o padrão brasileiro podem ser lidos e entendidos pelos mais diversos sistemas computacionais existentes.

Quais são as motivações para a criação do Padrão Brasileiro de Assinatura Digital e de Carimbo do Tempo?

As motivações são a manutenção da integridade e autenticidade por longo prazo e a garantia de legibilidade por todos dos documentos eletrônicos. Na prática, os documentos eletrônicos produzidos seguindo os preceitos desses padrões terão a garantia de que podem ser lidos e processados com segurança, ao longo do tempo, de forma praticamente independente da evolução tecnológica, tal como a substituição de antigos computadores por novos, de novas versões de sistemas operacionais ou a substituição de velhos sistemas de informação por outros mais modernos.

A partir de quando estes padrões entrarão em vigor?

O prazo final para as instituições adotarem o padrão brasileiro de assinatura digital é 12 de janeiro de 2010. O padrão brasileiro de carimbo do tempo já é válido, mas ainda falta a implantação da infraestrutura que proverá o serviço de sincronização de relógios para as Autoridades de Carimbo do Tempo (ACT). A instalação dessa infraestrutura pelo ITI está prevista para acontecer no último trimestre de 2009.

O Sistema SAJ vai mudar em função da aprovação destes novos padrões?

Internamente, sim. Todas as funcionalidades do sistema que realizam assinatura de documentos serão alteradas para realizar e validar assinaturas digitais conforme o padrão estabelecido. Para os usuários do SAJ, o sistema permanecerá o mesmo. A diferença é que os documentos assinados no SAJ poderão ser validados em qualquer outra aplicação que siga o padrão brasileiro de assinatura digital.

O que minha organização precisa fazer para utilizar o carimbo do tempo?

Você pode ter seu próprio sistema de carimbo do tempo, alugar um ou mesmo usar os serviços, via internet, de uma Autoridade de Carimbo do Tempo. Esses carimbos são emitidos por servidores e mantidos por autoridades de carimbo do tempo. Dependendo do volume e do requisito de disponibilidade de carimbos que um cliente ou instituição necessite, pode-se escolher entre utilizar os serviços remotos de uma Autoridade de Carimbo de Tempo (ACT) comercial, instalar uma carimbadora desta ACT na instituição ou ainda tornar-se uma ACT.

Onde posso obter mais informações sobre assinatura digital e carimbo de tempo?

Na página da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) - http://www.icpbrasil.gov.br – ou do Instituto Nacional de Tecnologia da Informação (ITI) – http://www.iti.gov.br – é possível obter mais informações sobre a regulamentação e detalhes técnicos relacionados a assinatura digital e carimbos de tempo. A Câmara Brasileira de Comércio Eletrônico - http://www.camara-e.net - também disponibiliza excelente material didático sobre o assunto.

Softplan

Poligraph