

CERTIFICAÇÃO ELETRÔNICA DOS ARQUIVOS DE PROTESTO

Objetivo

Este documento visa apresentar o projeto de Assinatura Digital dos arquivos de protesto transmitidos, entre os Bancos e os Tabelionatos.

Assinatura Digital

Muitos confundem o conceito de assinatura digital com digitalização de assinaturas, ou senha eletrônica ou até mesmo assinar em uma tela ou *pad* eletrônico. Abaixo seguem alguns conceitos para entender este novo paradigma.

A. O que é Assinatura Digital?

A assinatura digital é uma modalidade de assinatura eletrônica, resultante de uma operação matemática que utiliza algoritmos de criptografia 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.

B. Quais são as propriedades da assinatura digital?

Autenticidade (Quem assina é quem diz ser)

Integridade (Os dados não podem ser alterados)

Irretratibilidade/Não Repúdio (Não se pode negar ou cancelar a assinatura)

C. Amparo Legal na MP2200

Esta medida provisória (que tem caráter de lei) equipara juridicamente a assinatura digital à assinatura de punho:

No Art. 10. Consideram-se documentos públicos ou particulares, para todos os fins legais, os documentos eletrônicos de que trata esta Medida Provisória.

§ 1º As declarações constantes dos documentos em forma eletrônica produzidos com a utilização de processo de certificação disponibilizado pela ICP-Brasil presumem-se verdadeiros em relação aos signatários, na forma do art. 131 da Lei nº 3.071, de 1º de janeiro de 1916 - Código Civil.

§ 2º O disposto nesta Medida Provisória não obsta a utilização de outro meio de comprovação da autoria e integridade de documentos em forma eletrônica, inclusive os que utilizem certificados não emitidos pela ICP-Brasil, desde que admitido pelas partes como válido ou aceito pela pessoa a quem for oposto o documento.

D. ICP-Brasil

A ICP-Brasil (Infra-estrutura de Chaves Públicas no Brasil) é um órgão do Governo Federal (Casa Civil) que normatiza a Assinatura Digital no Brasil.

Este órgão é responsável pela arquitetura, organização técnicas, práticas e procedimentos que servem de base para implementação e operação do sistema criptográfico usado em certificados.

BENEFÍCIOS

1. Maior segurança (integridade dados)

A tecnologia de Assinatura Digital garante que o arquivo não foi alterado após assinatura.

2. Maior controle (sabe-se quem e quando assinou)

Através do rigoroso processo de certificação ICP-Brasil e também pela segurança oferecida pelo smartcard (cartão inteligente a prova de clonagem) é possível garantir a origem da assinatura realizada.

Além disto, todas as assinaturas são chanceladas com um carimbo de tempo para registrar a data e horário de cada operação, garantindo o recebimento dos arquivos pelos Tabelionatos.

3. Dá validade jurídica aos arquivos

Conforme a MP-2200, toda assinatura efetuada por um certificado emitido debaixo da ICP-Brasil tem validade jurídica como uma assinatura de punho.

4. Facilidade de expansão da arquitetura

Uma vez implementada a infra-estrutura necessária, a mesma poderá ser utilizada para outros processos de transmissão de arquivos assinados digitalmente.

PADRÃO DE ASSINATURA

Segue abaixo o padrão dos arquivos assinados digitalmente que é determinado pelo Bacen e Febraban:

- O formato é o PKCS#7 Signed-Data na codificação Base 64 ANSI

- Será aceita a transmissão via EDI-7 ou HTTPS Post

OBS.: Não foi escolhida a codificação binária ao invés da Base 64, pois a mesma pode causar transtornos na transmissão, quando do aparecimento de caracteres especiais no meio.

Não foi escolhido o formato UNICODE ao invés do ANSI, pois o mesmo pode causar problemas em comunicações via XML, com o truncamento das mensagens. Geralmente um texto com a codificação UNICODE é composto por uma "letra" e um "zero binário". Neste caso, o "zero binário" será interpretado com fim de "string".