BITSIGN

ASSINATURAS DIGITAIS

VALIDAÇÃO DE ASSINATURAS

Entenda como verificar a autenticidade de documentos assinados, incluindo o Manifesto de Assinaturas.

Versão 1.1 – Fevereiro/2022

https://bitsign.com.br

CONTEÚDO

INTRODUÇÃO 3
PADRÕES DE ASSINATURAS DIGITAIS 3
MANIFESTO DE ASSINATURAS 4
VISUALIZADOR DE DOCUMENTOS 5
AUTENTICIDADE DE ASSINATURA 6
ARTEFATOS 8
SUPORTE 9

INTRODUÇÃO

Os documentos assinados digitalmente produzem artefatos criptográficos e que precisam de ferramentas específicas para validar a autenticidade e integridade do respectivo documento. A BITSIGN oferece, na área pública de seu site, uma seção que permite a qualquer usuário a validar documentos assinados digitalmente, independente se tenha sido ou não assinado por sua plataforma. Este tutorial detalha como realiza esta validação.

PADRÕES DE ASSINATURAS DIGITAIS

Para que documentos (arquivos) que são assinados digitalmente tenham validade, eles precisam seguir um conjunto de regras e diretrizes que são mundialmente conhecidas, que tem a finalidade de estruturar como os artefatos da assinatura digital são gerados e armazenados. Atualmente existem três formatos e eles e suas características são detalhadas abaixo:

CAdES CMS Advanced Electronic Signatures	**PAdES** PDF Advanced Electronic Signatures	**XAdES** XML Advanced Electronic Signatures
Um dos mais flexíveis padrões, ele permite assinar qualquer tipo de documento (arquivo), desde planilhas em *Excel*, documentos PDF e até arquivos executáveis (EXE). Tem uma boa aceitação no mercado, mas como resultado, produz um arquivo com extensão **P7S**, que exigirá o uso de ferramentas ou visualizadores específicos para inspecionar, validar e visualizar o seu conteúdo.	Este padrão recorre à estrutura do próprio arquivo **PDF** para gerar e armazenar a assinatura digital. Um dos seus principais benefícios é ter a possibilidade de estampar no próprio documento os dados da assinatura, aproximando o modelo eletrônico ao que existe no mundo físico (impresso), facilitando sua análise e visualização. Obviamente está restrito a documentos PDF.	O padrão XAdES é específico para assinatura de documentos em formato **XML**. Em geral, arquivos XML servem para integração entre sistemas, e a assinatura nestes tipos de arquivos, tem a finalidade de garantir que os dados transitem entre a origem e o destino sem qualquer alteração. Este modelo é utilizado atualmente durante a emissão de documentos fiscais (NF-e, CT-e, etc.).

Cada um destes formatos possui características próprias para realizar a sua geração, o que inclui políticas de assinatura que a **ICP-Brasil** (órgão governamental que rege as assinaturas digitais no Brasil) especificou para garantir a validade jurídica delas. De acordo

com o padrão selecionado, a BITSIGN se encarrega de selecionar a política atual vigente e gerar os artefatos que atendam todas as normais atuais de cada um deles.

MANIFESTO DE ASSINATURAS

Para todos os arquivos submetidos para a ferramenta, a BITSIGN gera um relatório chamado de **"Manifesto de Assinaturas"**, que é um documento que detalha todas as assinaturas realizadas no arquivo (documento), o que inclui os dados do(s) assinante(s), a data em que foi assinado e as informações do certificado digital que foi apresentado e utilizado para a assinatura.

BITSIGN
ASSINATURAS DIGITAIS

MANIFESTO DE ASSINATURAS

Nome do Arquivo: **Documento.pdf.p7s**
Formato (Padrão): **application/x-pkcs7-signature (CAdES)**
Código: **2495d665-8939-4666-8213-ae3800b11e2d**
Tamanho: **< 1MB**
Data da Análise: **15/02/2022 às 11:15** (BRT)

Nome do Arquivo (Original): **Documento.pdf**
Descrição: **Nomeação para Cargo Administrativo**
Tipo: **Autorização**
Hash: **(SHA1) - 5FE7DFFF17245E0CF044F101FF834F4C6A559202**
Recebimento: **10/02/2022 às 07:44:51**
Conclusão: **15/02/2022 às 11:14:54**

ASSINATURAS
em ordem cronológica
Quantidade: **1** assinatura(s)

#	ASSINANTE	DATA	CERTIFICADO
1ª.	Jack Bauer CPF: 545.107.020-27 E-mail: jack.bauer@ctu.com Complemento: **Declarante**	**15/02/2022 às 11:14:52** Data da Assinatura (BRT (-03:00))	Emissor: BITSIGN - Ambiente de Sandbox Emissão: 10/02/2022 às 04:52:38 Validade: 10/03/2022 às 04:52:37 Número de Série: 00ED6CC4AB65012D6ABF6310398362...

Itens Analisados: Carimbo do Tempo · Integridade da Assinatura · Raiz Emissora · Revogação do Certificado

Este manifesto tem a única finalidade de apresentar, de uma forma amigável, as assinaturas que foram realizadas e constam no documento (arquivo) informado. São exibidos os dados de cada assinante, com o nome, o número do CPF/CNPJ e e-mail; além disso, é também apresentado diversos outros dados associados à assinatura, como a data em que a mesma foi realizada e o certificado (com suas características) utilizado. A BITSIGN é capaz de avaliar a integridade do documento, certificando de que seja um documento válido, que está estruturalmente correto e que atende as normas da certificação digital, porém não atesta que as entidades assinantes tem ou não poderes para tal; isso é de inteira responsabilidade do solicitante das assinaturas. Por fim, é importante dizer que este manifesto de assinaturas não tem qualquer validade legal. A base para qualquer auditoria ou análise de fraude deverá ser sempre realizada sobre o arquivo original digitalmente assinado, onde constarão todos os artefatos que foram gerados pelos algoritmos de criptografia, e que são, eventualmente, regulados pelas políticas de assinaturas.

https://www.bitsign.com.br
Página 1 de 1

Este relatório é disponibilizado de forma totalmente gratuita para qualquer usuário, contratante ou não, que queira validar um determinado arquivo/documento. Quando se tratar de um documento assinado pela própria plataforma, algumas informações complementares são exibidas, incluindo um *QR Code*, que informa o *link* oficial onde o documento está hospedado na BITSIGN; isso garante, para a pessoa que recebe o documento, que ele foi assinado pela própria plataforma.

Este manifesto tem a única finalidade de apresentar, de uma forma amigável, as assinaturas que foram realizadas e constam no documento (arquivo) informado. A BITSIGN é capaz de avaliar a integridade do documento, certificando de que seja um documento válido, que está estruturalmente correto e que atende as normas da certificação digital, porém não atesta que as entidades assinantes têm ou não poderes para tal; isso é de inteira responsabilidade do solicitante das assinaturas.

É importante dizer que este manifesto de assinaturas não tem qualquer validade legal. A base para qualquer auditoria ou análise de fraude deverá ser sempre realizada sobre o arquivo original, onde consta todos os artefatos que foram gerados pelos algoritmos de criptografia, e que são, eventualmente, regulados pelas políticas de assinaturas.

VISUALIZADOR DE DOCUMENTOS

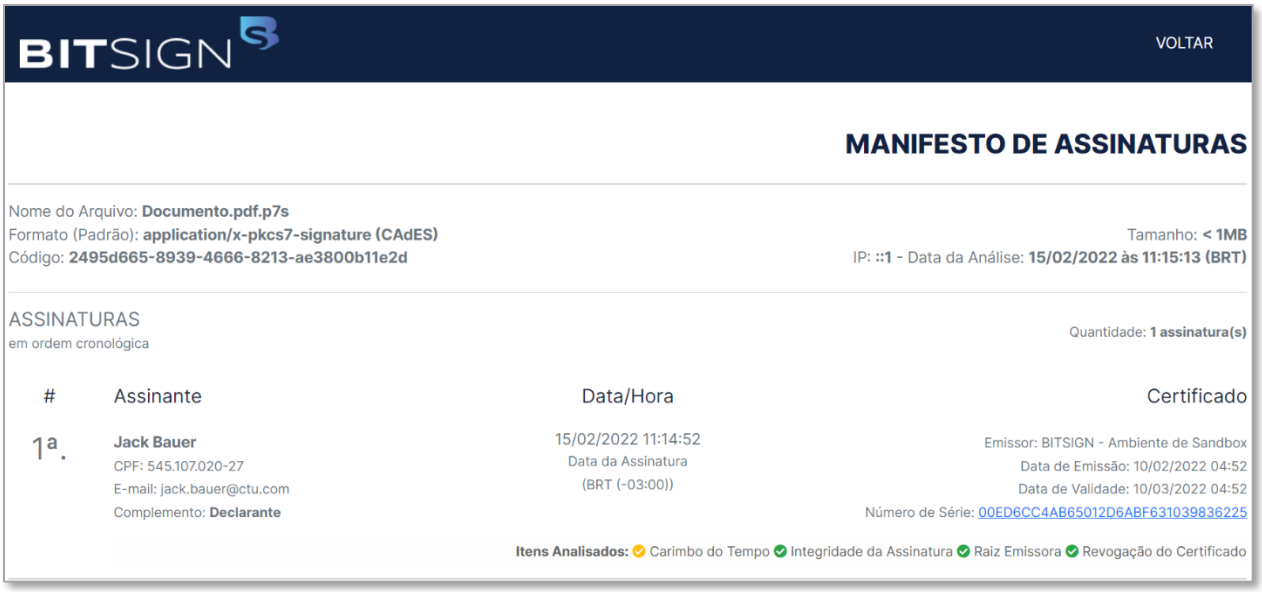
Como mencionado anteriormente, dependendo da forma como o documento é assinado, haverá a necessidade de *softwares* específicos para visualização e validação das assinaturas.

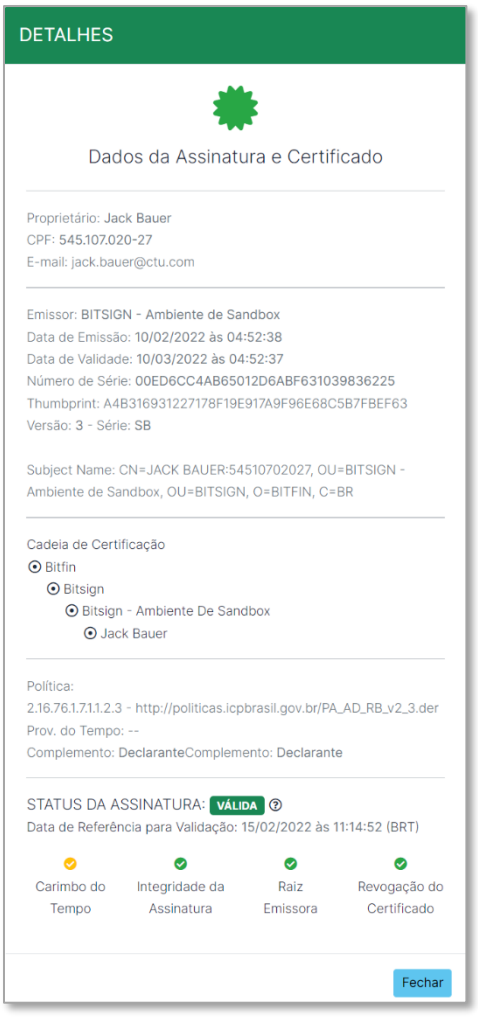
Sabendo desta dificuldade, a BITSIGN disponibiliza em seu site (https://bitsign.com.br), logo na página inicial, um visualizador (e validador) de documentos digitalmente assinados. Ele permite validar e certificar documentos assinados pela própria plataforma, bem como realizar a validação e exibição de documentos assinados por outros sites e serviços. Através da imagem a seguir vemos as duas opções que podemos utilizar, a depender daquilo que se tem à mão para validar.

- **Arquivo:** se estiver de posse de um arquivo digitalmente assinado (um PDF, um XML ou um arquivo P7S), você poderá submeter utilizando a opção **"Selecionar Arquivo"**; mesmo que este arquivo tenha sido assinado por outras plataformas ou aplicações, se estiver em conformidade com as especificações da ICP-Brasil, a BITSIGN será capaz de analisar e exibir os detalhes, incluindo a possibilidade da geração de "Manifesto de Assinaturas";
- **Código de Verificação:** já esta opção é exclusiva para documentos assinados na plataforma da BITSIGN. Todo documento cadastrado na plataforma recebe um identificador único, e que de posse dele, você poderá clicar no botão **"Código de Verificação"** e informá-lo; neste momento a BITSIGN tentará localizar e, se encontrado, exibirá todos os detalhes da assinatura, incluindo a possibilidade da geração do "Manifesto de Assinaturas". Este código de verificação possui 36 caracteres e é algo como *"D9FC0A47-BB42-4D8F-BDCF-84319C23F53B"*. Você poderá encontrá-lo estampado no documento ou no próprio "Manifesto de Assinaturas".

AUTENTICIDADE DE ASSINATURA

Independente da opção escolhida, se o arquivo estiver íntegro ou o código do documento for localizado, as assinaturas encontradas serão exibidas (em ordem cronológica), contendo as informações de cada um dos assinantes e os dados de qual certificado foi utilizado.





Ao clicar sobre o *link* que está no número de série do certificado, são exibidas mais informações sobre a respectiva assinatura, incluindo todo o detalhamento do certificado, a cadeia de certificação (emissores intermediários e raiz); inclui também a política de assinatura utilizada (as políticas definem um conjunto de regras e atributos que qualificam as assinaturas digitais e que são, geralmente, criadas e geridas pela ICP-Brasil.

Por fim, é exibida o *status* da assinatura, que pode ser válida ou inválida. Junto ao *status*, são apresentadas as validações que são realizadas: análise do carimbo do tempo, integridade da assinatura, raiz emissora válida e revogação do certificado.

ARTEFATOS

Depois de analisado e validado, a BITSIGN oferece algumas opções que permitem ao usuário, a depender da sua necessidade, baixar um ou mais documentos que exibem e/ou certificam as assinaturas digitais encontradas. As opções são apresentadas no final da página, conforme é mostrado através da imagem a seguir:

- **Documento Original:** refere-se ao documento original que foi mandado pelo contratante para fazer a coleta da(s) assinatura(s);
- **Documento Assinado:** arquivo que possui, além do conteúdo, todas as informações criptográficas sobre as assinaturas. É este arquivo que é sua garantia e que em caso de questionamento ou fraude, é ele que deve ser submetido para análise, auditoria ou perícia;
- **Manifesto de Assinaturas:** relatório para simples conferência, contendo a análise das assinaturas realizadas;
- **Original + Manifesto:** quando se tratar de um arquivo PDF assinado no padrão CAdES, é possível gerar um relatório do documento original, sufixado o "Manifesto de Assinaturas", que também é de simples conferência, ou seja, é útil para anexar ou imprimir, mas o que garante a autenticidade é o "Documento Assinado".

SUPORTE

Para outras informações ou maiores esclarecimentos, entre em contato através do endereço de e-mail contato@bitsign.com.br ou através do *WhatsApp* pelo número (19) 9.9901-1065. Opcionalmente você poderá consultar também a seção de ajuda no site da BITSIGN, que disponibiliza outros conteúdos: https://bitsign.com.br/ajuda.