**Assinatura**

**1. Introdução**

O Flowbee oferece 2 modalidades de assinatura à seus usuários, assinatura eletrônica e digital. Ambas modalidades de assinatura resultam em uma assinatura digital usando um certificado A1 no servidor, no entanto são separadas em 2 tipos para que o usuário não seja obrigado a ter um certificado digital para fazer assinaturas.

Para entender os detalhes do processo de assinatura acesse o documento: <https://docs.google.com/document/d/1iCbWQ5gesCBcb46a1MHWjLB9nRAq7ZibcYcVvlTC9FI/edit?usp=sharing>

**1.1 Assinatura Eletrônica**

A assinatura eletrônica é uma maneira simplificada de assinar um documento, o processo todo é feito em duas etapas. Inicialmente basta que o usuário informe alguns dados pessoais como nome, documento e e-mail. Dessa forma o sistema responde com um token para confirmação da assinatura que deve ser informado na etapa final.

Nesse processo o servidor utiliza um certificado digital previamente configurado para realizar a assinatura no documento, utilizando apenas os dados do usuário.

**1.2. Assinatura Digital**

Na assinatura digital o sistema espera que o usuário possua um certificado digital o qual será utilizado para assinar o documento. A diferença desse processo para o anterior é que toda a parte de validação do certificado é realizada no lado do cliente, ou seja, no próprio navegador do usuário através da extensão Web PKI da Lacuna (o tutorial de instalação é exibido durante o processo de assinatura se necessário).

Também é realizado em duas etapas, a primeira o cliente escolhe o certificado que deseja usar e a extensão Web PKI faz a leitura da chave pública do mesmo, essa informação é enviada ao servidor que responde com um hash de assinatura, este usado na segunda etapa pela extensão Web PKI para efetivar a assinatura.

**2. Pré requisitos**

Para utilizar a funcionalidade de assinatura eletrônica é preciso configurar o certificado digital e senha na configuração do sistema.

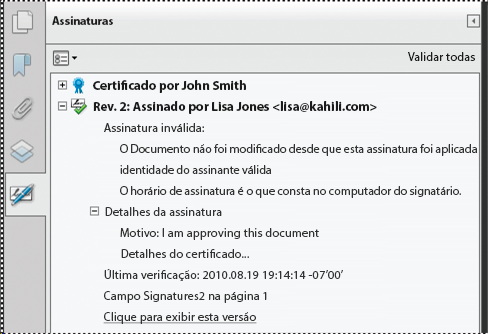
Para utilizar a assinatura digital é preciso obter uma licença do Lacuna atualizada para o domínio em questão (exceto localhost) e configurá-la na parte de configurações do sistema. Também é preciso instalar a extensão do web PKI conforme o tutorial <https://get.webpkiplugin.com/Setup?brand=&jslib=&browser=Chrome&returnUrl=>.

Mais detalhes acesse a documentação de configuração: <https://docs.google.com/document/d/1dAaJbI0ycWviingLpWnFbVOKKZv0ODDs_O18S-1MqS8/edit?usp=sharing>**.**

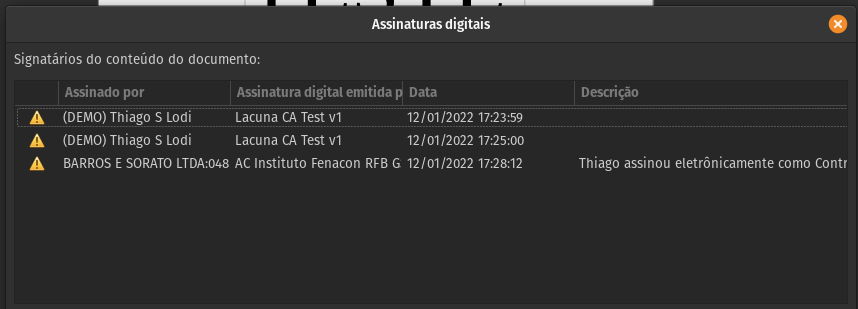
**3.Visualização da assinatura**

Para visualizar os dados da assinatura (digital ou eletrônica) é preciso abrir a versão assinada do documento em um visualizador de PDF, os mais comuns são Adobe Acrobat Reader (Windows e Mac) e LibreOffice Draw (Windows, Mac e Linux).

No Adobe: O painel “Assinaturas” exibe informações sobre cada assinatura digital no documento e o histórico de alterações desde a primeira assinatura digital. Cada assinatura digital possui um ícone que identifica seu status de verificação. Os detalhes de verificação são listados atrás de cada assinatura e podem ser visualizados quando a assinatura for expandida. O painel Assinaturas também fornece informações sobre o horário em que o documento foi assinado e os detalhes sobre o signatário e o nível de segurança.



No Libre Office Draw acesse o menu ***Arquivos > Assinaturas Digitais > Assinaturas Digitais…*** dessa forma uma janela pop-up será exibida com os detalhes da(s) assinatura(s) realizada(s) no documento.



**4. API**

**4.1. [POST] /documentos/{id}/assinaturas/digitais/iniciar**

Inicia o processo de assinatura digital.

**Path parameters:**

{id} - ID do documento

**Exemplo de request body (Plain Text):**

certificado: Conteúdo público do certificado digital.

**Exemplo de response body:**

{

"algoritmoHash": "string",

"assinaturaTemporariaId": "string",

"hashParaAssinar": "string"

}

Os dados retornados pela API nesse passo serão usadas para finalizar a assinatura no passe seguinte.

**4.2. [POST] /documentos/{id}/assinaturas/digitais/finalizar**

Finaliza o processo de assinatura digital.

**Path parameters:**

{id} - ID do documento

**Exemplo de request body (JSON):**

| Nome | Tipo | Obrigatório | Descrição |
| --- | --- | --- | --- |
| assinatura | String | Sim | Hash identificador da assinatura realizada pelo Web PKI |
| assinaturaTemporariaId | String | Sim | ID da assinatura temporária iniciada pelo processo anterior |
| dadosExtras | Object Array | Não | Lista de objetos contendo dados de autenticidade da assinatura |
| participacao | String | Não | Participação do signatário no documento |
| rubricaBase64 | String | Não | Imagem em Base64 da rubrica do signatário |

O parâmetro **dadosExtras** é uma lista de objetos do tipo:

{

"nome":"string",

"tipoDado":"TEXTO | IMAGEM\_BASE\_64 | DATA | DATA\_HORA",

"valor":"string"

}

**Exemplo de response body:**

{

"assinatura":"string",

"assinaturaTemporariaId":"string",

"dadosExtras":[

{

"nome":"string",

"tipoDado":"TEXTO",

"valor":"string"

}

],

"participacao":"string",

"rubricaBase64":"string"

}

Exemplo de dado extra:

Abaixo foi adicionado um dado extra chamado Endereço eletrônico.



**4.3. [POST] /documentos/{id}/assinaturas/eletronicas/iniciar**

Inicia o processo de assinatura eletrônica.

**Path parameters:**

{id} - ID do documento

**Query parameters:**

| Nome | Tipo | Obrigatório | Descrição |
| --- | --- | --- | --- |
| enviarTokenPorEmail | boolean | não (padrão: false) | Booleano que indica se o código de confirmação da assinatura deve ser enviado por email |

**Exemplo de request body (JSON):**

| Nome | Tipo | Obrigatório | Descrição |
| --- | --- | --- | --- |
| cpf | String | Sim | cpf ou documento do signatário |
| dadosExtras | Object Array | Não | Lista de objetos contendo dados de autenticidade da assinatura |
| email | String | Sim | email do signatário |
| participacao | String | Não | Participação do signatário no documento |
| rubricaBase64 | String | Não | Imagem em Base64 da rubrica do signatário |
| telefone | String | Não | Telefone |

O parâmetro **dadosExtras** é uma lista de objetos do tipo:

{

"nome":"string",

"tipoDado":"TEXTO | IMAGEM\_BASE\_64 | DATA | DATA\_HORA",

"valor":"string"

}

**Exemplo de response body:**

{

"assinaturaDados":"string",

"codigoConfirmacao":"string"

}

**4.4. [POST] /documentos/{id}/assinaturas/eletronicas/finalizar**

Finaliza o processo de assinatura eletrônica.

**Path parameters:**

{id} - ID do documento

**Query parameters:**

| Nome | Tipo | Obrigatório | Descrição |
| --- | --- | --- | --- |
| token | string | sim | Token de confirmação da assinatura |

**Exemplo de response body:**

{

"sha512":"string"

}