# Manual de Instalação

Procedimento para instalação em diversos cenários

Sumário

[Manual de Instalação 1](#_Toc455483528)

[Sumário 2](#_Toc455483529)

[O que é? 5](#_Toc455483530)

[Processo de instalação do Servidor (Vagrant e Virtual Box) 7](#_Toc455483531)

[Processo de instalação do Servidor (JDK e Tomcat) 10](#_Toc455483532)

[Download dos Componentes para instalação 11](#_Toc455483533)

[Processo de instalação das ACs Confiáveis 12](#_Toc455483534)

[Processo de configuração do Log 13](#_Toc455483535)

[Processo de instalação (clientes) 14](#_Toc455483536)

[Processo de instalação (do servidor e do exemplo) 15](#_Toc455483537)

[Componentes cliente e sua compatibilidade 16](#_Toc455483538)

[Componente ActiveX 18](#_Toc455483539)

[Componente Apple Java 19](#_Toc455483540)

[Componente Rest Signer 20](#_Toc455483541)

[Componente Extensão Chrome 21](#_Toc455483542)

[Utilizando a aplicação 24](#_Toc455483543)

[Utilizando o activeX 25](#_Toc455483544)

[Requisitos 25](#_Toc455483545)

[Acessando a pagina 25](#_Toc455483546)

[Upload do conteúdo 26](#_Toc455483547)

[Inicie a assinatura 27](#_Toc455483548)

[Escolha o certificado 28](#_Toc455483549)

[Digite a senha 29](#_Toc455483550)

[O sistema exibe o resultado 30](#_Toc455483551)

[Utilizando o Applet Java CAPI 31](#_Toc455483552)

[Requisitos 31](#_Toc455483553)

[Acessando a pagina 31](#_Toc455483554)

[Upload do conteúdo 32](#_Toc455483555)

[Inicie a assinatura 33](#_Toc455483556)

[Escolha o certificado 34](#_Toc455483557)

[Digite a senha 35](#_Toc455483558)

[O sistema exibe o resultado 36](#_Toc455483559)

[Utilizando o Applet Java PKCS#11 37](#_Toc455483560)

[Requisitos 37](#_Toc455483561)

[Acessando a pagina 38](#_Toc455483562)

[Upload do conteúdo 39](#_Toc455483563)

[Selecione o mecanismo 39](#_Toc455483564)

[Escolha o certificado 41](#_Toc455483565)

[Inicie a assinatura 42](#_Toc455483566)

[O sistema exibe o resultado 43](#_Toc455483567)

[Utilizando o Rest Signer 44](#_Toc455483568)

[Requisitos 44](#_Toc455483569)

[Acessando a pagina 44](#_Toc455483570)

[Upload do conteúdo 45](#_Toc455483571)

[Escolha o certificado 46](#_Toc455483572)

[Digite a senha 47](#_Toc455483573)

[O sistema exibe o resultado 48](#_Toc455483574)

[Utilizando a extensão para o Chrome 49](#_Toc455483575)

[Requisitos 49](#_Toc455483576)

[Acessando a pagina 49](#_Toc455483577)

[Upload do conteúdo 51](#_Toc455483578)

[Escolha o certificado 52](#_Toc455483579)

[Digite a senha 53](#_Toc455483580)

[O sistema exibe o resultado 54](#_Toc455483581)

# O que é?

Ferramenta para desenvolvedores.

A solução divide-se em 2 componentes:

Servidor: Responsável pela validação dos certificados, geração de envelopes criptográficos..

Cliente: Responsável por todas as operações que envolvam acesso à chave privada;

Esse manual descreve ainda a instalação do exemplo que permite a qualquer usuário ver o sistema operacional.

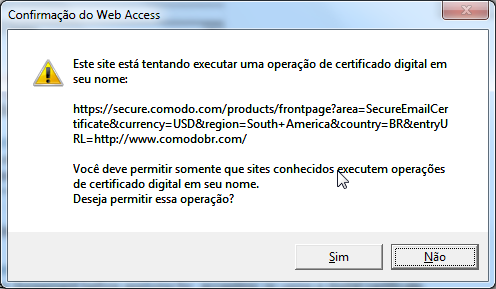
# Criando um certificado de testes

Muitas vezes os desenvolvedores precisam configurar e testar o ambiente e não possuem um certificado digital ICP-Brasil. Assim, descrevemos o procedimento para emitir um certificado de testes.

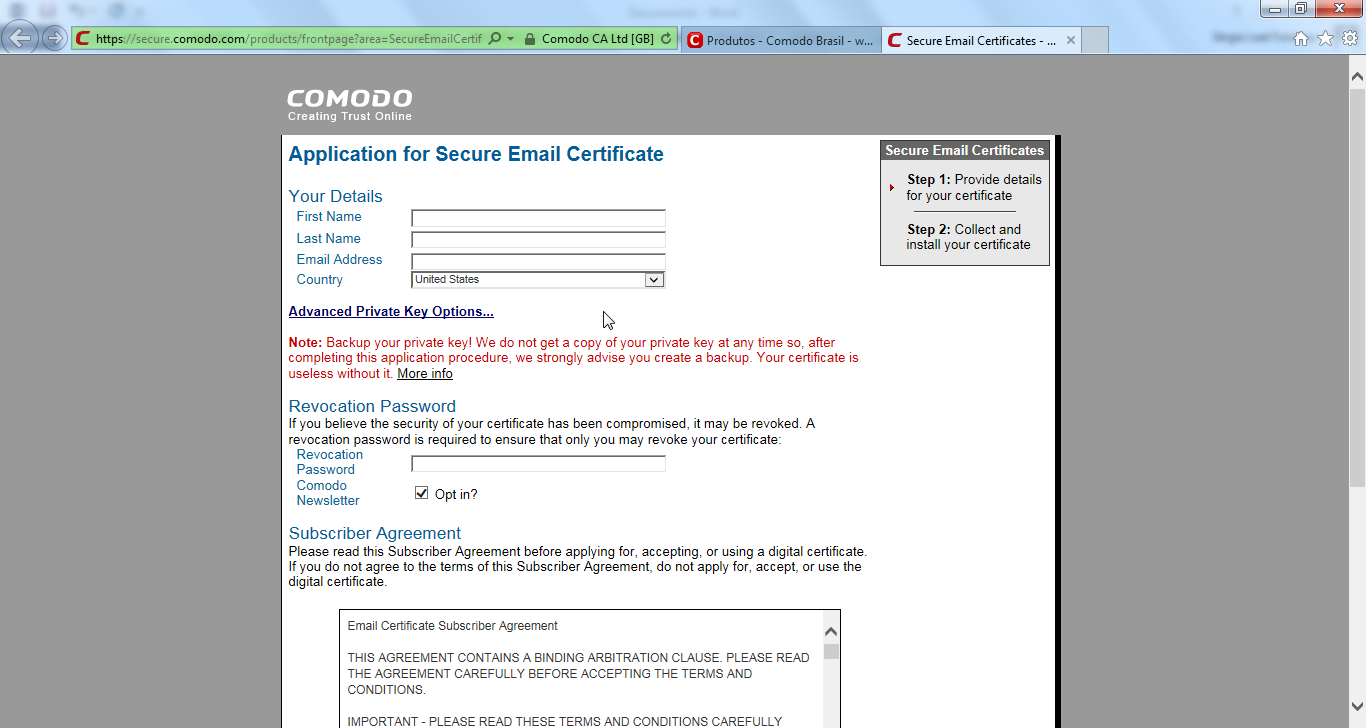
1. Acesse a pagina de Email Seguro Gratis da Comodo (https://secure.comodo.com/products/frontpage?area=SecureEmailCertificate&currency=USD&region=South+America&country=BR&entryURL=http://www.comodobr.com/.);
2. Se você for utilizar o Firefox apenas preencha os dados do formulário e siga em frente;
3. O certificado estará disponível no repositório do Firefox, mas não no do Windows;

Caso você deseje utilizar o repositório do Windows, ou armazenar seu certificado em token ou smart card, siga os passos abaixo. Não abordaremos como utilizar token e smart card no Linux ou Mac.

1. Iniciamente você será questionado sobre o acesso aos serviços de certificados. Diga “Sim”;

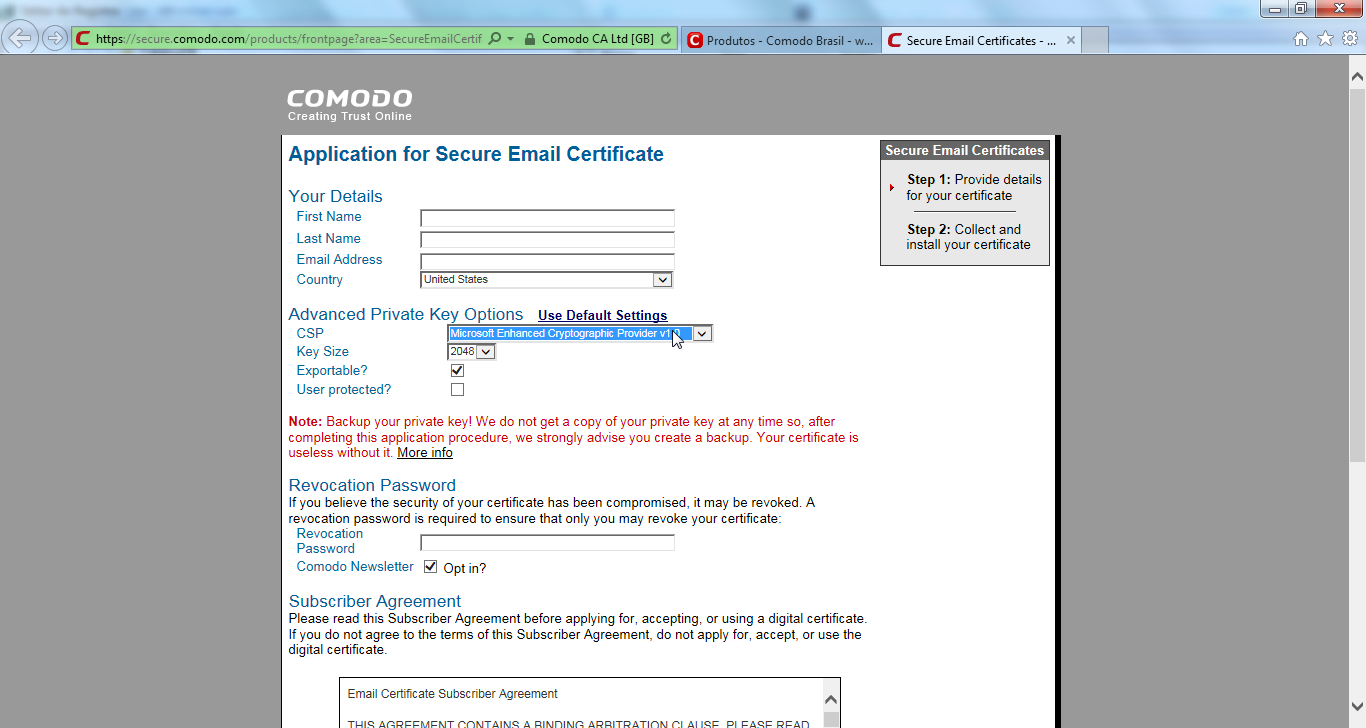


1. Selecione a opção “Advanced Private Key Options”;

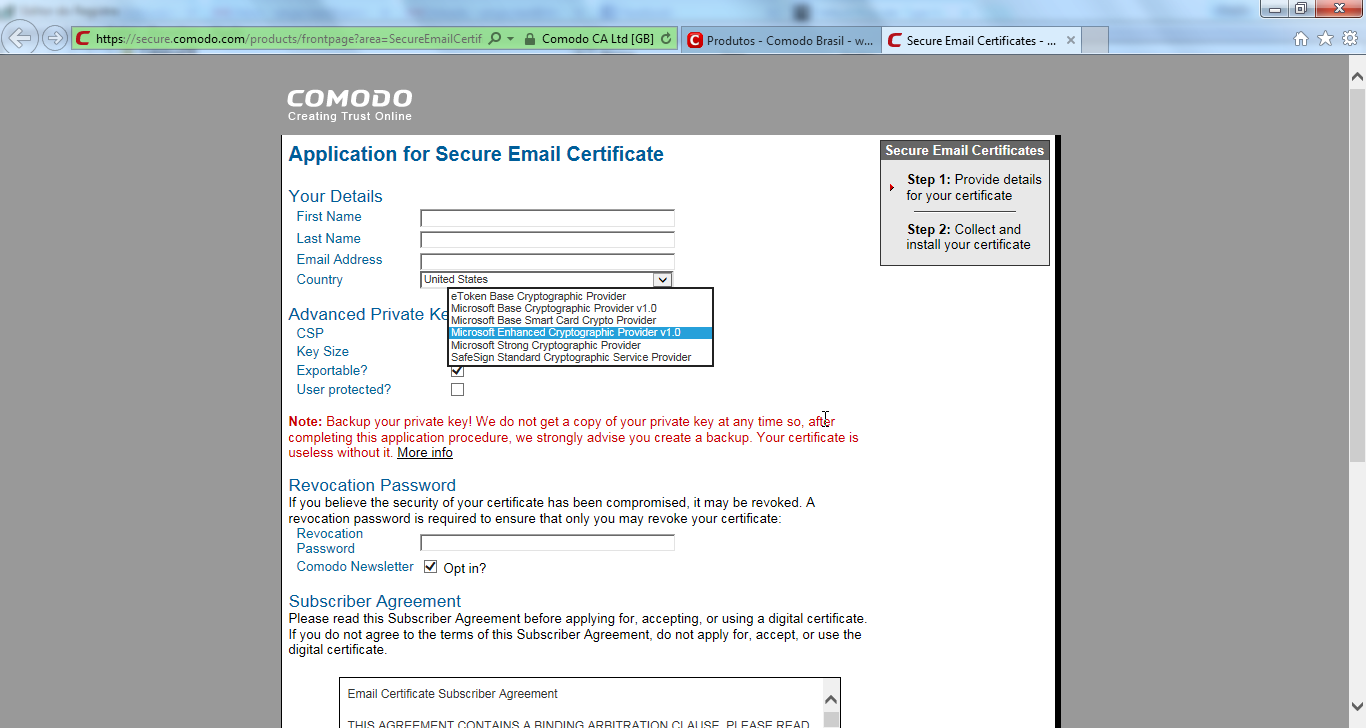


É importante selecionar:

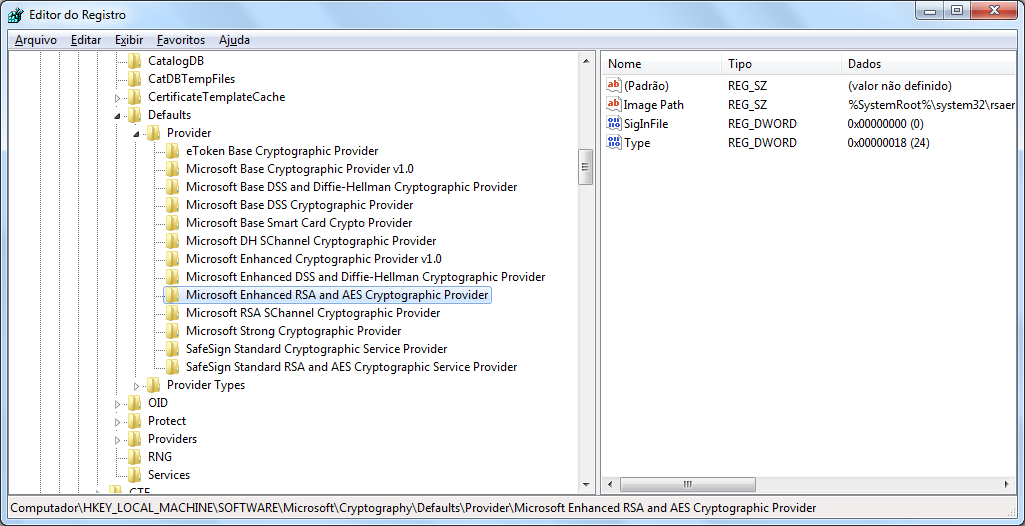
* Key Size: 2048;
* Exportable: Selecionado;
* User protected: Não selecionado;



Na hora de selecionar o “CSP”, você deve selecionar o “Microsoft Enhanced RSA and AES Cryptographic Provider” (caso apareça na lista). Ou o “CSP” relativo ao seu Token ou Smart card;



Na dúvida, abra a Registry (usando o regedit) e verifique na chave (*HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Cryptography\Defaults\Provider*) qual dos provedores tem o tipo “24”).



Caso não exista na lista nenhum provedor com o tipo “24” escolha outro genérico.

# Processo de instalação do Servidor (Vagrant e Virtual Box)

Essa é a maneira mais simples de instalar localmente para avaliação.

1. Faça a instalação do Virtual Box (<https://www.virtualbox.org/>);
2. Faça a instalação do Vagrant (<https://www.vagrantup.com/>);
3. [Em seguida copie para sua máquina o arquivo “Vagrantfile” do repositório:](http://www.oracle.com/technetwork/pt/java/javase/downloads/jdk8-downloads-2133151.html)

* Para subir um servidor baseado no Ubuntu 14.04 (<https://github.com/bluecrystalsign/signer-deploy/tree/master/vagrant/ubuntu14.04-tomcat8>[);](http://www.oracle.com/technetwork/pt/java/javase/downloads/jdk8-downloads-2133151.html)
* Para subir um servidor baseado no CentOS 7.2 (<https://github.com/bluecrystalsign/signer-deploy/tree/master/vagrant/centos7.2-tomcat8>[);](http://www.oracle.com/technetwork/pt/java/javase/downloads/jdk8-downloads-2133151.html)

1. Abra o “command” do Windows (executando o programa “cmd”) ou o “shell” do Linux ou MacOS;
2. Mude para o diretório onde colocou o arquivo do passo 5;
3. Execute o comando:
   * *vagrant up*
4. Quando terminar a execução (aparecer novamente o prompt) teste o funcionamento com: [**http://localhost:8080/**](http://localhost:8080/) você deve ver a tela inicial do tomcat.

# Processo de instalação do Servidor (JDK e Tomcat)

1. A instalação pode ser feita no Windows, Mac OS X ou Linux;
2. [Instale o JDK 8 (http://www.oracle.com/technetwork/pt/java/javase/downloads/jdk8downloads-2133151.html);](http://www.oracle.com/technetwork/pt/java/javase/downloads/jdk8-downloads-2133151.html)
3. [Baixe e descompacte o Tomcat](https://tomcat.apache.org/download-80.cgi) [8 Core (https://tomcat.apache.org/download-](https://tomcat.apache.org/download-80.cgi)

[80.cgi);](https://tomcat.apache.org/download-80.cgi)

1. Chamaremos a pasta raiz do Tomcat de **<raiz tomcat>***;*

## Download dos Componentes para instalação

Utilize o repositório disponível em:

<https://github.com/bluecrystalsign/signer-distibution>

## Processo de instalação das ACs Confiáveis

1. Extraia o arquivo **AcRepo.zip**;
   1. Crie a pasta **<raiz tomcat>/AcRepo;**
   2. Extraia o conteúdo desse arquivo para a pasta **<raiz tomcat>/AcRepo;**
2. Copie o arquivo **bluc.properties**;
   1. Copie esse arquivo para a pasta **<raiz tomcat>/lib**;
   2. Edite seu conteúdo, no item ***FSRepoLoader.certFolder=*** coloque o valor **<raiz tomcat>/AcRepo;**

## Processo de configuração do Log

1. Copie o arquivo **logback..xml**;
   1. Copie esse arquivo para a pasta **<raiz tomcat>/lib**;
   2. Edite seu conteúdo, na linha

*<file>\*\* caminho do arquivo de logs\*\* </file>* coloque caminho do arquivo onde você quer gerar o log.

Ao final da instalação (com a aplicação rodando) acesse <http://localhost:8080/bluc/logView.html> e veja se o log está sendo gerado.

**Importante**: A configuração de log disponível está configurada para nível **debug:** *<root level="DEBUG">*

Antes de subir a aplicação para produção altere para *<root level="WARN">* para que não gere logs em excesso.

## Processo de instalação (clientes)

1. Esse passo é opcional para quem deseje utilizar os componentes e adequado apenas ao Windows:
   1. ActiveX;
   2. Rest Signer;
   3. Extensão do Chrome (componente Native Messaging);
2. No pacote **signer-distibution-master.zip** extraia o arquivo **blue\_crystal.zip**;
   1. Extraia o conteúdo desse arquivo para qualquer pasta local;
   2. Na pasta ‘DISK 1’ execute o arquivo **instalador.exe**;

## Processo de instalação (do servidor e do exemplo)

1. No pacote **signer-distibution-master.zip** extraia o arquivo **bluc.war** e **example.war**;

1. Copie esses arquivos para a pasta **<raiz tomcat>/webapps;**
2. Execute o Tomcat em **<raiz tomcat>/bin;**
3. No Windows use **startup.bat** e **startup.sh** no Linux e Mac OS X;

# Componentes cliente e sua compatibilidade

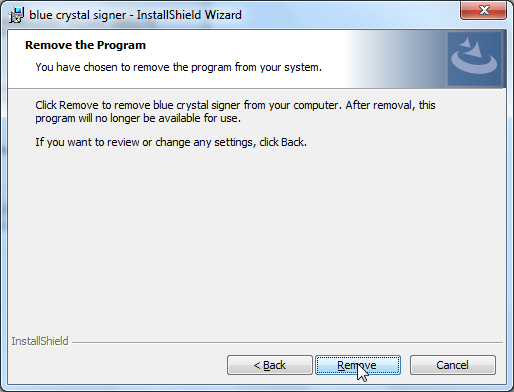
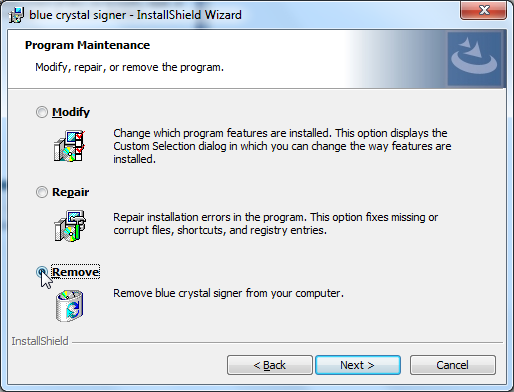
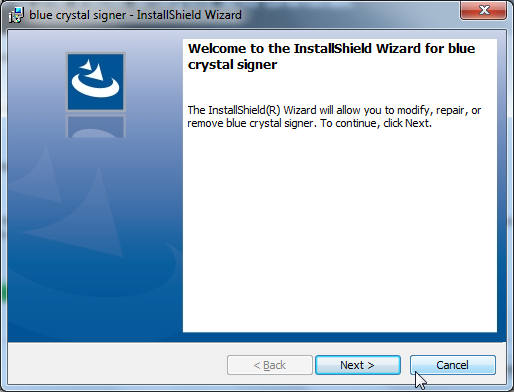
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Componente** | **Sistema**  **Operacional** | **Navegador** | **Exige instalação local** | **Obs.** |
| ActiveX | Windows | IE | Sim |  |
| Applet Java (MSCAPI) | Windows | IE, Firefox | Não |  |
| Applet Java (PKCS#11) | Windows, Linux, Mac OS X | IE, Firefox | Não |  |
| Rest Signer | Windows | Qualquer um | Sim | Java, Mac OS X e Linux em desenvolvimento |
| Extensão Chrome | Windows | Chrome | Sim | Java, Mac OS X e Linux em desenvolvimento |

## Desinstalação dos componentes Windows

## 

Selecione a opção “advanced”

Selecione o botão “Next”

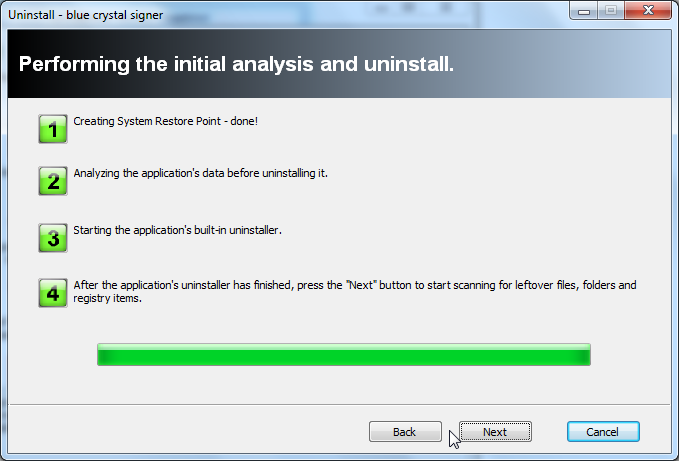
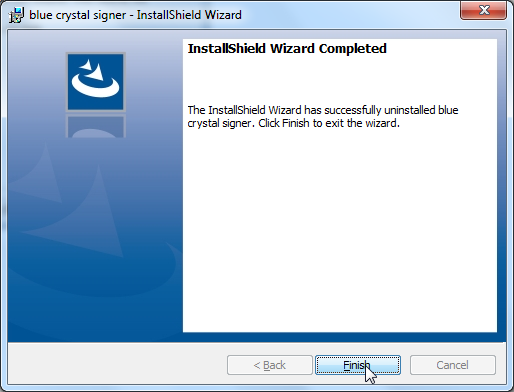


Selecione o botão “Remove”

Selecione o botão “Next”

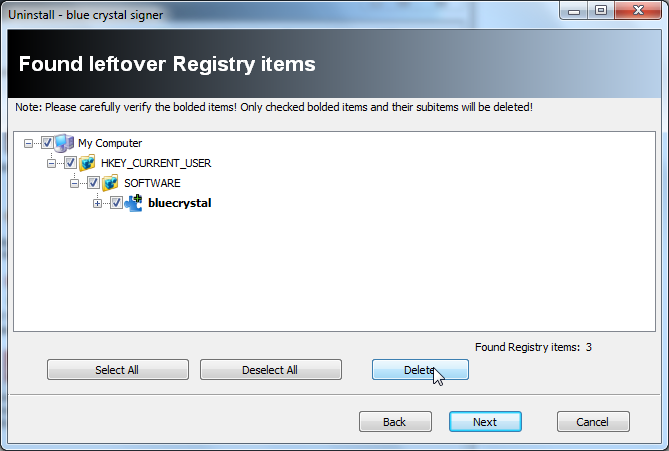
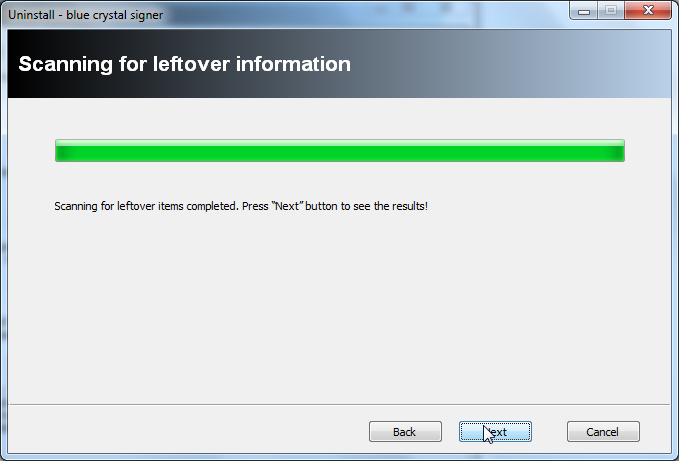
Selecione a opção “Remove”

Selecione o botão “Next”



Selecione o botão “Next”

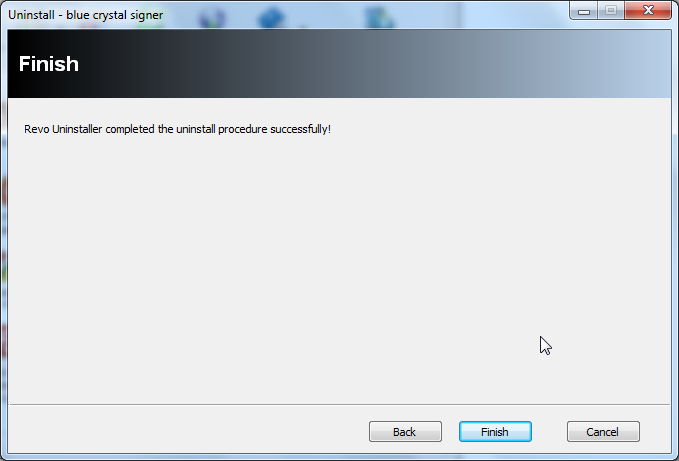
Selecione o botão “Finish”



Selecione o botão “Next”

Várias telas podem aparecer e em todas elas selecione “Delete All”

Selecione o botão “Next”



Caso apareçam novas telas selecione “Delete All” e siga até encontrar a tela final, e selecione “Finish”

## 

## Componente ActiveX

Utiliza a tecnologia da Microsoft, já considerada obsoleta, mas ainda muito utilizada;

Pode ser usado para substituir facilmente o CAPICOM;

Exige instalação local do compente;

Pode ser utilizado no IE ou aplicativos Desktop Windows (como Delphi, ou VB.NET) no Windows;

## Componente Apple Java

Utiliza a tecnologia Java Applet, já considerada obsoleta, mas ainda muito utilizada;

Exige a instalação do JDK 8;

**Não** exige instalação local;

A versão MS-CAPI pode ser utilizado no IE ou Firefox no Windows;

A versão PKCS#11 pode ser utilizado no IE ou Firefox em múltiplos sistemas operacionais;

## Componente Rest Signer

Aplicativo que roda na *tray* (atualmente no Windows apenas) e recebe chamadas como um ‘micro-servidor web’;

Exige instalação local;

Baseado em MS-CAPI pode ser utilizado em qualquer navegador ou aplicativo desktop no Windows;

Em desenvolvimento novas versões: Java, Mac OS X (nativo) e Linux (nativo)

## Componente Extensão Chrome

Extensão desenvolvida para o Chrome;

Exige instalação local;

Baseado em MS-CAPI pode ser utilizado em qualquer navegador ou aplicativo desktop no Windows;

Em desenvolvimento novas versões: Java, Mac OS X (nativo) e Linux (nativo);

Disponivel para instalação da Chrome Web Store

(<https://chrome.google.com/webstore/detail/blue-crystalsigner/inlgdajmhicinhamnepnpdneamfgjcgl?hl=pt-BR&authuser=2>)

 Caso você já tenha rodado o instalador Windows e deseje apenas atualizar os arquivos, sem passar por todo o processo. Baixe os arquivos da pasta “Windows arquivos”, e substitua em “C:\Program Files (x86)\blue crystal”.

 Lembre-se de abrir o Windows Explorer como Administrador, ou o Windows bloqueará a cópia.

# Utilizando a aplicação

Como utilizar a aplicação exemplo com cada um dos componentes cliente

## Utilizando o activeX

Como utilizar a aplicação exemplo com o componente ActiveX

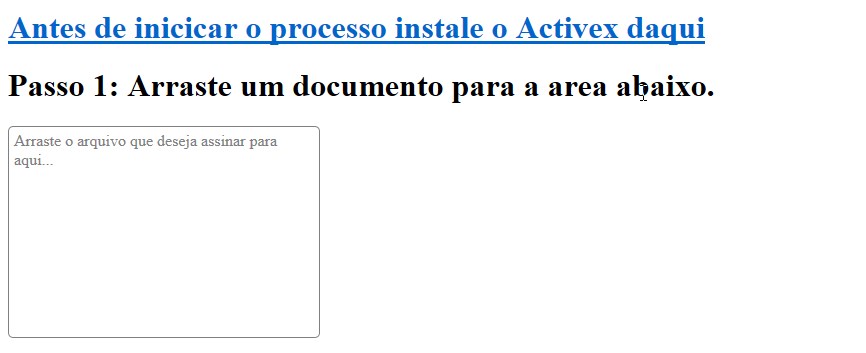
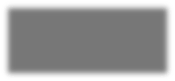
### Requisitos

1. Esse componente exige a plataforma
   1. Navegador: Internet Explorer
   2. Sistema Operacional: Windows
2. Caso ainda não tenha instalado os componentes cliente, deve fazêlo antes de continuar o processo. (ver pagina 10)

### Acessando a pagina

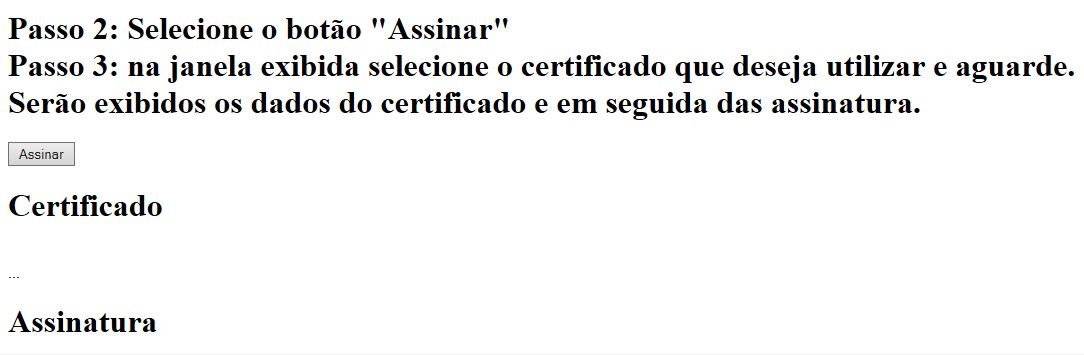
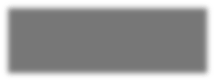
1. Acesse a página <http://localhost:8080/example/>
   1. Caso você esteja usando o IE e tenha o ActiveX instalado você permanecerá nessa página
   2. Caso contrário será redirecionado para outra página com outro componente cliente;
2. Na pagina vista no próximo slide comece fazendo o drag and drop de um arquivo;

### Upload do conteúdo



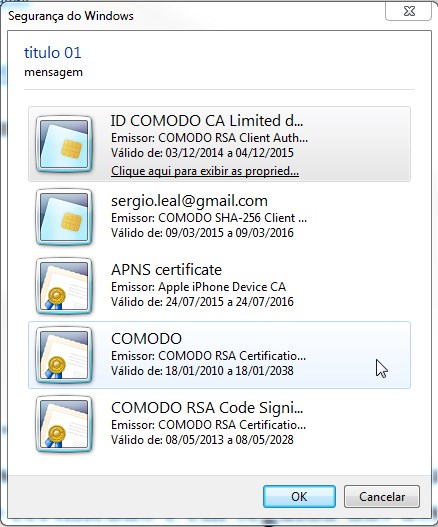
Arraste e solte um arquivo nessa área

### Inicie a assinatura



Selecione ‘Assinar’

### Escolha o certificado



Lista de

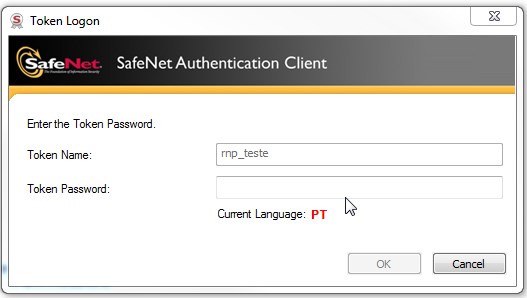
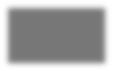
certificados para

assinatura



Selecione um certificado da lista

### Digite a senha



Digite o PIN de proteção do seu

certificado

OBS: Essa tela poderá ser diferente dependendo da marca e modelo do seu token ou smart card

### O sistema exibe o resultado



Ao final informações retiradas do

certificado serão exibidas...



... E em baixo a assinatura feita

## Utilizando o Applet Java CAPI

Como utilizar a aplicação exemplo com o componente Applet Java CAPI

### Requisitos

1. Esse componente exige a plataforma
   1. Navegador: Internet Explorer, ou Firefox
   2. Sistema Operacional: Windows
2. É necessário instalar o JDK 8

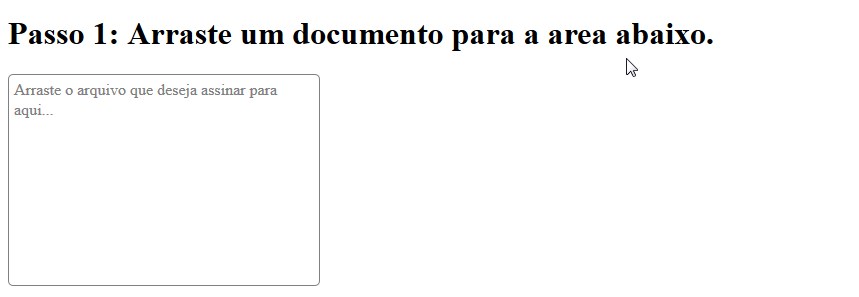
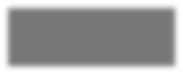
[(http://www.oracle.com/technetwork/pt/java/javase/downloads/jdk8-downloads-](http://www.oracle.com/technetwork/pt/java/javase/downloads/jdk8-downloads-2133151.html)

[2133151.html);](http://www.oracle.com/technetwork/pt/java/javase/downloads/jdk8-downloads-2133151.html)

### Acessando a pagina

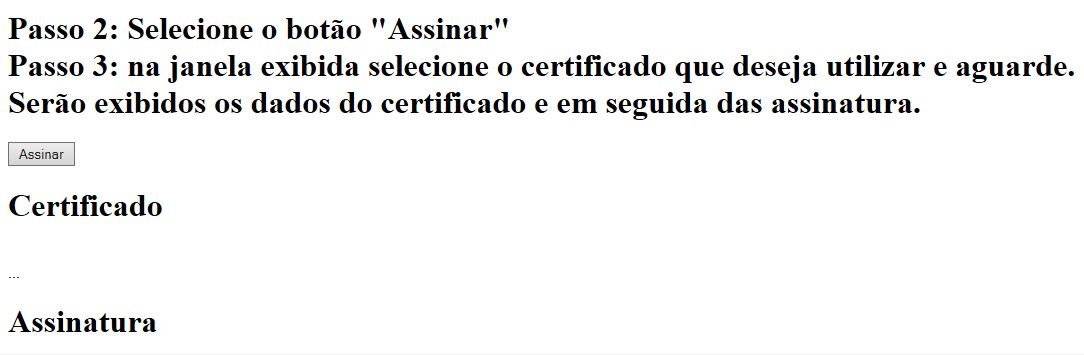
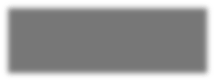
1. Acesse a página <http://localhost:8080/example/upload_java_capi.html>
   1. Caso você esteja usando o Windows você permanecerá nessa página
   2. Caso contrário será redirecionado para outra página com outro componente cliente;
   3. É possível que o sistema questione se você deseja confiar no componente, responda que “Sim”.
2. Na pagina vista no próximo slide comece fazendo o drag and drop de um arquivo;

### Upload do conteúdo



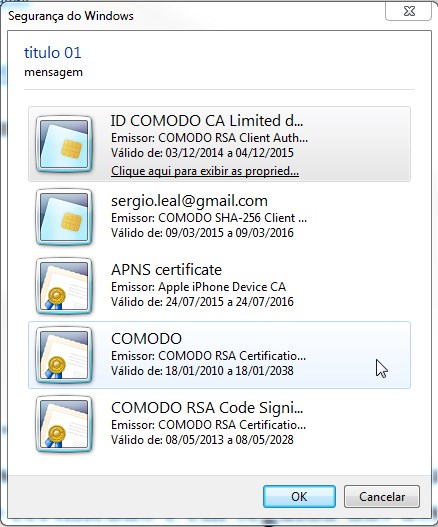
Arraste e solte um arquivo nessa área

### Inicie a assinatura



Selecione ‘Assinar’

### Escolha o certificado



Lista de

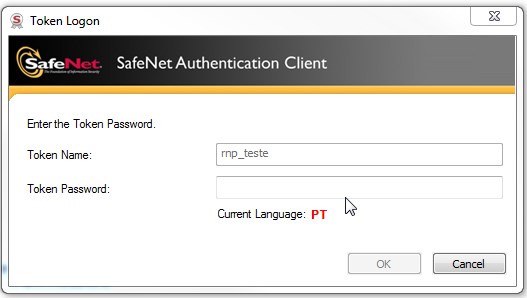
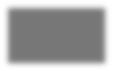
certificados para

assinatura



Selecione um certificado da lista

### Digite a senha



Digite o PIN de proteção do seu

certificado

OBS: Essa tela poderá ser diferente dependendo da marca e modelo do seu token ou smart card

### O sistema exibe o resultado



Ao final informações retiradas do

certificado serão exibidas...



... E em baixo a assinatura feita

## Utilizando o Applet Java PKCS#11

Como utilizar a aplicação exemplo com o componente Applet Java PKCS#11

### Requisitos

1. Esse componente exige a plataforma
   1. Navegador: Internet Explorer, ou Firefox
   2. Sistema Operacional: Windows, Mac OS x, Linux
2. É necessário instalar o JDK 8

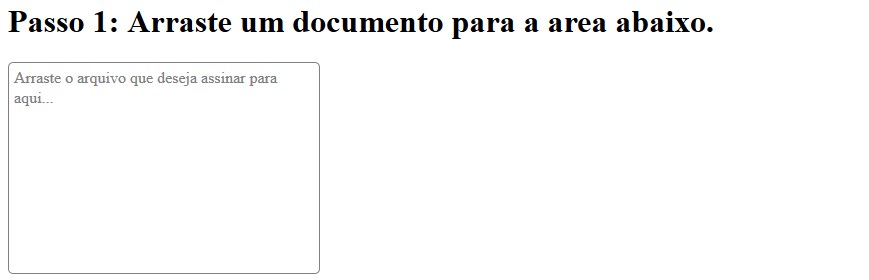
[(http://www.oracle.com/technetwork/pt/java/javase/downloads/jdk8-downloads2133151.html);](http://www.oracle.com/technetwork/pt/java/javase/downloads/jdk8-downloads-2133151.html)

1. É necessário instalar o driver PKCS#11 do seu token / cartão;

### Acessando a pagina

1. Acesse a página <http://localhost:8080/example/upload_java_capi.html>
   1. Caso você esteja usando o Windows você permanecerá nessa página
   2. Caso contrário será redirecionado para outra página com outro componente cliente;
   3. É possível que o sistema questione se você deseja confiar no componente, responda que “Sim”.
2. Na pagina vista no próximo slide comece fazendo o drag and drop de um arquivo;

### Upload do conteúdo

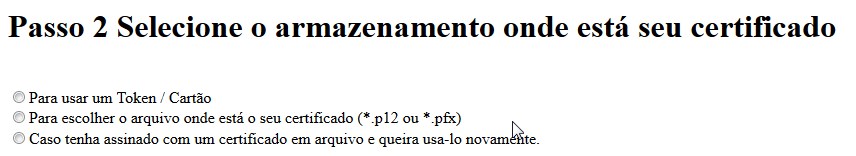


Arraste e solte um arquivo nessa área

## Selecione o mecanismo



Selecione ‘Assinar’

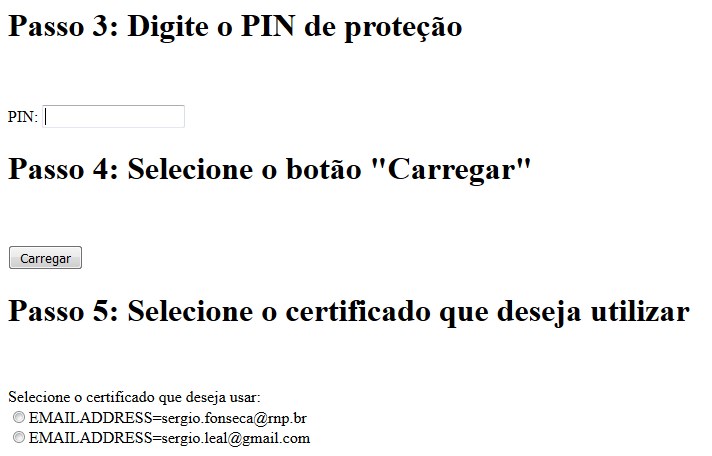


Selecione o tipo de armazenamento do seu certificado: Token ou cartão; Arquivo:

Na segunda opção o sistema perguntará o caminho que você deseja usar;

Na terceira opção o sistema utilizará o mesmo certificado do passo anterior;

### Escolha o certificado



Digite o PIN do certificado



Selecione ‘Carregar’

Lista de

certificados

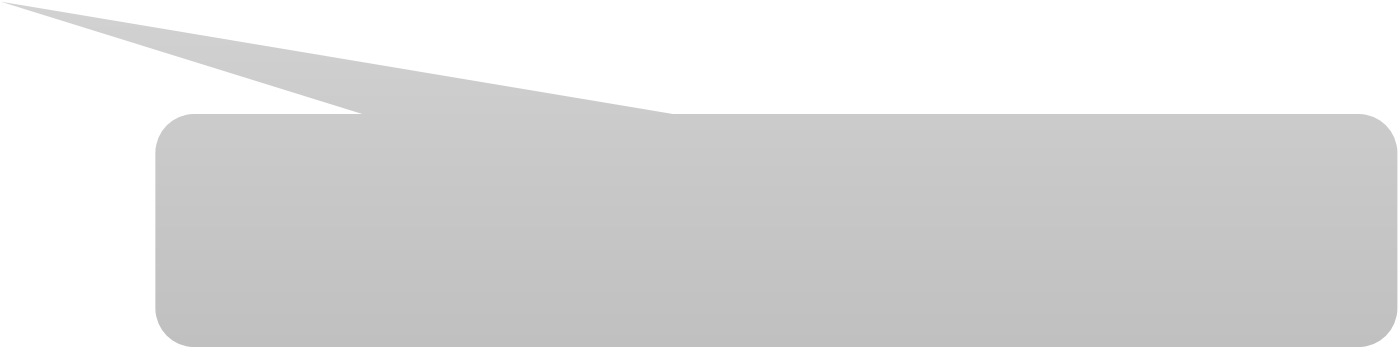
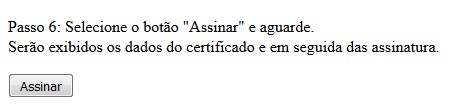
para

assinatura



Escolha o certificado pelo “DN”

### Inicie a assinatura



Selecione ‘Assinar’

### O sistema exibe o resultado



Ao final informações retiradas do

certificado serão exibidas...



... E em baixo a assinatura feita

## Utilizando o Rest Signer

Como utilizar a aplicação exemplo com o componente Rest Signer

### Requisitos

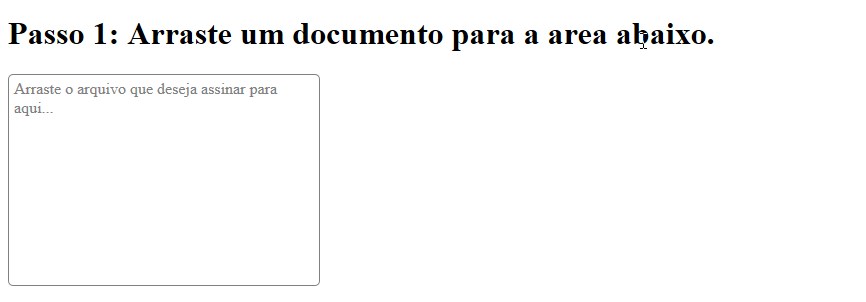
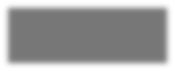
1. Esse componente exige a plataforma
   1. Navegador: Qualquer um
   2. Sistema Operacional: Windows
2. Caso ainda não tenha instalado os componentes cliente, deve fazêlo antes de continuar o processo. (ver pagina 10);
3. Certifique-se que o Rest Signer esteja em execução na tray do Windows, com o ícone:



### Acessando a pagina

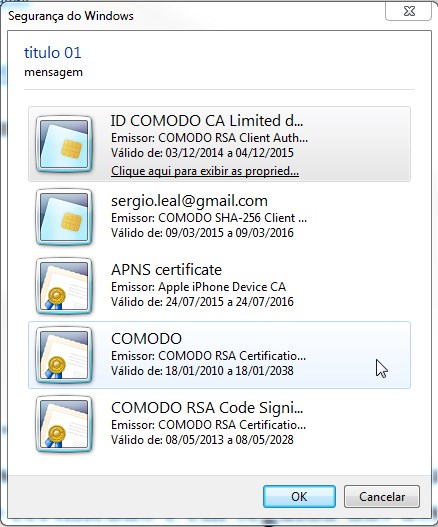
1. Acesse a página <http://localhost:8080/example/upload_RestSigner.html>
2. Na pagina vista no próximo slide comece fazendo o drag and drop de um arquivo;

### Upload do conteúdo



Arraste e solte um arquivo nessa área

### Escolha o certificado



Lista de

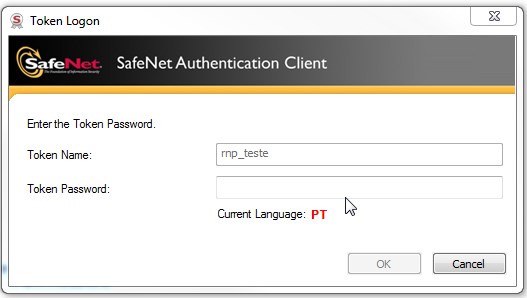
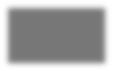
certificados para

assinatura



Selecione um certificado da lista

### Digite a senha



Digite o PIN de proteção do seu

certificado

OBS: Essa tela poderá ser diferente dependendo da marca e modelo do seu token ou smart card

### O sistema exibe o resultado



Ao final informações retiradas do

certificado serão exibidas...



... E em baixo a assinatura feita

## Utilizando a extensão para o Chrome

Como utilizar a aplicação exemplo com a extensão pra o Chrome

### Requisitos

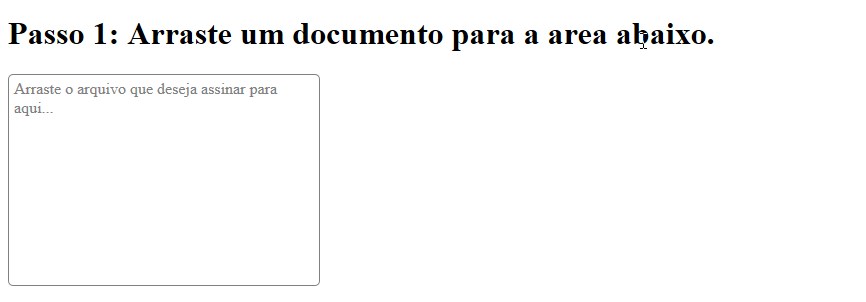
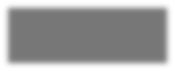
1. Esse componente exige a plataforma
   1. Navegador: Chrome
   2. Sistema Operacional: Windows
2. Caso ainda não tenha instalado os componentes cliente, deve fazêlo antes de continuar o processo. (ver pagina 10);

### Acessando a pagina

1. Acesse a página <http://localhost:8080/example/upload_ChromeExt.html>
2. Na pagina vista no próximo slide comece fazendo o drag and drop de um arquivo;
3. Certifique-se que a extensão esteja funcional pelo ícone na barra de endereços:



### Upload do conteúdo



Arraste e solte um arquivo nessa área

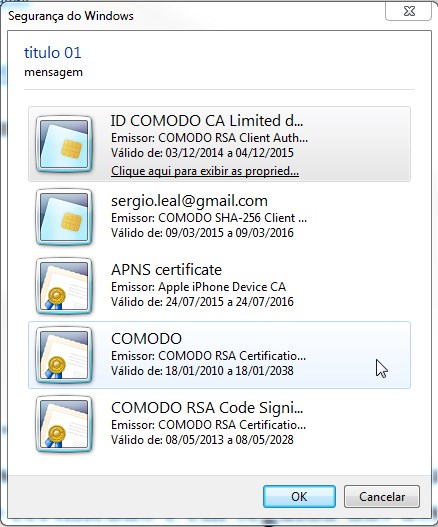


Clique no ícone



Clique no botão ‘Assinar’

### Escolha o certificado



Lista de

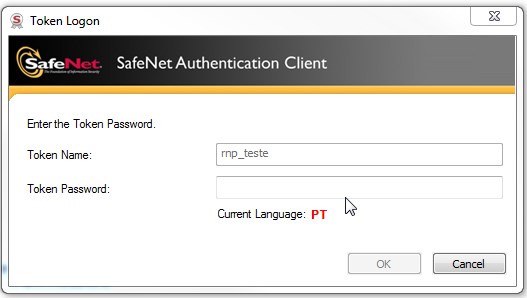
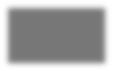
certificados para

assinatura



Selecione um certificado da lista

### Digite a senha



Digite o PIN de proteção do seu

certificado

OBS: Essa tela poderá ser diferente dependendo da marca e modelo do seu token ou smart card

### O sistema exibe o resultado



Ao final informações retiradas do

certificado serão exibidas...



... E em baixo a assinatura feita