

# **Manual de Instalação**

Procedimento para instalação em diversos cenários

## Sumário

Manual de Instalação.....	1
Sumário .....	2
O que é? .....	5
Criando um certificado de testes.....	6
Processo de instalação do Servidor (Vagrant e Virtual Box) .....	12
Processo de instalação do Servidor (JDK e Tomcat) .....	14
Download dos Componentes para instalação .....	14
Processo de instalação das ACs Confiáveis .....	16
Processo de configuração do Log.....	17
Processo de instalação (clientes) .....	18
Processo de instalação (do servidor e do exemplo) .....	19
Componentes cliente e sua compatibilidade .....	20
Desinstalação dos componentes Windows .....	22
Componente ActiveX.....	27
Componente Apple Java .....	28
Componente Rest Signer.....	29
Componente Extensão Chrome .....	30
Utilizando a aplicação .....	32
Utilizando o activeX.....	33

Requisitos.....	33
Acessando a pagina.....	33
Upload do conteúdo .....	34
Inicie a assinatura .....	35
Escolha o certificado .....	36
Digite a senha.....	37
O sistema exibe o resultado .....	38
Utilizando o Applet Java CAPI .....	39
Requisitos.....	39
Acessando a pagina.....	39
Upload do conteúdo .....	40
Inicie a assinatura .....	41
Escolha o certificado .....	42
Digite a senha.....	43
O sistema exibe o resultado .....	44
Utilizando o Applet Java PKCS#11.....	45
Requisitos.....	45
Acessando a pagina.....	46
Upload do conteúdo .....	47
Selecione o mecanismo.....	48
Escolha o certificado .....	49
Inicie a assinatura .....	50
O sistema exibe o resultado .....	51

Utilizando o Rest Signer .....	52
Requisitos.....	52
Acessando a pagina.....	52
Upload do conteúdo .....	53
Escolha o certificado .....	54
Digite a senha.....	55
O sistema exibe o resultado .....	56
Utilizando a extensão para o Chrome.....	57
Requisitos.....	57
Acessando a pagina.....	57
Upload do conteúdo .....	59
Escolha o certificado .....	60
Digite a senha.....	61
O sistema exibe o resultado .....	62

## 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.

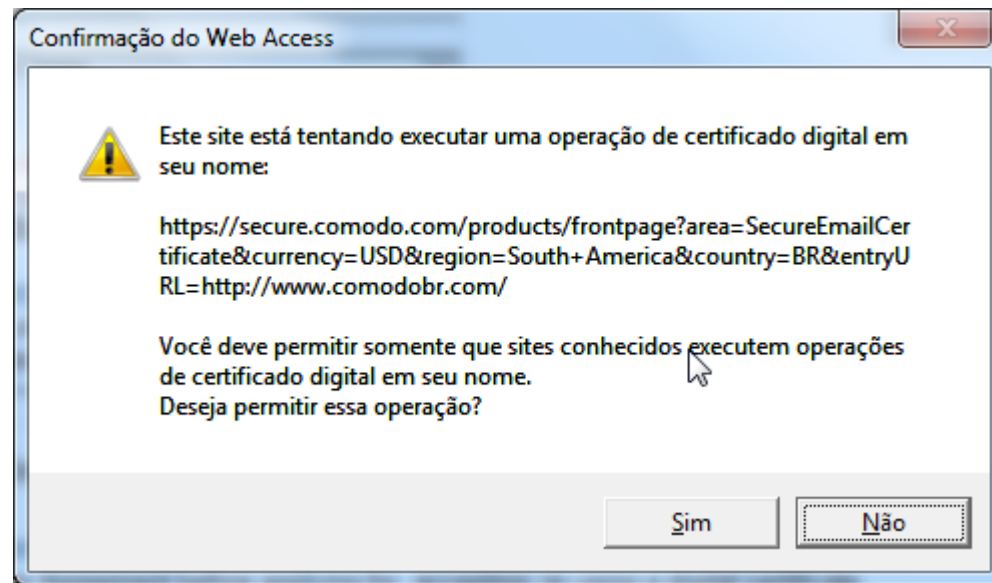
# **Criando um certificado de testes**

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



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

## Application for Secure Email Certificate

### Your Details

First Name	<input type="text"/>
Last Name	<input type="text"/>
Email Address	<input type="text"/>
Country	<input type="text" value="United States"/> ▼

[Advanced Private Key Options...](#)

É importante selecionar:

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



### Application for Secure Email Certificate

**Your Details**

First Name

Last Name

Email Address

Country

**Advanced Private Key Options** [Use Default Settings](#)

CSP

Key Size

Exportable? ☒

User protected? ☐

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;

## Application for Secure Email Certificate

**Your Details**

First Name

Last Name

Email Address

Country

**Advanced Private Key Settings**

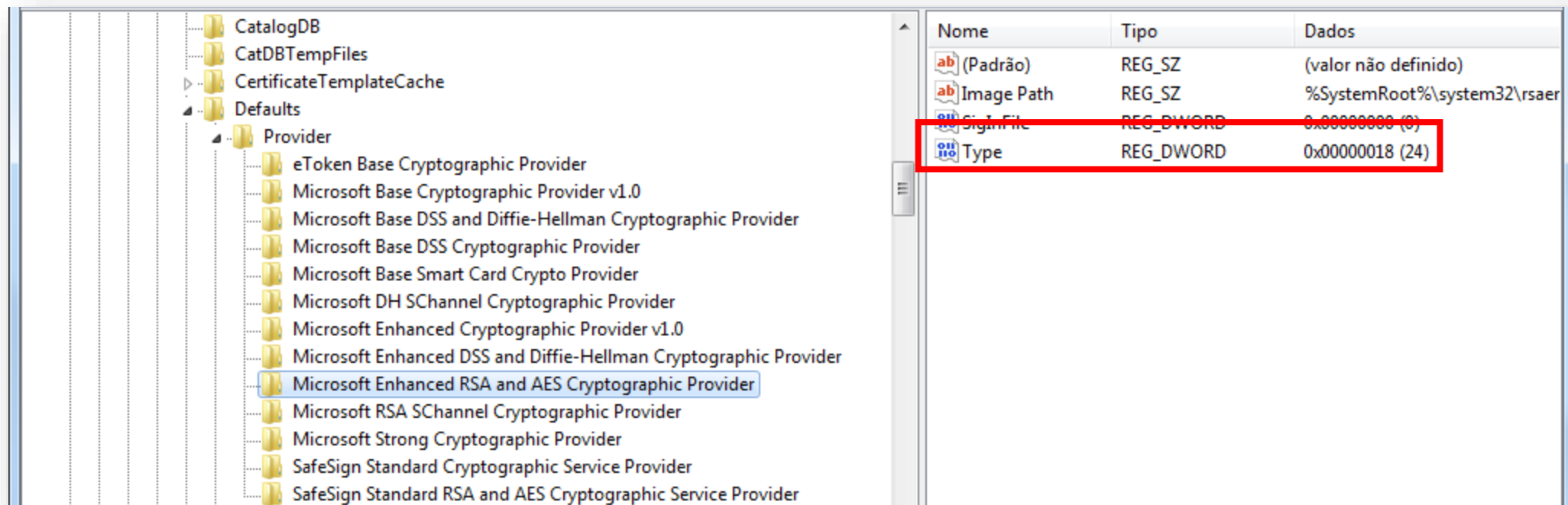
CSP

Key Size

Exportable? ☒

User protected? ☐

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.

4. Faça a instalação do Virtual Box (<https://www.virtualbox.org/>);
5. Faça a instalação do Vagrant (<https://www.vagrantup.com/>);
6. Em seguida copie para sua máquina o arquivo “Vagrantfile” do repositório:
  - Para subir um servidor baseado no Ubuntu 14.04 (<https://github.com/bluecrystalsign/signer-deploy/tree/master/vagrant/ubuntu14.04-tomcat8>);

- . Para subir um servidor baseado no CentOS 7.2 (<https://github.com/bluecrystalsign/signer-deploy/tree/master/vagrant/centos7.2-tomcat8>);

7. Abra o “command” do Windows (executando o programa “cmd”) ou o “shell” do Linux ou MacOS;
8. Mude para o diretório onde colocou o arquivo do passo 5;
9. Execute o comando:
  - *vagrant up*
10. Quando terminar a execução (aparecer novamente o prompt) teste o funcionamento com: <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>);
3. Baixe e descompacte o Tomcat 8 Core (<https://tomcat.apache.org/download-80.cgi>);
4. Chamaremos a pasta raiz do Tomcat de <raiz tomcat>;

## Download dos Componentes para instalação

Utilize o repositório disponível em:

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

# Processo de instalação das ACs Confiáveis

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



# Processo de configuração do Log

1. Copie o arquivo logback.xml;

a) Copie esse arquivo para a pasta <raiz tomcat>/lib;

b) 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:
  - a) ActiveX;
  - b) Rest Signer;
  - c) Extensão do Chrome (componente Native Messaging);
2. No pacote signer-distribution-master.zip extraia o arquivo blue\_crystal.zip;
  - a) Extraia o conteúdo desse arquivo para qualquer pasta local;
  - b) Na pasta 'DISK 1' execute o arquivo instalador.exe;

# Processo de instalação (do servidor e do exemplo)

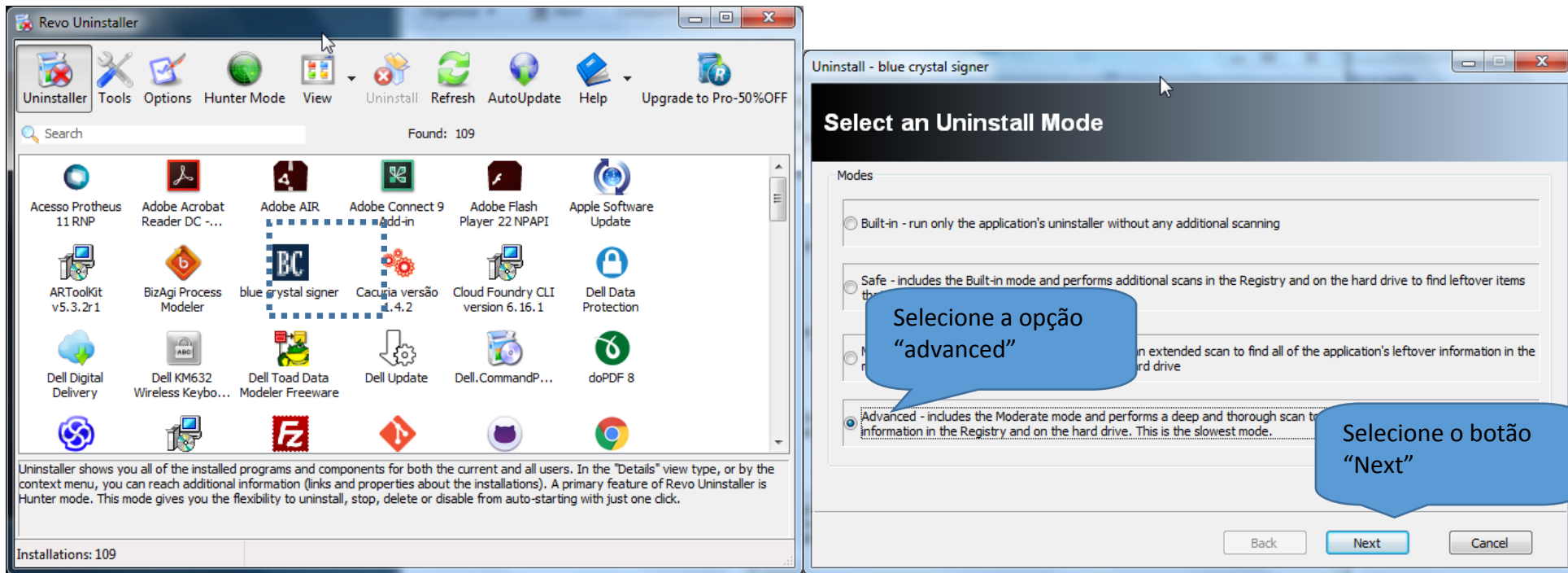
1. No pacote signer-distribution-master.zip extraia o arquivo bluc.war e example.war;
  - a) Copie esses arquivos para a pasta <raiz tomcat>/webapps;
  - b) Execute o Tomcat em <raiz tomcat>/bin;
  - c) No Windows use startup.bat e startup.sh no Linux e Mac OS X;

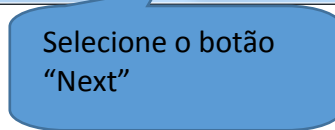
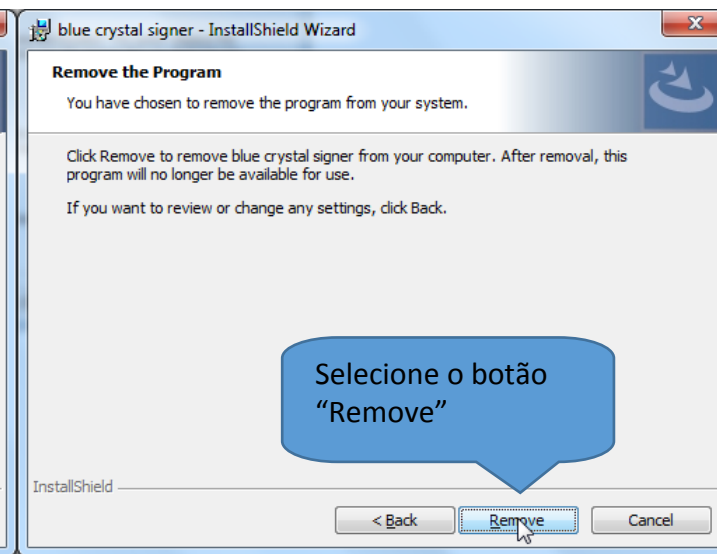
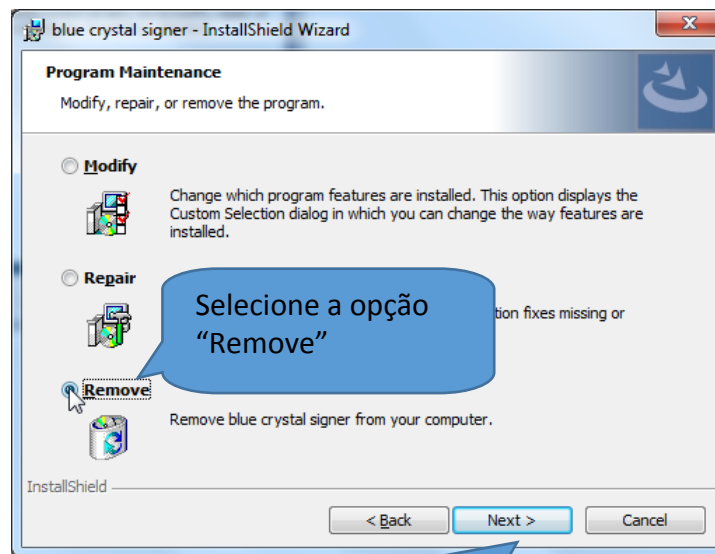
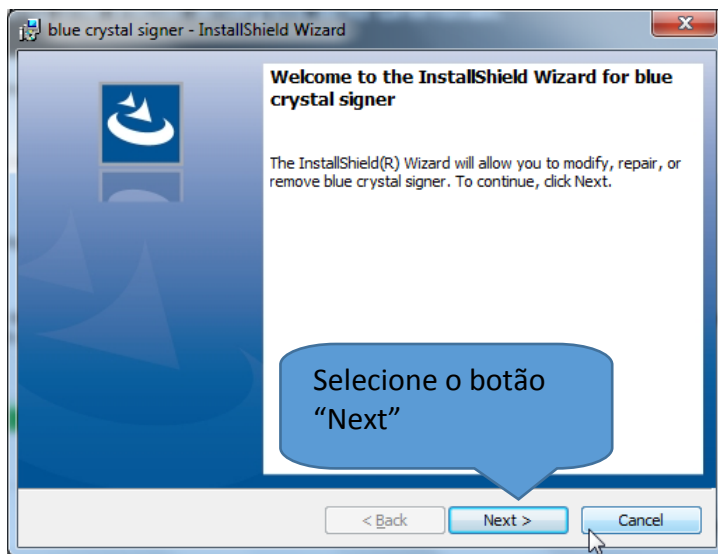
# Componentes cliente e sua compatibilidade

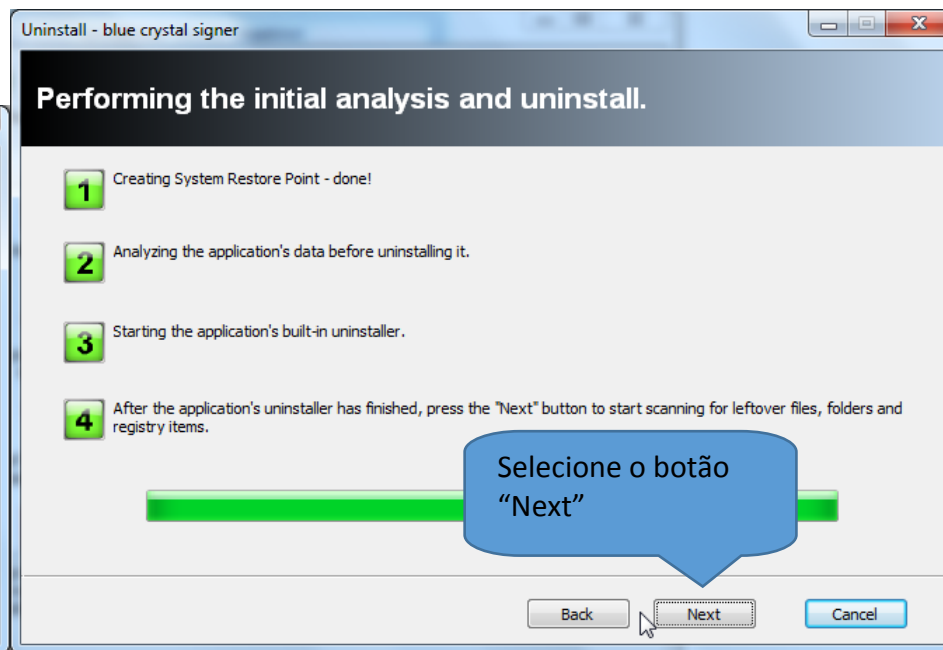
Componente	Sistema Operacional	Navegador	Exige instalação local	Obs.
ActiveX	Windows	IE	Sim	
Applet Java (MSCAPI)	Windows	IE, Firefox	Não	
Applet Java (PKCS#11)	Windows, Linux, Mac OS X	IE, Firefox	Não	
Rest Signer	Windows	Qualquer um	Sim	Java, Mac OS X e Linux em desenvolvimento
Extensão Chrome	Windows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



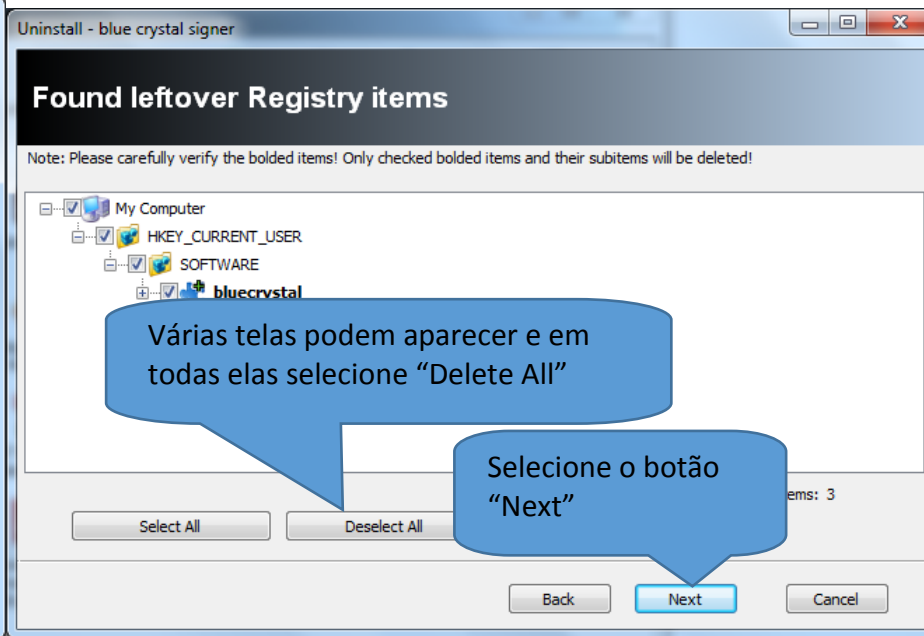
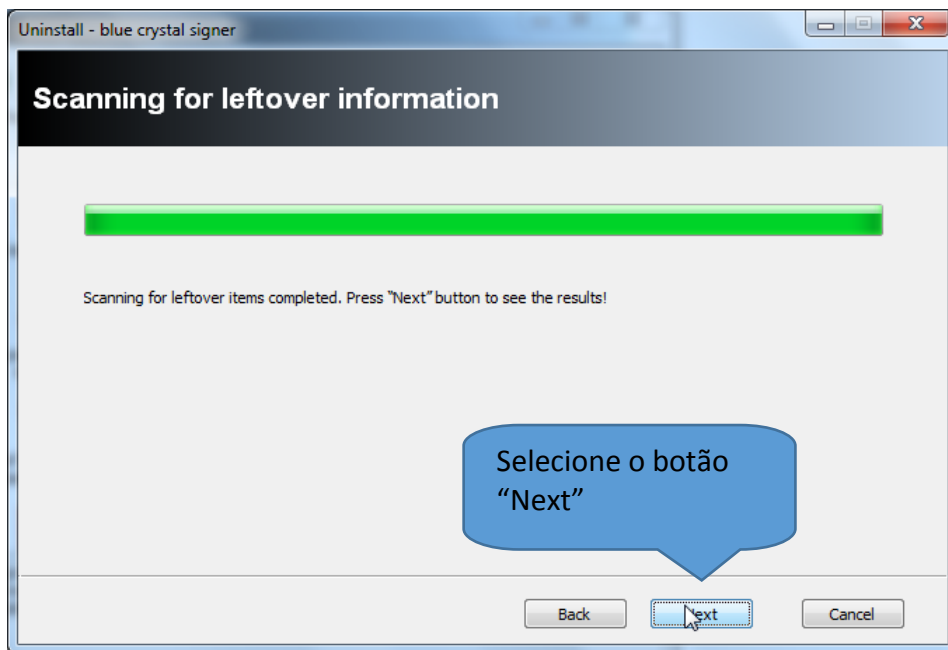
# Desinstalação dos componentes Windows

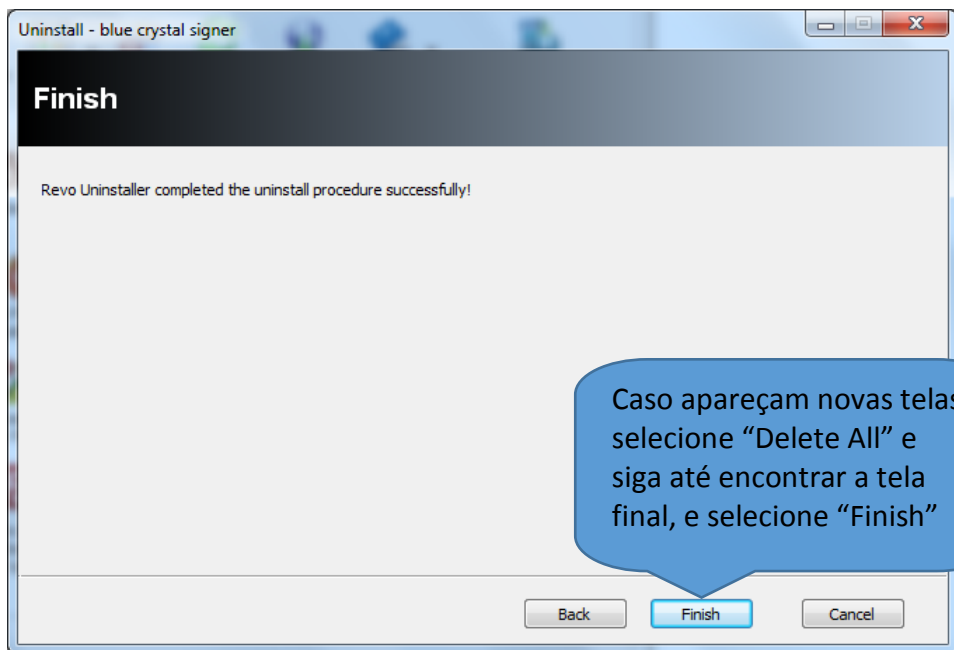












# Componente ActiveX

- ✓ Utiliza a tecnologia da Microsoft, já considerada obsoleta, mas ainda muito utilizada;
- ✓ Pode ser usado para substituir facilmente o CAPICOM;
- ✓ Exige instalação local do componente;
- ✓ 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);
- ✓ Disponível para instalação da Chrome Web Store  
(<https://chrome.google.com/webstore/detail/blue-crystalsigner/inlgdajmhicinhamnepnpdneamfgjcg?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

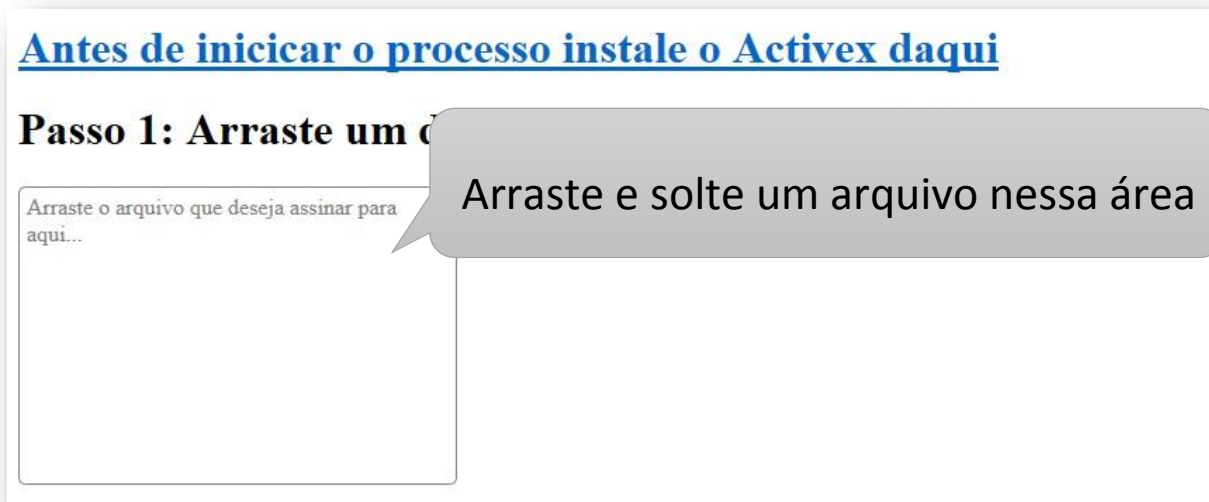
1. Esse componente exige a plataforma
  - a) Navegador: Internet Explorer
  - b) Sistema Operacional: Windows
2. Caso ainda não tenha instalado os componentes cliente, deve fazê-lo antes de continuar o processo. (ver pagina 10)

## 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



## Inicie a assinatura

**Passo 2: Selecione o botão "Assinar"**

**Passo 3:** Selecione o certificado que deseja utilizar e aguarde.

**Serão exibidos os certificados disponíveis para assinatura.**

Selecione 'Assinar'

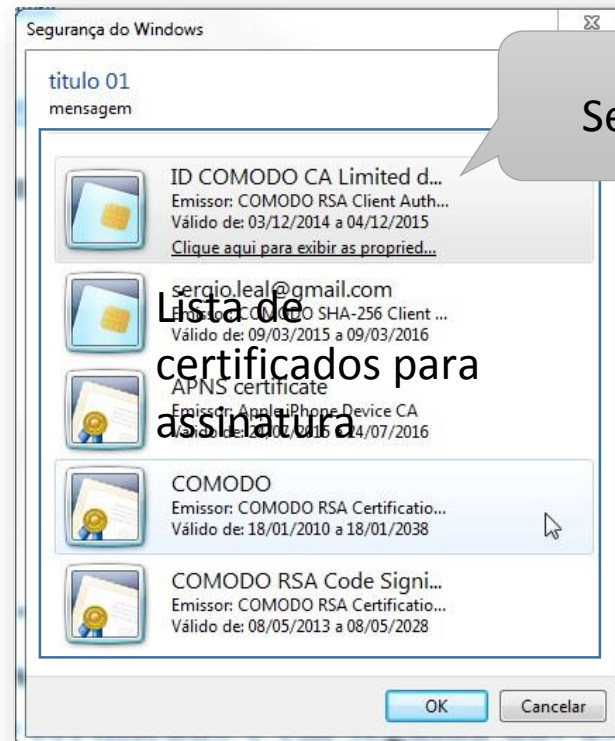
Assinar

**Certificado**

...

**Assinatura**

## Escolha o certificado



Selecione um certificado da lista

Lista de  
certificados para  
assinatura

Digite a senha



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

## O sistema exibe o resultado

### Certificado

Nome	Valor
issuer0	CN=COMODO SHA-256 Client Authentication and Secure Email CA, O=COMODO CA Limited, I
serial0	239978131432459574058407871863249784083
subject0	EMAILADDRESS=sergio.leal@gmail.com
ku0	digitalSignature,keyEncipherment
cert_type0	standard
eku0	ekuEmailProt
crlDP0	http://crl.comodoca.com/COMODOSHA256ClientAuthenticationandSecureEmailCA.crl
certPolOid0	1.3.6.1.4.1.6449.1.2.1.1.1
basicConstraint0	-1
ocsp0	http://ocsp.comodoca.com
version0	3
notBefore0	1425945600000
san_email0	sergio.leal@gmail.com
certPolQualifier0	https://secure.comodo.net/CPS
chain0	http://crt.comodoca.com/COMODOSHA256ClientAuthenticationandSecureEmailCA.crt
key_length0	2048
notAfter0	1457567999000
aki0	92616B82E1A2A0AA4FEC67F1C2A3F7B48000C1EC
certSha2560	B060451E4DB83F95E99A70E99887D79A0450DE4001E140FFED31A2D863317600D

Ao final informações retiradas do certificado serão exibidas...

### Assinatura

... E em baixo a assinatura feita

MIJWQYJKoZIhvcNAQcCoIIJSjCCCUYCAQExDzANBgIghkgBZQMEAgEFADALBgkqhkiG9w0BBwGgggVGMIIFQjCCBCqgAwIBAgIRALSKG1/rwOUqIITzg3VJTRMwDQYJKoZIhvc

# Utilizando o Applet Java CAPI

Como utilizar a aplicação exemplo com o componente Applet Java CAPI

## Requisitos

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

**Passo 1: Arraste um documento para a area abaixo.**

Arraste o arquivo que deseja assinar para aqui...

Arraste e solte um arquivo nessa área



## Inicie a assinatura

**Passo 2: Selecione o botão "Assinar"**

**Passo 3:** Selecione o certificado que deseja utilizar e aguarde.

**Serão exibidos os certificados disponíveis para assinatura.**

Selecione 'Assinar'

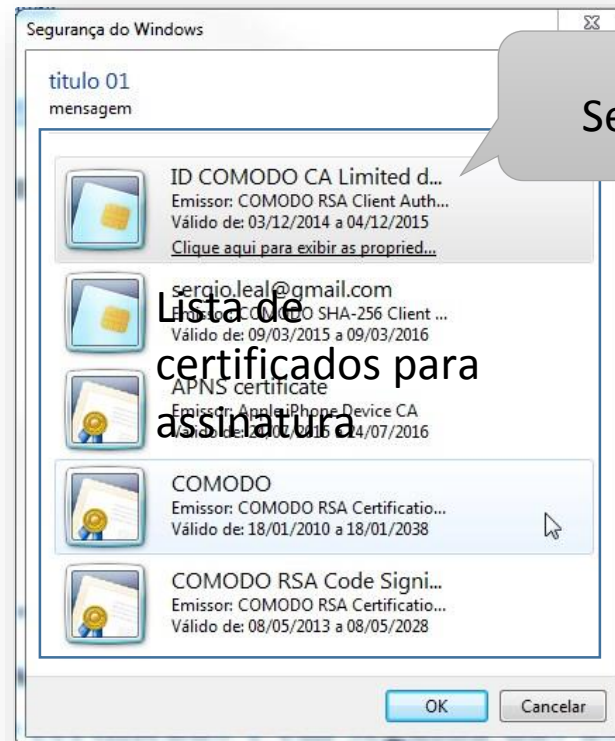
Assinar

**Certificado**

...

**Assinatura**

## Escolha o certificado



Selecione um certificado da lista

Lista de  
certificados para  
assinatura

Digite a senha



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

## O sistema exibe o resultado

### Certificado

Nome	Valor
issuer0	CN=COMODO SHA-256 Client Authentication and Secure Email CA, O=COMODO CA Limited, I
serial0	239978131432459574058407871863249784083
subject0	EMAILADDRESS=sergio.leal@gmail.com
ku0	digitalSignature,keyEncipherment
cert_type0	standard
eku0	ekuEmailProt
crlDP0	http://crl.comodoca.com/COMODOSHA256ClientAuthenticationandSecureEmailCA.crl
certPolOid0	1.3.6.1.4.1.6449.1.2.1.1.1
basicConstraint0	-1
ocsp0	http://ocsp.comodoca.com
version0	3
notBefore0	1425945600000
san_email0	sergio.leal@gmail.com
certPolQualifier0	https://secure.comodo.net/CPS
chain0	http://crt.comodoca.com/COMODOSHA256ClientAuthenticationandSecureEmailCA.crt
key_length0	2048
notAfter0	1457567999000
aki0	92616B82E1A2A0AA4FEC67F1C2A3F7B48000C1EC
certSha2560	B060451E4DB83F95E99A70E99887D79A0450DE4001E140FEFE31A2D863317600D

Ao final informações retiradas do certificado serão exibidas...

### Assinatura

... E em baixo a assinatura feita

MIJWQYJKoZIhvcNAQcCoIISjCCCCUYCAQExDzANBgkqhkiG9w0BBwGgggVGMIIFQjCCBCqgAwIBAgIRALSKG1/rwOUqIITzg3VJTRMwDQYJKoZIhvc

# 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
  - a) Navegador: Internet Explorer, ou Firefox
  - b) 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>);
3. 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](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

### **Passo 1: Arraste um documento para a area abaixo.**

Arraste o arquivo que deseja assinar para aqui...

Arraste e solte um arquivo nessa área

# Selecione o mecanismo

## **Passo 2 Selecione o armazenamento onde está seu certificado**

- ☐ Para usar um Token / Cartão
- ☐ Para escolher o arquivo onde está o seu certificado (\*.p12 ou \*.pfx)
- ☐ Caso tenha assinado com um certificado em arquivo e queira usa-lo novamente.

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

### Passo 3: Digite o PIN de proteção

PIN: |

Digite o PIN do certificado

### Passo 4: Selecione o botão "Carregar"

Carregar

Selecione 'Carregar'

### Passo 5: Selecione o certificado que deseja utilizar

Selecione o certificado que deseja usar:

- ☐ EMAILADDRESS=sergio.fonseca@rnp.br
- ☐ EMAILADDRESS=sergio.leal@gmail.com

Escolha o certificado pelo "DN"

Lista de certificados para  
assinatura

## Inicie a assinatura

Passo 6: Selecione o botão "Assinar" e aguarde.  
Serão exibidos os dados do certificado e em seguida das assinatura.

Assinar

Selecione 'Assinar'

## O sistema exibe o resultado

### Certificado

Nome	Valor
issuer0	CN=COMODO SHA-256 Client Authentication and Secure Email CA, O=COMODO CA Limited, I
serial0	239978131432459574058407871863249784083
subject0	EMAILADDRESS=sergio.leal@gmail.com
ku0	digitalSignature,keyEncipherment
cert_type0	standard
eku0	ekuEmailProt
crlDP0	http://crl.comodoca.com/COMODOSHA256ClientAuthenticationandSecureEmailCA.crl
certPolOid0	1.3.6.1.4.1.6449.1.2.1.1.1
basicConstraint0	-1
ocsp0	http://ocsp.comodoca.com
version0	3
notBefore0	1425945600000
san_email0	sergio.leal@gmail.com
certPolQualifier0	https://secure.comodo.net/CPS
chain0	http://crt.comodoca.com/COMODOSHA256ClientAuthenticationandSecureEmailCA.crt
key_length0	2048
notAfter0	1457567999000
aki0	92616B82E1A2A0AA4FEC67F1C2A3F7B48000C1EC
certSha2560	B060451E4DB83F95E99A70E99887D79A0450DE4001E140FEFE31A2D863317600D

Ao final informações retiradas do certificado serão exibidas...

### Assinatura


... E em baixo a assinatura feita

MIlJWQYJKoZIhvcNAQcCoIIJSjCCCUYCAQExDzANBgkqhkiG9w0BBwGgggVGMIIIFQjCCBCqgAwIBAgIRALSKG1/rwOUqIITzg3VJTRMwDQYJKoZIhvc

# Utilizando o Rest Signer

Como utilizar a aplicação exemplo com o componente Rest Signer

## Requisitos

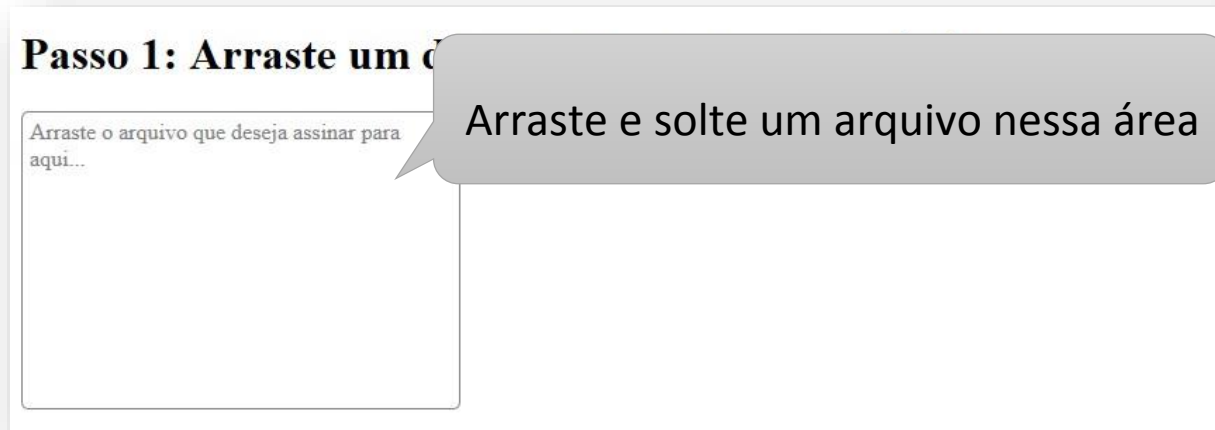
1. Esse componente exige a plataforma
  - a) Navegador: Qualquer um
  - b) Sistema Operacional: Windows
2. Caso ainda não tenha instalado os componentes cliente, deve fazê-lo antes de continuar o processo. (ver pagina 10);
3. Certifique-se que o Rest Signer esteja em execução na tray do Windows, com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

## Acessando a pagina

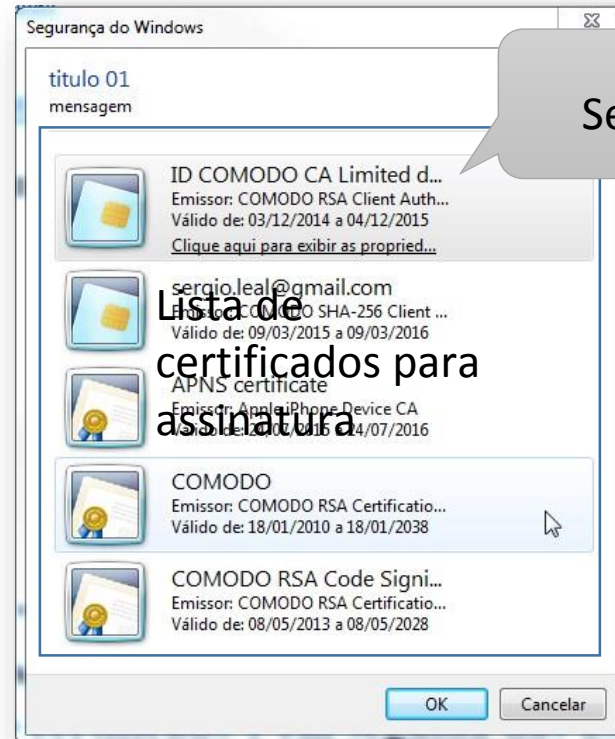
1. Acesse a página [http://localhost:8080/example/upload\\_RestSigner.html](http://localhost:8080/example/upload_RestSigner.html)

2. Na pagina vista no próximo slide comece fazendo o drag and drop de um arquivo;

Upload do conteúdo



## Escolha o certificado



Selecione um certificado da lista

Lista de  
certificados para  
assinatura

Digite a senha



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

## O sistema exibe o resultado

### Certificado

Nome	Valor
issuer0	CN=COMODO SHA-256 Client Authentication and Secure Email CA, O=COMODO CA Limited, I
serial0	239978131432459574058407871863249784083
subject0	EMAILADDRESS=sergio.leal@gmail.com
ku0	digitalSignature,keyEncipherment
cert_type0	standard
eku0	ekuEmailProt
crlDP0	http://crl.comodoca.com/COMODOSHA256ClientAuthenticationandSecureEmailCA.crl
certPolOid0	1.3.6.1.4.1.6449.1.2.1.1.1
basicConstraint0	-1
ocsp0	http://ocsp.comodoca.com
version0	3
notBefore0	1425945600000
san_email0	sergio.leal@gmail.com
certPolQualifier0	https://secure.comodo.net/CPS
chain0	http://crt.comodoca.com/COMODOSHA256ClientAuthenticationandSecureEmailCA.crt
key_length0	2048
notAfter0	1457567999000
aki0	92616B82E1A2A0AA4FEC67F1C2A3F7B48000C1EC
certSha2560	B060451E4DB83F95E99A70E99887D79A0450DE4001E140FFDE31A2D863317600D

Ao final informações retiradas do certificado serão exibidas...

### Assinatura

... E em baixo a assinatura feita

MIlJWQYJKoZIhvcNAQcCoIIJSjCCCUYCAQExDzANBgkqhkiG9w0BBwGgggVGMIIIFQjCCBCqgAwIBAgIRALSKG1/rwOUqIITzg3VJTRMwDQYJKoZIhvc



# Utilizando a extensão para o Chrome

Como utilizar a aplicação exemplo com a extensão pra o Chrome

## Requisitos

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

## Acessando a pagina

1. Acesse a página [http://localhost:8080/example/upload\\_ChromeExt.html](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



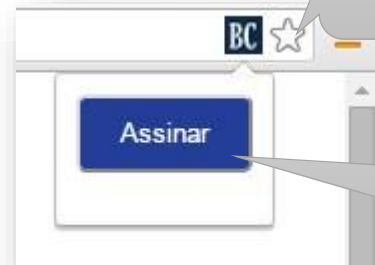
de endereços:

## Upload do conteúdo

### Passo 1: Arraste um documento

Arraste o arquivo que deseja assinar para aqui...

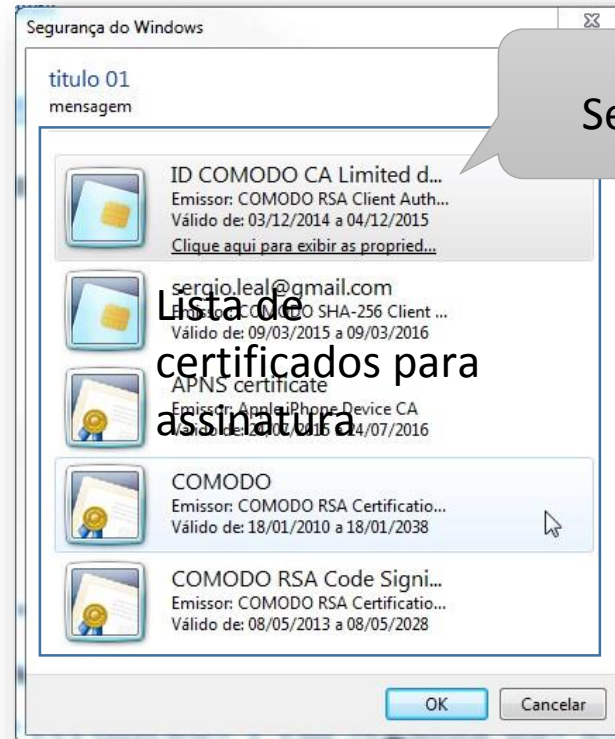
Arraste e solte um arquivo nessa área



Clique no ícone

Clique no botão 'Assinar'

## Escolha o certificado



Selecione um certificado da lista

Lista de  
certificados para  
assinatura

Digite a senha



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

## O sistema exibe o resultado

### Certificado

Nome	Valor
issuer0	CN=COMODO SHA-256 Client Authentication and Secure Email CA, O=COMODO CA Limited, I
serial0	239978131432459574058407871863249784083
subject0	EMAILADDRESS=sergio.leal@gmail.com
ku0	digitalSignature,keyEncipherment
cert_type0	standard
eku0	ekuEmailProt
crlDP0	http://crl.comodoca.com/COMODOSHA256ClientAuthenticationandSecureEmailCA.crl
certPolOid0	1.3.6.1.4.1.6449.1.2.1.1.1
basicConstraint0	-1
ocsp0	http://ocsp.comodoca.com
version0	3
notBefore0	1425945600000
san_email0	sergio.leal@gmail.com
certPolQualifier0	https://secure.comodo.net/CPS
chain0	http://crt.comodoca.com/COMODOSHA256ClientAuthenticationandSecureEmailCA.crt
key_length0	2048
notAfter0	1457567999000
aki0	92616B82E1A2A0AA4FEC67F1C2A3F7B48000C1EC
certSha2560	B060451E4DB83F95E99A70E99887D79A0450DE4001E140EED01A2D060017600D

Ao final informações retiradas do certificado serão exibidas...

### Assinatura

... E em baixo a assinatura feita

MIJWQYJKoZIhvcNAQcCoIIJSjCCCUYCAQExDzANBgkqhkiG9w0BBwGgggVGMIIIFQjCCBCqgAwIBAgIRALSKG1/rwOUqIITzg3VJTRMwDQYJKoZIhvc