

Manual de Instalação

Procedimento para instalação em diversos cenários

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.

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

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/inlgdajmhcicinhampnnpdneamfgjcgl?hl=pt-BR&authuser=2>)

Processo de instalação (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;

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

[Antes de iniciar o processo instale o Activex daqui](#)

Passo 1: Arraste um c

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'

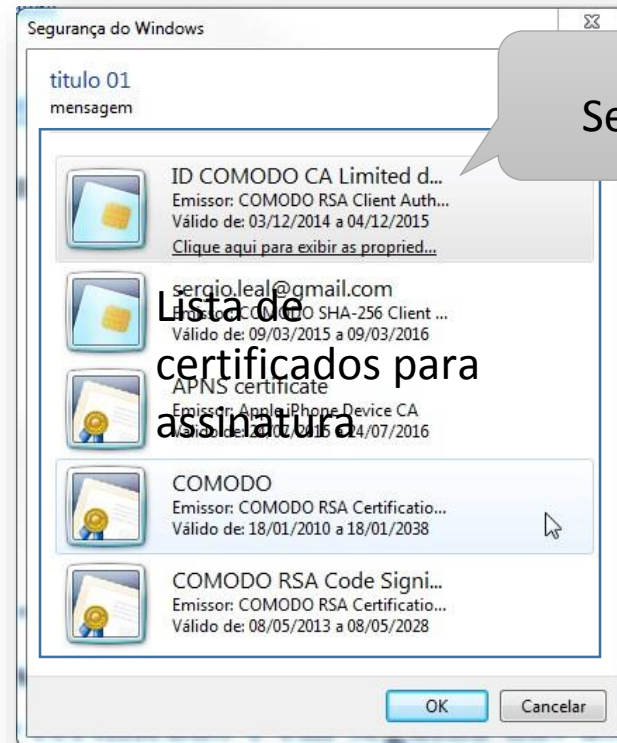
Assinar

Certificado

...

Assinatura

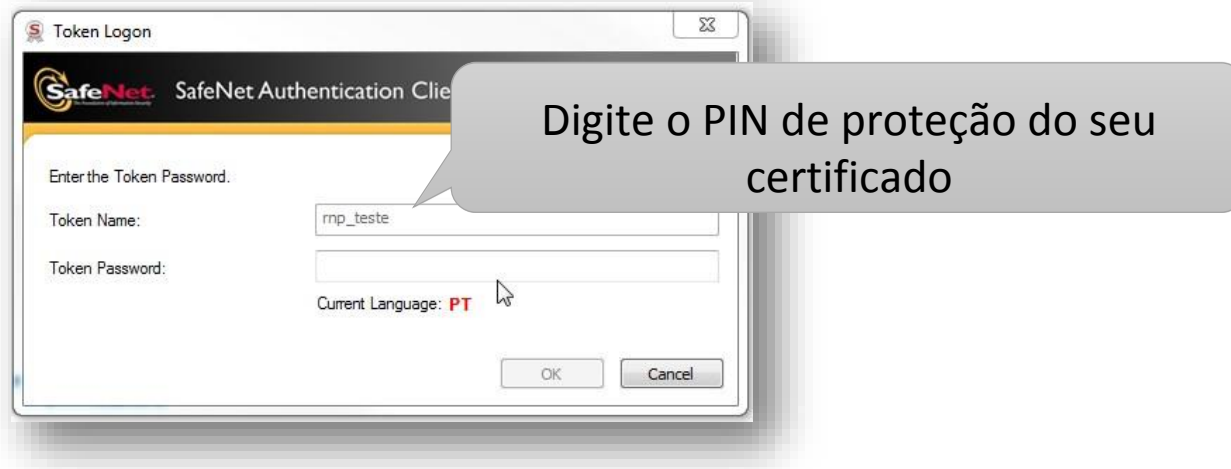
Escolha o certificado



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://crl.comodoca.com/COMODOSHA256ClientAuthenticationandSecureEmailCA.crt
key_length0	2048
notAfter0	1457567999000
aki0	92616B82E1A2A0AA4FEC67F1C2A3F7B48000C1EC
certSha2560	B060451E4DB83F95E99A70E99887D79A0450DE4004E10FEFE01A3B060017600D

Ao final informações retiradas do certificado serão exibidas...

Assinatura

... E em baixo a assinatura feita

MIIJWQYJKoZIhvcNAQcCoIIJSjCCCUYCAQEEDzANBgkqhkiG9w0BBwGgggVGMIIFQjCCBCqgAwIBAgIRALSKG1/rwOUqlITzg3VJTRMwDQYJKoZIhvc

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
 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'

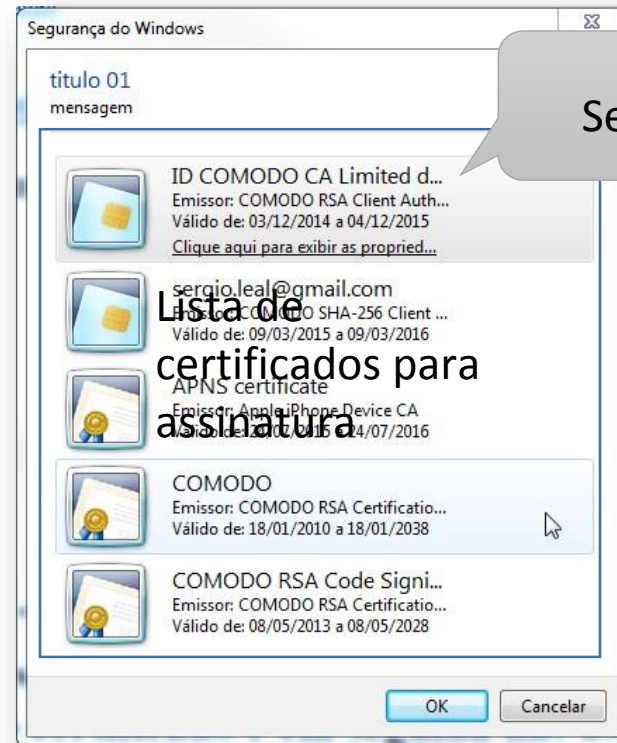
Assinar

Certificado

...

Assinatura

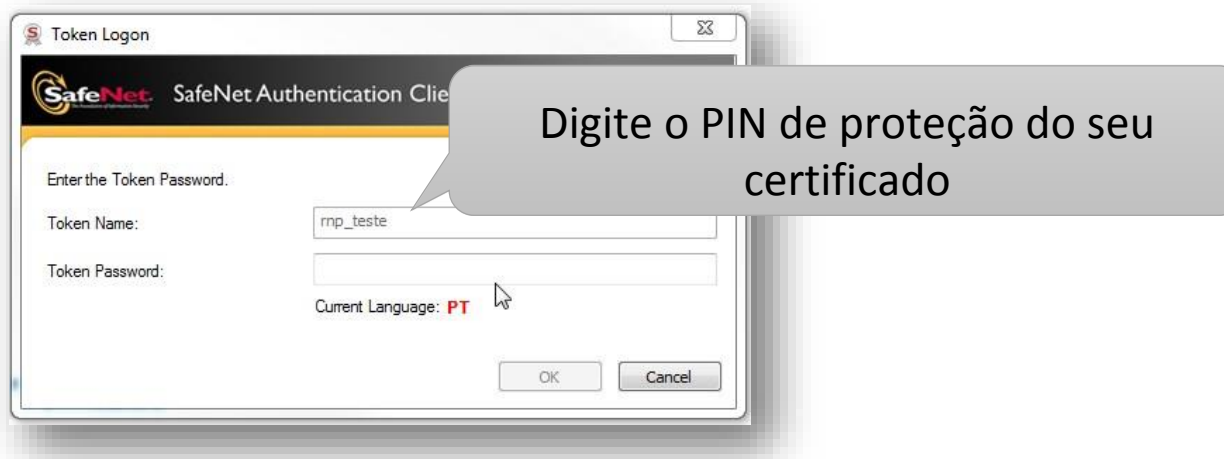
Escolha o certificado



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://crl.comodoca.com/COMODOSHA256ClientAuthenticationandSecureEmailCA.crt
key_length0	2048
notAfter0	1457567999000
aki0	92616B82E1A2A0AA4FEC67F1C2A3F7B48000C1EC
certSha2560	B060451E4DB83F95E99A70E99887D79A0450DE4004E10FEEF01A3B063017600D

Ao final informações retiradas do certificado serão exibidas...

Assinatura

... E em baixo a assinatura feita

MIIJWQYJKoZIhvcNAQcCoIIJSjCCCUYCAQEhDzANBgkqhkiG9w0BBwGgggVGMIIFQjCCBCqgAwIBAgIRALSKG1/rwOUqlITzg3VJTRMwDQYJKoZIhvc

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
 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

Digite o PIN do certificado

PIN: |

Passo 4: Selecione o botão "Carregar"

Selecione 'Carregar'

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 a 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://crl.comodoca.com/COMODOSHA256ClientAuthenticationandSecureEmailCA.crt
key_length0	2048
notAfter0	1457567999000
aki0	92616B82E1A2A0AA4FEC67F1C2A3F7B48000C1EC
certSha2560	B060451E4DB83F95E99A70E99887D79A0450DE4004E10FEEF01A3B063017600D

Ao final informações retiradas do certificado serão exibidas...

Assinatura


... E em baixo a assinatura feita

MIJWQYJKoZIhvcNAQcCoIJSjCCCUYCAQEEDzANBgglghkgBZQMEAgEFADALBgkqhkiG9w0BBwGgggVGMIIFQjCCBCqgAwIBAgIRALSKG1/rwOUqlITzg3VJTRMwDQYJKoZIhvc

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

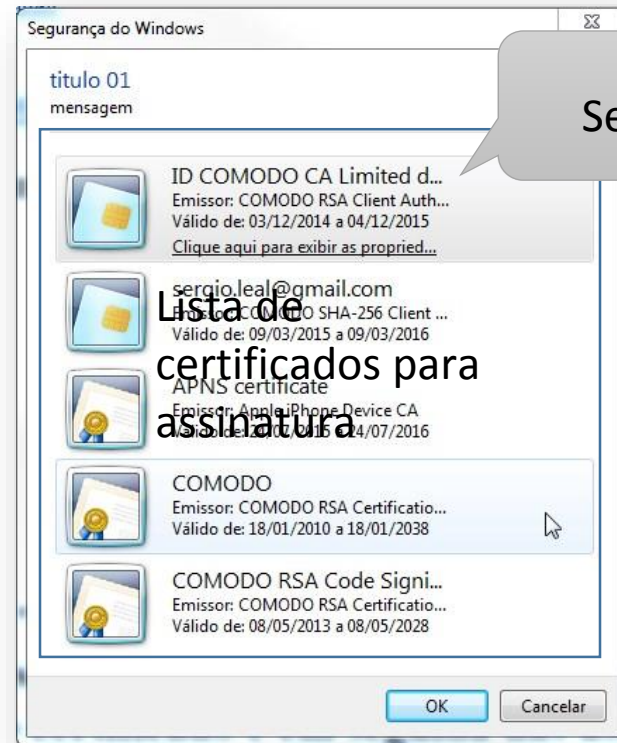
Upload do conteúdo

Passo 1: Arraste um documento

Arraste o arquivo que deseja assinar para aqui...

Arraste e solte um arquivo nessa área

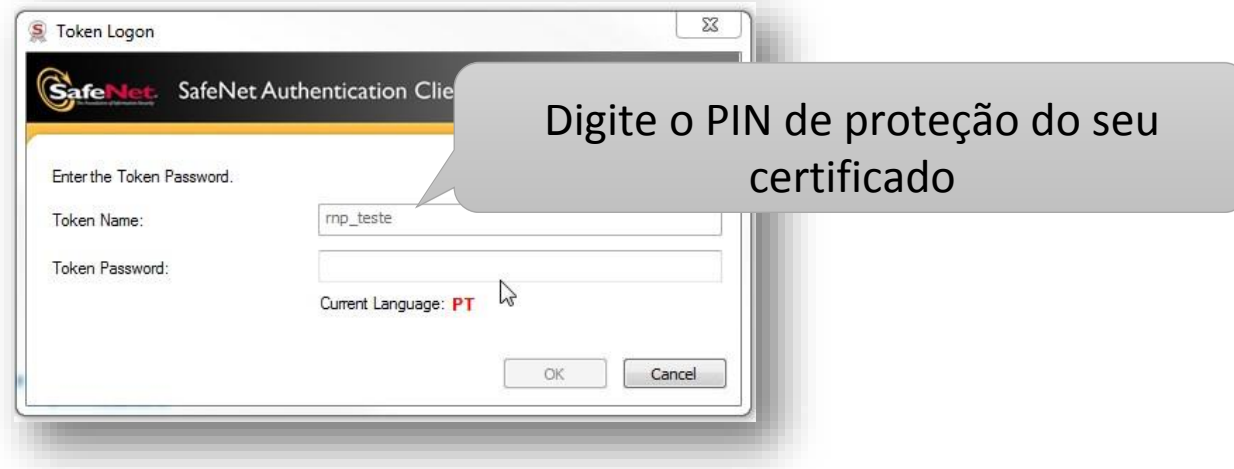
Escolha o certificado



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://crl.comodoca.com/COMODOSHA256ClientAuthenticationandSecureEmailCA.crt
key_length0	2048
notAfter0	1457567999000
aki0	92616B82E1A2A0AA4FEC67F1C2A3F7B48000C1EC
certSha2560	B060451E4DB83F95E99A70E99887D79A0450DE4004E10FEFE01A3B060017600D

Ao final informações retiradas do certificado serão exibidas...

Assinatura

... E em baixo a assinatura feita

MIIJWQYJKoZIhvcNAQcCoIIJSjCCCUYCAQExDzANBgkqhkiG9w0BBwGgggVGMIIFQjCCBCqgAwIBAgIRALSKG1/rwOUqlITzg3VJTRMwDQYJKoZIhvc

Utilizando o Chrome Ext

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
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...

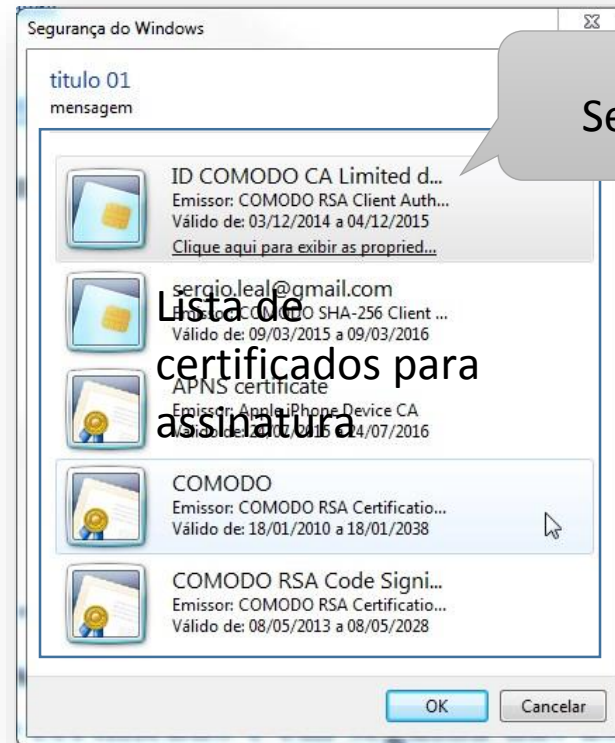
Arraste e solte um arquivo nessa área



Clique no ícone

Clique no botão 'Assinar'

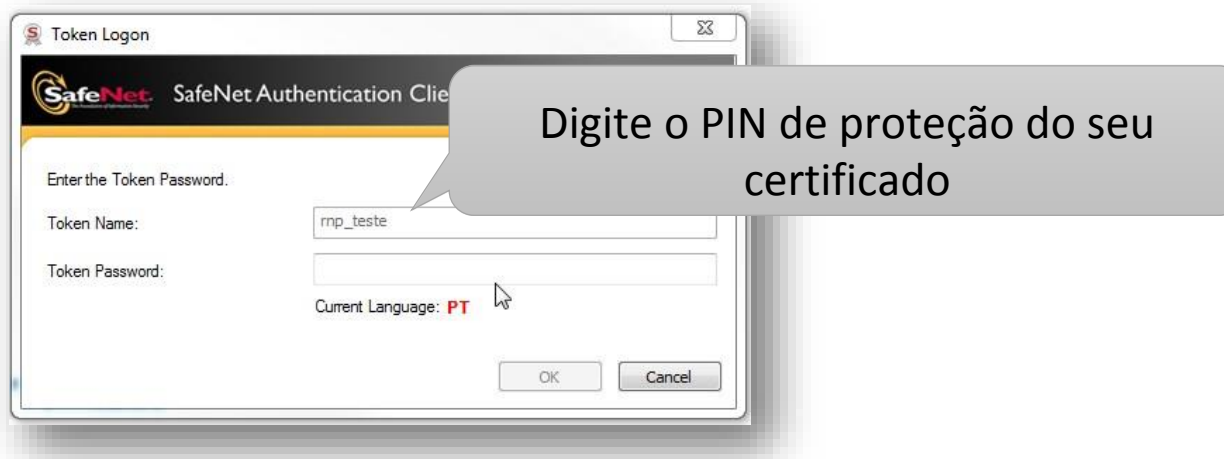
Escolha o certificado



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://crl.comodoca.com/COMODOSHA256ClientAuthenticationandSecureEmailCA.crt
key_length0	2048
notAfter0	1457567999000
aki0	92616B82E1A2A0AA4FEC67F1C2A3F7B48000C1EC
certSha2560	B060451E4DB83F95E99A70E99887D79A0450DE4004E10FEEF01A3B063017600D

Ao final informações retiradas do certificado serão exibidas...

Assinatura

... E em baixo a assinatura feita

MIIJWQYJKoZIhvcNAQcCoIIJSjCCCUYCAQExDzANBgglghkgBZQMEAgEFADALBgkqhkiG9w0BBwGgggVGMIIFQjCCBCqgAwIBAgIRALSKG1/rwOUqlITzg3VJTRMwDQYJKoZIhvc