



NOTA FISCAL DE SERVIÇO ELETRÔNICA (NFS-e)

**Manual de Utilização
WebService**

Versão 1.2

SUMÁRIO

SUMÁRIO.....	2
1. INTRODUÇÃO	3
2. CRIANDO UM CERTIFICADO DIGITAL	3
3. VINCULANDO UM CERTIFICADO DIGITAL A UM USUÁRIO DO ISS CURITIBA	6
4. EXPORTANDO O CERTIFICADO PARA UM ARQUIVO	8
5. INTERFACES DISPONÍVEIS NO WEBSERVICE	14
6. PADRÕES TÉCNICOS	15
7. WEBSERVICE NFS-E.....	16
8. ARQUIVOS DE EXEMPLO	17
9. RESUMO LINKS	18

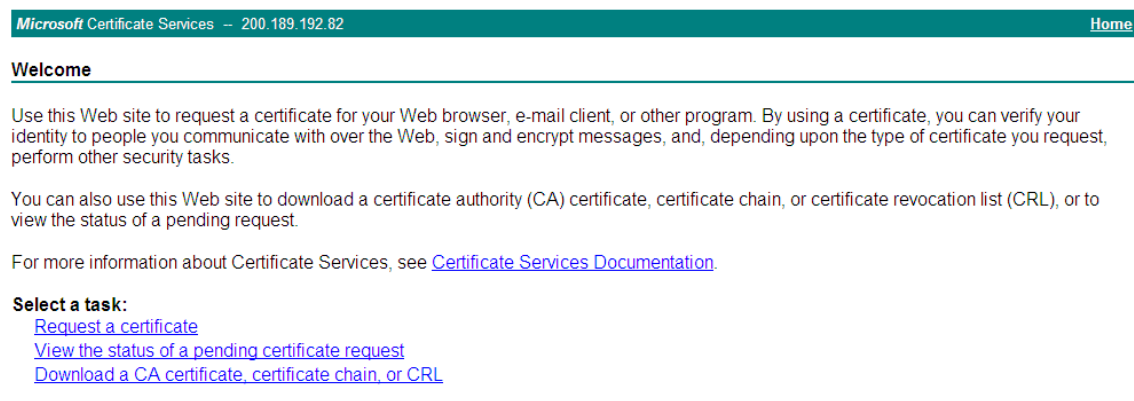
1. Introdução

Este manual tem por objetivo explicar como criar e utilizar um certificado digital em ambiente piloto, a fim de realizar os testes com o WebService.

2. Criando um certificado digital

Para dar início a criação do certificado digital (em ambiente piloto) deve-se utilizar o endereço <http://200.189.192.82/certsrv/>

Tal endereço irá apresentar a seguinte tela:



The screenshot shows the 'Microsoft Certificate Services' page for IP 200.189.192.82. The page has a teal header with the title and a 'Home' link. Below the header, the section 'Welcome' is followed by a paragraph explaining the site's purpose: to request certificates for web browsers, email clients, etc., and to verify identity. It also mentions downloading CA certificates, certificate chains, or CRLs. A link to 'Certificate Services Documentation' is provided. Under 'Select a task:', there are three links: 'Request a certificate', 'View the status of a pending certificate request', and 'Download a CA certificate, certificate chain, or CRL'.

Para criarmos o nosso certificado de testes clique em (Request a certificate).

Clicando no link referido acima o sistema irá apresentar a seguinte tela:



The screenshot shows the 'Request a Certificate' page. It has the same teal header as the previous page. Below the header, the section 'Request a Certificate' is followed by the instruction 'Select the certificate type:'. There are two links: 'Web Browser Certificate' and 'E-Mail Protection Certificate'. Below these, it says 'Or, submit an advanced certificate request' with a link.

Neste passo necessitamos criar um certificado de browser, ou seja, clique no link (Web Browser Certificate).

Alguns dados pessoais serão solicitados como mostrado abaixo:

Microsoft Certificate Services -- 200.189.192.82
Home

Web Browser Certificate - Identifying Information

To complete your certificate, type the requested information in the following boxes.

Name:

E-Mail:

Company:

Department:

City:

State:

Country/Region:

[More Options >>](#)

Submit >

Para que possamos criar um certificado válido (em ambiente piloto) é necessário clicar no link (More Options >>), após selecionado será apresentada a seguinte tela:

Microsoft Certificate Services -- 200.189.192.82
Home

Web Browser Certificate - Identifying Information

To complete your certificate, type the requested information in the following boxes.

Name:

E-Mail:

Company:

Department:

City:

State:

Country/Region:

More Options:

Select a Cryptographic Service Provider:

CSP:

☐ Enable strong private key protection

Request Format: ☒ CMC ☐ PKCS10

If you need to use an advanced option that is not listed here, [use the Advanced Certificate Request form](#).

Submit >

Após o carregamento da página mostrada acima deveremos clicar no link (use the Advanced Certificate Request form), pois necessitamos marcar uma opção para tornar a chave pública exportável.

Após clicar no link referido acima será apresentada a seguinte tela:

Advanced Certificate Request

Identifying Information:

Name:

E-Mail:

Company:

Department:

City:

State:

Country/Region:

Type of Certificate Needed:

Key Options:

☒ Create new key set ☐ Use existing key set

CSP:

Key Usage: ☐ Exchange ☐ Signature ☒ Both

Key Size: Min: 384 Max: 16384 (common key sizes: [512](#) [1024](#) [2048](#) [4096](#) [8192](#) [16384](#))

☒ Automatic key container name ☐ User specified key container name

☐ Mark keys as exportable

☐ Enable strong private key protection

☐ Store certificate in the local computer certificate store
Stores the certificate in the local computer store instead of in the user's certificate store. Does not install the root CA's certificate. You must be an administrator to generate or use a key in the local machine store.

Additional Options:

Request Format: ☒ CMC ☐ PKCS10

Hash Algorithm:
Only used to sign request.

☐ Save request to a file

Attributes:

Friendly Name:

Preencha os dados do formulário mostrado acima.

Selecione a opção (Mark Keys as exportable), como mostrado abaixo.

☒ Mark keys as exportable


☐ Export keys to file



Deixe apenas a opção (Mark Keys as exportable) selecionada a opção (Export Keys to file) não deverá ser marcada.

Após os dados serem preenchidos clique no botão (submit). Irá aparecer uma tela de confirmação conforma mostrado abaixo:

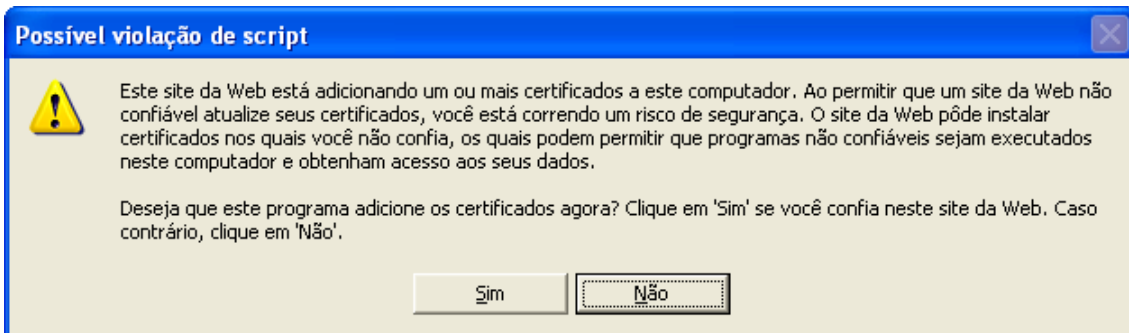
Possível violação de script

 Este site da Web está solicitando um novo certificado em seu nome. Você só deve permitir que sites da Web confiáveis solicitem um certificado em seu nome. Deseja solicitar um certificado agora?

Após confirmar a solicitação do certificado, irá aparecer uma tela para que possamos instalar o certificado digital em nossa máquina, como mostrado a seguir:



Clicando no link (Install this certificate) irá aparecer a seguinte tela de confirmação:



Confirmando a instalação de nosso certificado digital irá aparecer a seguinte tela:



Pronto agora temos um certificado digital (válido em ambiente piloto), mas ainda é necessário vincular o mesmo ao nosso usuário do sistema ISS Curitiba para que o sistema reconheça o mesmo.

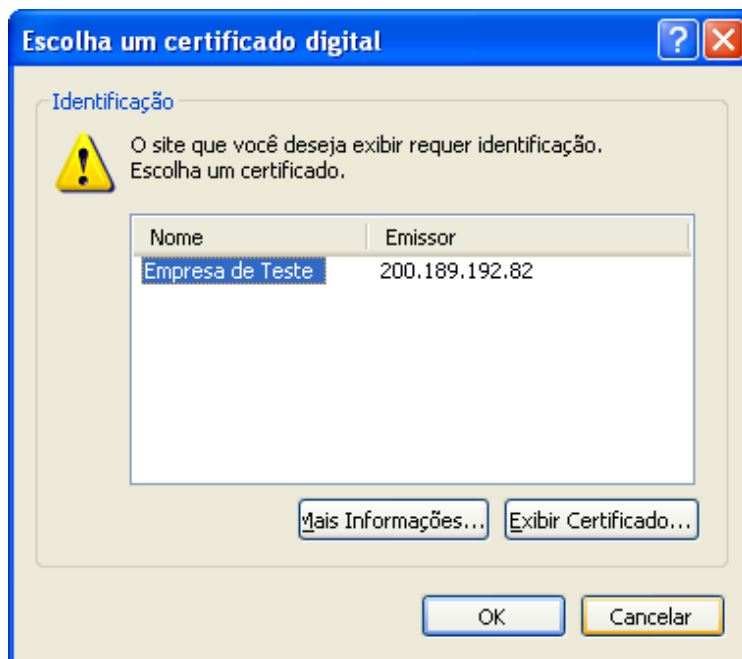
3. Vinculando um Certificado Digital a um usuário do ISS Curitiba

Após realizarmos todos os passos descritos anteriormente precisamos vincular o certificado digital recém criado ao nosso usuário do ISS Curitiba.

Para isso devemos entrar no ISS Curitiba em ambiente (piloto) utilizando HTTPS, ou seja, utilizando um canal seguro de comunicação:

https://200.189.192.82/pilotonota_iss/

Ao carregar o endereço acima no navegador, deverá aparecer uma caixa de diálogo, conforme figura abaixo:



Na caixa de diálogo acima irão aparecer todos os certificados digitais válidos para nossa entidade certificadora (para ambiente piloto).

Selecione o certificado digital desejado e clique em OK.

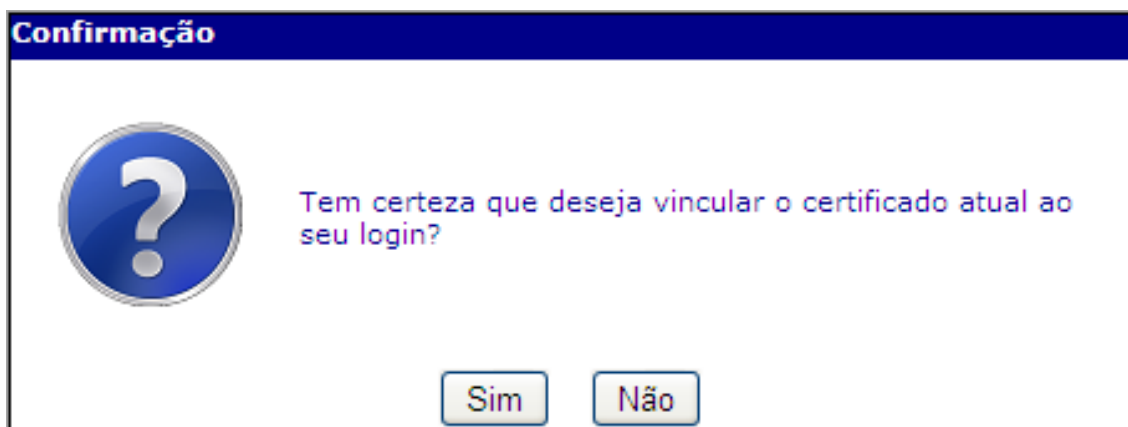
Após selecionar o certificado digital entre no ISS Curitiba utilizando o usuário e senha de acesso ao mesmo.

IMPORTANTE: Para acesso ao ambiente Piloto, deve-se usar o usuário já utilizado no sistema ISS Curitiba com a senha = 123456 .

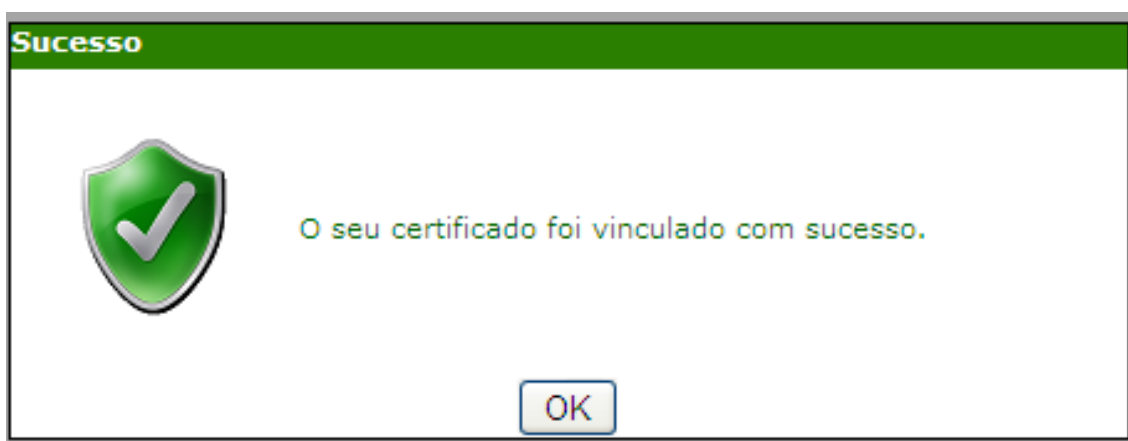
Uma vez logado no sistema, digite o seguinte endereço no browser (navegador):

https://200.189.192.82/pilotonota_iss/Principal/frmVincularCertificadoDigital.aspx

Irá aparecer uma tela de confirmação perguntando se você realmente deseja vincular seu certificado digital ao seu usuário do ISS Curitiba, como mostrado na figura abaixo:



Confirme a vinculação clicando em (Sim). Feito isso irá aparecer uma tela confirmando a vinculação do certificado, como descrito abaixo:



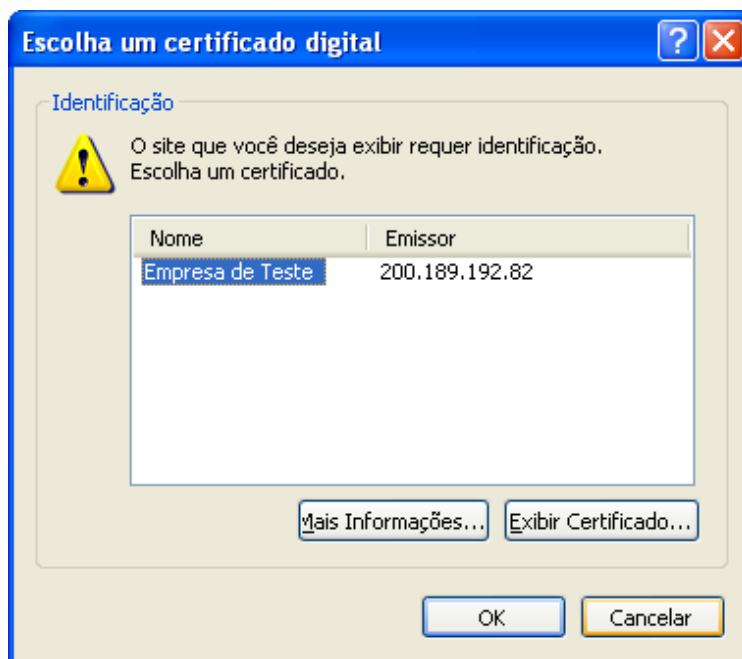
Depois de realizados tais passos já podemos utilizar o WebService para a empresa a qual o usuário pertence, pois já existe um certificado digital vinculado.

4. Exportando o Certificado para um arquivo

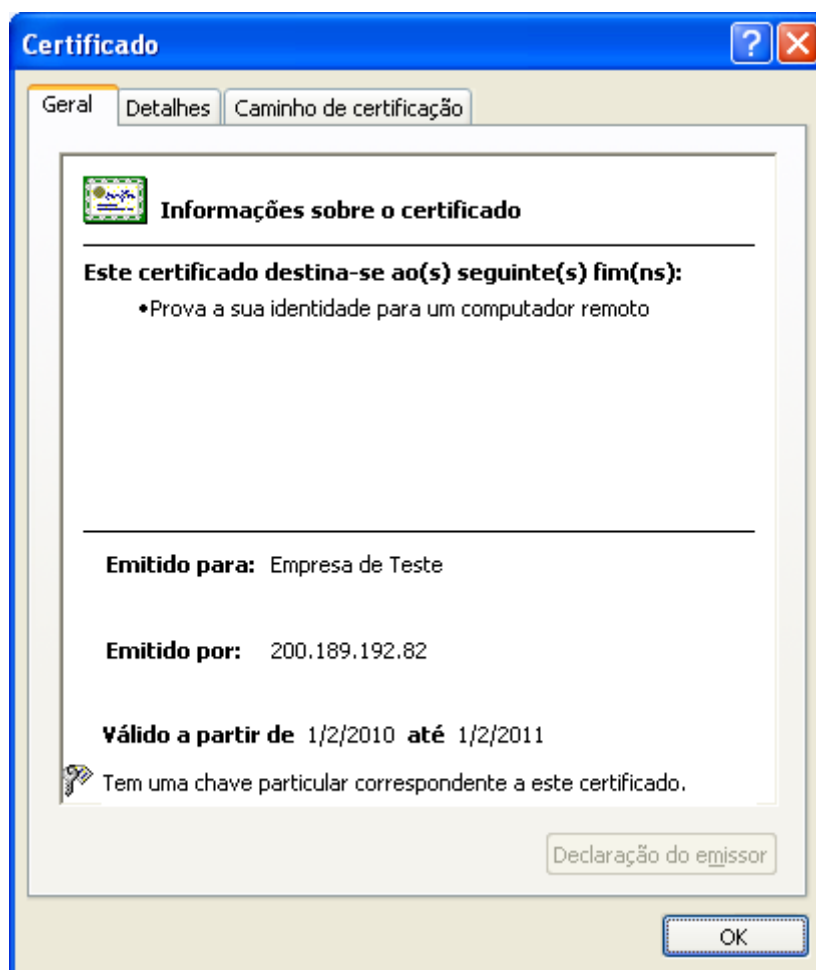
A exportação do certificado digital para um arquivo se dá pelo seguinte motivo.

Necessidade de integração de sistemas legados com o sistema de emissão de NFS-e da Prefeitura Municipal de Curitiba, onde toda requisição ao WebService é necessário anexar o certificado digital da empresa prestadora do serviço.

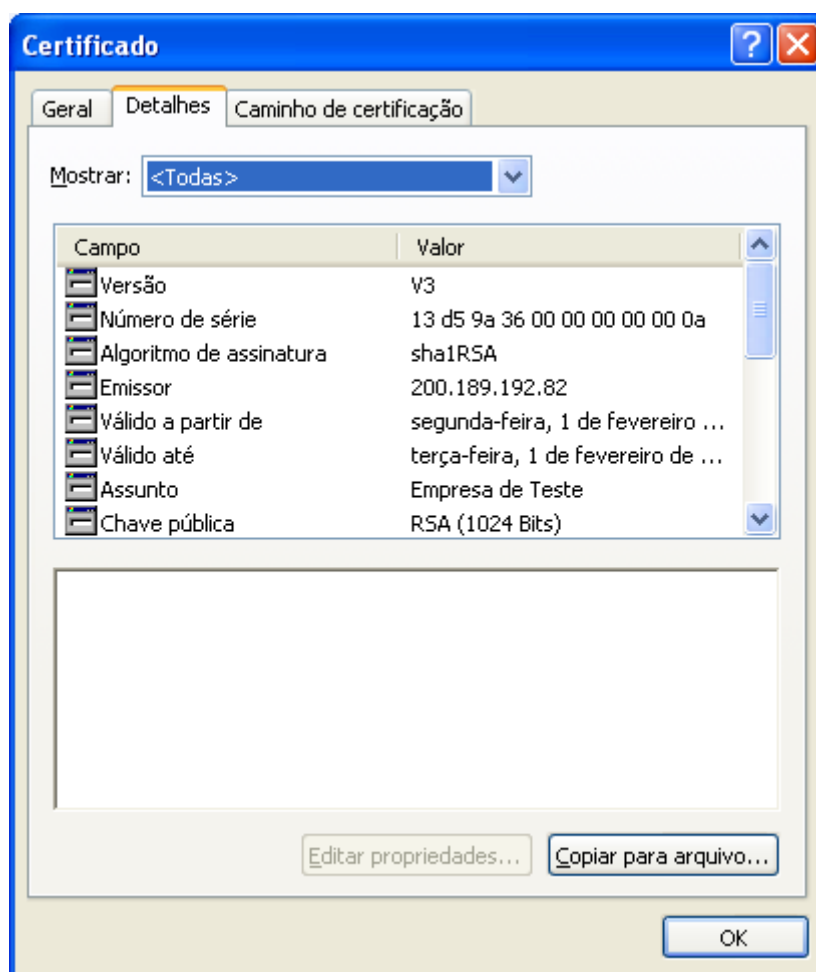
Na caixa de diálogo com os certificados digitais instalados em sua máquina, selecione um certificado e clique no botão (Exibir Certificado).



Irá ser mostrado a seguinte tela:



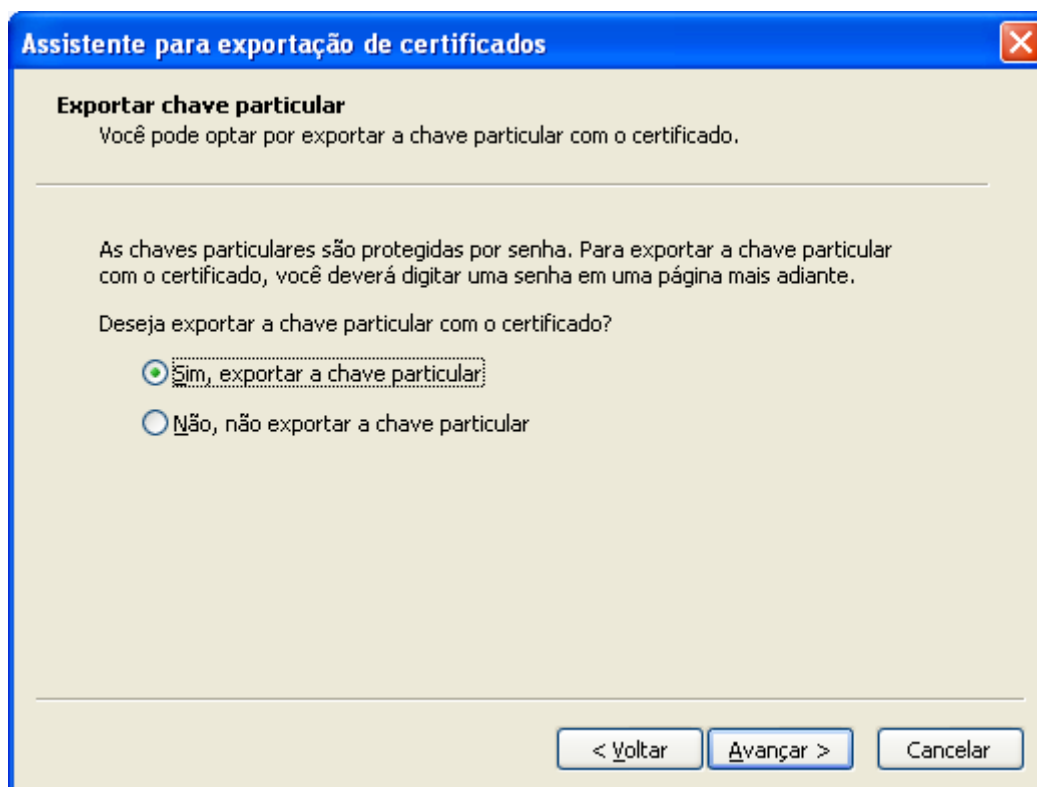
Clique na aba (Detalhes)

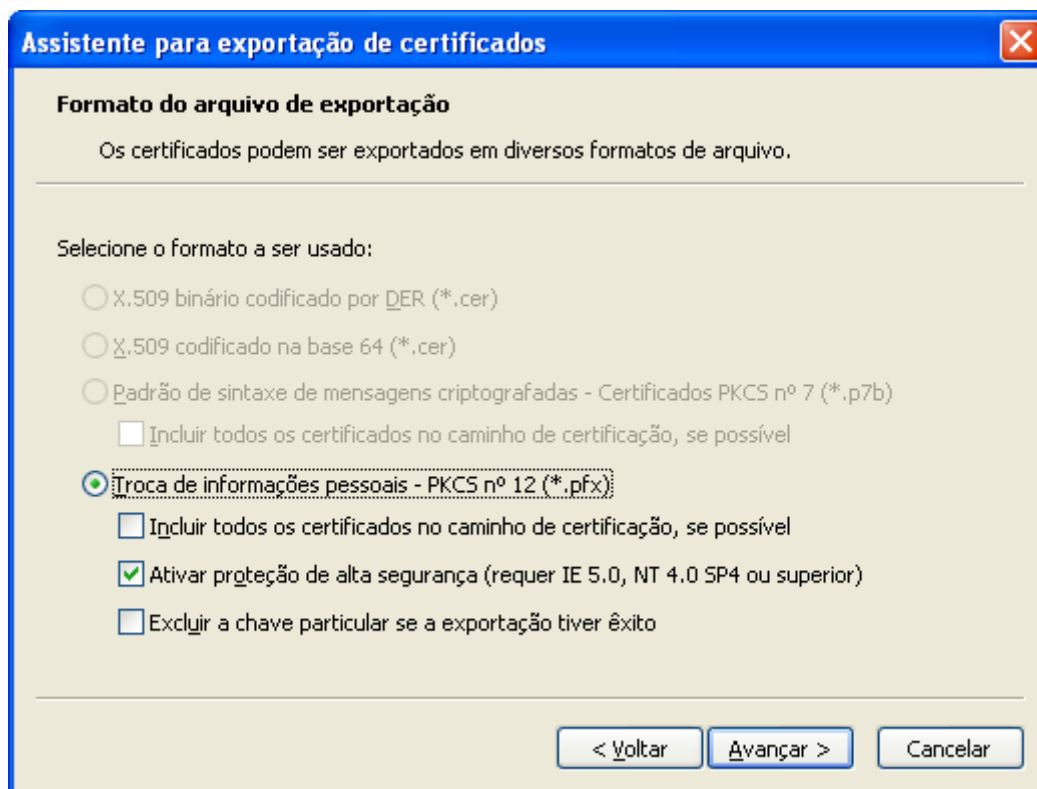


Logo em seguida clique no botão (Copiar para arquivo). Onde será apresentada a seguinte tela:



Clique no botão (Avançar), e será mostrado a tela abaixo, onde a opção (Sim, exportar a chave particular) deve ser marcada.





Assistente para exportação de certificados

Formato do arquivo de exportação

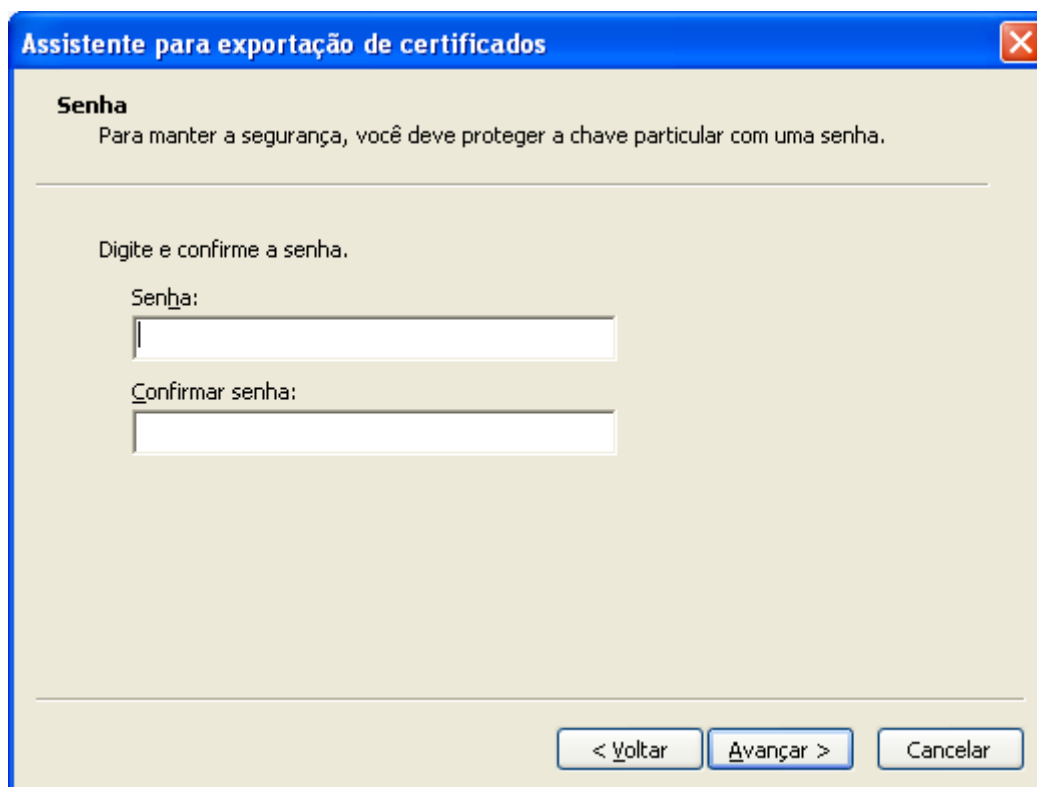
Os certificados podem ser exportados em diversos formatos de arquivo.

Selecione o formato a ser usado:

- ☐ X.509 binário codificado por DER (*.cer)
- ☐ X.509 codificado na base 64 (*.cer)
- ☐ Padrão de sintaxe de mensagens criptografadas - Certificados PKCS nº 7 (*.p7b)
 - ☐ Incluir todos os certificados no caminho de certificação, se possível
- ☒ Troca de informações pessoais - PKCS nº 12 (*.pfx)
 - ☐ Incluir todos os certificados no caminho de certificação, se possível
 - ☒ Ativar proteção de alta segurança (requer IE 5.0, NT 4.0 SP4 ou superior)
 - ☐ Excluir a chave particular se a exportação tiver êxito

< Voltar Avançar > Cancelar

Irá aparecer uma tela solicitando uma senha para o certificado, tal senha não é necessária, portanto deixe-a em branco.



Assistente para exportação de certificados

Senha

Para manter a segurança, você deve proteger a chave particular com uma senha.

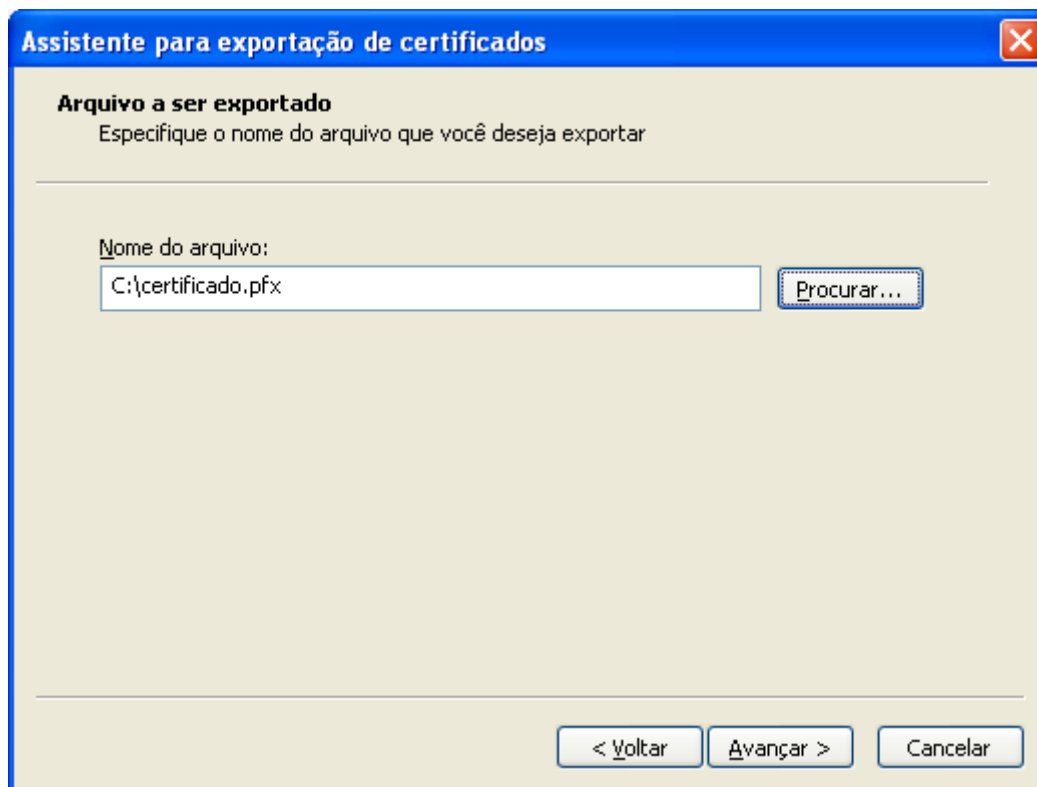
Digite e confirme a senha.

Senha:

Confirmar senha:

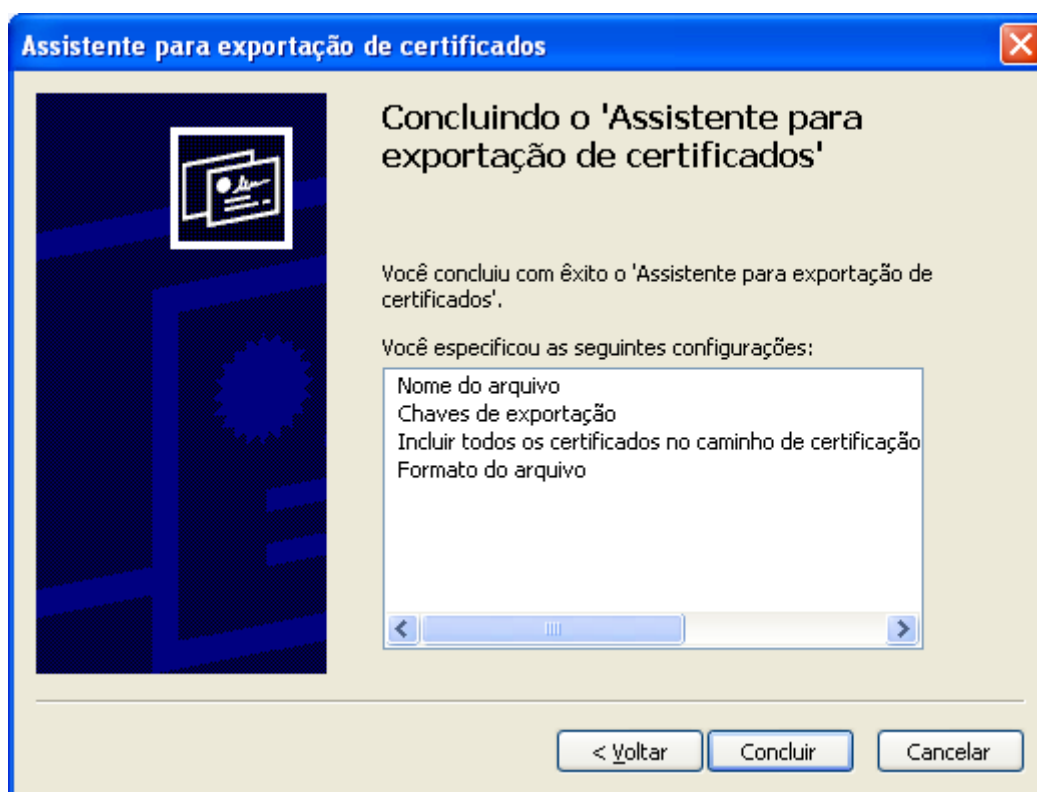
< Voltar Avançar > Cancelar

Na próxima tela selecione o nome do arquivo para qual o certificado será salvo e clique em (Avançar), como mostra a figura abaixo:

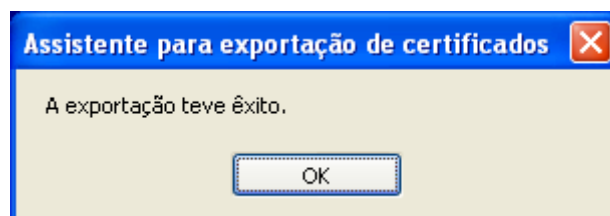


A screenshot of a Windows-style dialog box titled "Assistente para exportação de certificados". The dialog has a blue title bar with a close button (X) in the top right corner. The main area has a light beige background. At the top, the text "Arquivo a ser exportado" is followed by the instruction "Especifique o nome do arquivo que você deseja exportar". Below this is a horizontal line. Underneath the line, the label "Nome do arquivo:" is positioned to the left of a text input field. The input field contains the text "C:\\certificado.pfx". To the right of the input field is a button labeled "Procurar...". At the bottom of the dialog, there are three buttons: "< Voltar", "Avançar >", and "Cancelar".

Após feito os passos acima irá aparecer a seguinte tela, onde deveremos clicar no botão (Concluir).



Após feito isso irá aparecer uma mensagem dizendo que a importação obteve êxito, como descrito abaixo.



5. Interfaces disponíveis no WebService

5.1. RECEPÇÃO DE LOTE DE RPS

Através desta interface, os prestadores de serviços poderão enviar lotes de RPS emitidos em seus sistemas, para que os mesmos sejam convertidos em Notas Fiscais de Serviços Eletrônica.

Destina-se á prestadores de serviços que desejam emitir NFS-e off-line ou em grandes volumes.

5.2. CONSULTA A SITUAÇÃO DE LOTE DE RPS

Após o envio bem sucedido de um Lote de RPS, o WebService retorna o número do Lote de RPS e o número do protocolo de recebimento do lote. Com esta interface, basta informar o número do protocolo para receber a informação sobre o status de processamento do lote que pode ser um dos seguintes:

- Não processado;
- Processado com erros;
- Processado com sucesso.

5.3. CONSULTA DE LOTE DE RPS

Após o processamento de um Lote de RPS, é possível consultar todas as informações sobre o lote de RPS, tais informações como o número da NFS-e o valor gerado para crédito de abatimento no IPTU, entre outras informações.

Para o recebimento das informações sobre as notas geradas através de um lote de RPS, basta apenas informar o número do protocolo de recebimento do Lote de RPS e o WebService irá retornar todas as informações sobre as NFS-e geradas.

5.4. CONSULTA NOTA FISCAL DE SERVIÇOS ELETRÔNICA POR RPS

Esta interface permite aos prestadores de serviços consultarem as NFS-e emitidas por ele, através das informações do RPS anteriormente emitido pelo prestador.

5.5. CONSULTA NOTA FISCAL DE SERVIÇOS ELETRÔNICA

Esta interface permite aos prestadores de serviços consultarem as NFS-e por ele emitidas.

5.6. VALIDAÇÃO BÁSICA DO LOTE DE RPS

Esta interface fornece um meio para o prestador de serviços realizar uma pré-validação do arquivo XML a ser enviado com um Lote de RPS. Tal validação irá garantir que não irão faltar a informações básicas para a conversão dos RPS.

6. Padrões Técnicos

A comunicação entre os sistemas dos prestadores de serviços e o Sistema de Notas Fiscais de Serviços Eletrônica da Prefeitura Municipal de Curitiba será baseada em WebService.

O meio físico de comunicação utilizado será a Internet, com o uso do protocolo SSL (Socket Secure Layer), que além de garantir a segurança das informações trafegadas através da Internet, permite a identificação do servidor e do cliente através de certificados digitais, eliminando a necessidade do usuário se identificar através de usuário e senha.

O modelo de comunicação segue o padrão para WebService definido pelo WS-I Basic Profile. A troca de mensagens entre o WebService do sistema de NFS-e da Prefeitura Municipal de Curitiba utilizará o protocolo SOAP, com troca de mensagens XML.

6.1. PADRÃO DE CERTIFICADO DIGITAL

Os certificados digitais utilizados no Sistema de Notas Fiscais de Serviços Eletrônica da Prefeitura Municipal de Curitiba serão emitidos por Autoridade Certificadora credenciada pela Infra-estrutura de Chaves Públicas Brasileira – ICP Brasil. Serão aceitos certificados do tipo A1 ou A3, devendo conter o CNPJ do prestador de serviços.

Exclusivamente em ambiente piloto deverá ser utilizado certificados digitais oferecidos pelo próprio ambiente piloto. Vide capítulo 1 e 2. Tais certificados gerados em ambiente piloto não são válidos para o ambiente de produção.

6.2. SCHEMAS XML

Para garantir minimamente a integridade dos arquivos XML, o prestador de serviços deverá submeter cada arquivo XML para validação através do arquivo com os schemas XML para validação.

Um Schema XML define o conteúdo de uma mensagem XML, descrevendo os seus atributos, elementos e a sua organização, além de estabelecer regras de preenchimento de conteúdo e de obrigatoriedade de cada elemento ou grupo de informação.

O Schema XML poderá ser encontrado em <http://isscuritiba.curitiba.pr.gov.br/iss/nfse.xsd>.

7. WebService NFS-e

O WebService do Sistema de Notas Fiscais de Serviços Eletrônica da Prefeitura Municipal de Curitiba, disponibiliza os serviços que serão utilizados pelos sistemas dos prestadores de serviços. O mecanismo de utilização do WebService segue as seguintes premissas:

- Serão disponibilizados vários métodos dentro do mesmo WebService, cada um desses métodos executando uma funcionalidade específica.
- Alguns serviços disponibilizados serão processados de forma assíncrona, ou seja, os dados serão recebidos e serão processados em um momento mais oportuno.

7.1. WSDL

Para que os sistemas de informação dos prestadores de serviços saibam quais parâmetros enviar ao WebService e quais parâmetros serão retornados, os prestadores deverão utilizar a definição WSDL (Web Service Description Language, linguagem de descrição do serviço Web).

A documentação do WSDL pode ser obtida através do endereço http://200.189.192.82/pilotonota_websevice/NfseWs.asmx?WSDL.

7.2. TIPOS UTILIZADOS

Para obter a definição de todos os tipos utilizados pelo Sistema de Emissão de Notas Fiscais de Serviços Eletrônica basta acessar o endereço <http://isscuritiba.curitiba.pr.gov.br/iss/nfse.xsd>.

7.3. REALIZANDO UMA CHAMADA A UM MÉTODO DO WEBSERVICE

Para a utilização do WebService através de um sistema de informação de algum prestador de serviços é necessário anexar a requisição do serviço o certificado digital do prestador de serviços.

Tal certificado deve estar vinculado a um usuário dentro do ISS Curitiba, para que o sistema possa reconhecer a empresa.

7.4. REALIZANDO A VALIDAÇÃO BÁSICA DO ARQUIVO DE LOTE DE RPS

Para garantir que o mínimo das informações exigidas para a conversão do Lote de RPS em Notas Fiscais de Serviços Eletrônica, uma pré-validação do arquivo XML a ser enviado para processamento deverá ser realizada.

O elemento raiz do arquivo de Lote de RPS deve ficar da seguinte maneira:

```
<EnviarLoteRpsEnvio xmlns=http://isscuritiba.curitiba.pr.gov.br/iss/nfse.xsd  
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"  
xsi:schemaLocation="http://isscuritiba.curitiba.pr.gov.br/iss/nfse.xsd">
```

Desta forma garantiremos que o arquivo a ser validado pegue todas as informações dos schemas de validação dos dados.

Também foi disponibilizado um programa que realiza tal pré-validação sem a necessidade de conexão com o WebService. Tal programa está contido junto aos arquivos de exemplo (Vide Capítulo 8).

8. Arquivos de Exemplo

Para obter arquivos de exemplo acesse o link <http://isscuritiba.curitiba.pr.gov.br/iss/arquivos.zip>

9. Resumo Links

Abaixo seguem um resumo dos links necessários para que as empresas configurem seus sistemas para emissão de Notas Fiscais Eletrônicas optando pelo modo WebService:

- 1) Manual de Integração de Sistemas -
http://isscuritiba.curitiba.pr.gov.br/portalfse/Manuais/NFSE-NACIONAL_ManualDeIntegracao_Curitiba.pdf
- 2) Manual de Utilização de Envio Arquivos RPS -
http://isscuritiba.curitiba.pr.gov.br/portalfse/Manuais/Manual_Layout_Arquivo_RPS_Curitiba.pdf
- 3) Definições de chamadas dos métodos do WebService em ambiente piloto:
http://200.189.192.82/pilotonota_webservice/nfsews.asmx;
- 4) Definição WSDL do WebService:
http://200.189.192.82/pilotonota_webservice/nfsews.asmx?wsdl
- 5) Schema XSD para validação do XML:
http://200.189.192.82/pilotonota_iss/nfse.xsd
- 6) O endereço da área de testes (piloto) é: [http://200.189.192.82/pilotonota_iss/;](http://200.189.192.82/pilotonota_iss/)
- 7) Modelo XML para recepção de lote RPS em ambiente piloto:
http://200.189.192.82/pilotonota_iss/recepcionar_lote.xml
- 8) Para testes de envio via WS será necessário solicitar um certificado digital (testes) no endereço: <http://200.189.192.82/certsrv/>
- 9) Para vincular o certificado (teste) criado ao login do usuário para envio de WS:
https://200.189.192.82/pilotonota_iss/Principal/frmVincularCertificadoDigital.aspx

