

## 01. FUNÇÃO:

O programa <AssinadorRS.exe> tem as funções que seguem:

- Assinatura digital de Nota Fiscal Eletrônica (NF-e) e Conhecimento de Transporte Eletrônico (CT-e), doravante denominados Documento Fiscal Eletrônico (DF-e), no padrão XML Signature da W3C, conforme especificação dos projetos NF-e e CT-e;
- Verificação da Assinatura digital de Documento Fiscal Eletrônico;
- Geração de Lotes de Documento Fiscal Eletrônico, a partir de DF-e selecionados;
- Visualização de Documento Fiscal Eletrônico;
- Validação do Schema de todas as mensagens previstas nos Projeto NF-e e CT-e;
- Assinatura e verificação de assinatura de qualquer documento XML, no padrão de assinatura previsto nos Projetos NF-e e CT-e.

## 02. FRAMEWORK MICROSOFT

O programa foi desenvolvido na plataforma “**.NET**” da Microsoft e precisa da instalação prévia do **Framework 2.0** para poder ser executado.

O “Microsoft .NET Framework Version 2.0 Redistributable Package (x86)” pode ser obtido na internet no site da própria Microsoft no link: <http://www.microsoft.com/downloads/details.aspx?familyid=0856EACB-4362-4B0D-8EDD-AAB15C5E04F5&displaylang=en>

Após o download, deve ser feita a instalação do framework, executando o programa baixado (programa <dotnetfx.exe>).

## 03. PACOTE DE INSTALAÇÃO

O pacote de instalação cria o diretório <C:\Arquivos de programas\DFE>, contendo as sub-pastas e arquivos que seguem:

- **Pasta <Certificados>**  
Contém os Certificados Digitais de teste (Certificados “frios”) utilizados na aplicação.  
Os Certificados de teste estão nos arquivos:
  - <associacaoNFe.pfx>
  - <condominioNFe.pfx>
- **Pasta <DFe a Assinar>**  
Contém exemplos de arquivos XML de Documentos Fiscais Eletrônicos que podem ser utilizados para efetuar as assinaturas.
- **Pasta <DFe Assinada>**  
Diretório vazio que será utilizado para salvar DF-e assinadas pelo programa AssinadorRS.
- **Pasta <Schema>**  
Contém os Schemas (arquivo “.xsd”) utilizados.

Adicionalmente, o instalador cria um atalho no menu Iniciar para facilitar a execução do programa AssinadorRS:

*Iniciar ⇒ Programas ⇒ Secretaria da Fazenda – RS ⇒ DFe ⇒ AssinadorRS*

## 04. INSTALAÇÃO DO CERTIFICADO DIGITAL

Os Certificados Digitais “frios” utilizados foram gerados para testes e contém toda a cadeia de certificação necessária.

Foram disponibilizados 2 conjuntos de Certificados do padrão e-CNPJ, tipo A1 (certificado em arquivo).

Cada arquivo com extensão <.pfx> contém:

- Certificado Digital do Estabelecimento fictício:
  - “NFe - Associacao NF-e” (SENHA:associacao)
  - “NFe - Condominio NF-e” (SENHA:condominio)
- Certificado de AC Intermediária (NFe - AC Intermediaria 1) e
- Certificado de AC Raiz (NFe - AC Raiz).

### **Instalação do Certificado:**

Dar duplo-clique no arquivo do Certificado, acionando o “Assistente de Importação de Certificados” do Windows.

O “Assistente” irá se encarregar de efetuar a instalação do Certificado na área de armazenamento de certificados do próprio Windows. Responder as opções de instalação sempre com “Avançar”, “Avançar”, ... e “Concluir”.

Os Certificados apresentados serão armazenados na área de usuário do Windows, nas pastas:

- <Pessoal>: Certificado do Estabelecimento (Certificado com a chave privada a ser utilizada na assinatura);
- <Autoridades de Certificação intermediárias>: Certificado NFe - AC Intermediaria 1;
- <Autoridades de Certificação Raiz>: Certificado NFe - AC Raiz.

Nota: Para visualizar os Certificados armazenados no Windows execute o Internet Explorer e acione:

- Menu Ferramentas / Opções da Internet / aba Conteúdo / botão Certificados

## **05. ARQUIVOS XML: LOTE OU DF-e INDIVIDUAL**

A princípio, o AssinadorRS está direcionado para assinar e/ou conferir a assinatura digital unicamente do Lote de DF-e a e/ou do arquivo XML de um Documento Fiscal individual.

A identificação do arquivo de Lote ou do arquivo de DF-e é feita utilizando os esquemas XML (arquivo .xsd) definidos para o Projeto de Nota Fiscal Eletrônica e Conhecimento de Transporte Eletrônico. A identificação do tipo de arquivo é feita pela TAG raiz da estrutura de XML presente no arquivo na forma:

- Arquivo de Lote: raiz = <enviNFe> ou raiz <enviCTe>
- Arquivo de DF-e individual: raiz = <NFe> ou raiz <CTe>

Como uma funcionalidade extra do programa AssinadorRS, é apresentado na área de LOG o motivo da rejeição para os arquivos não validados pelo Schema.

## **06. VISÃO GERAL DO PROGRAMA**

A interface com o Operador apresenta 4 áreas distintas, conforme segue:

- Barra de menus e barra de botões
- Área de Entrada (redimensionável)
- Área de Saída (redimensionável)
- Área de LOG (redimensionável)

Através da Barra de Menu, o Operador comanda as **Tarefas**, efetuando as **Configurações** e executando as **Funções** desejadas. As **Configurações** e **Funções** disponíveis são:

### **A. Configura Diretório de Entrada**

Configura a pasta onde estão os arquivos XML a serem assinados.

### **B. Configura Diretório de Saída**

Configura a pasta onde serão arquivados os arquivos XML assinados. Se for de interesse do Operador, pode ser configurado o Diretório de Saída idêntico ao Diretório de Entrada. Para poder diferenciar os arquivos que foram assinados pelo AssinadorRS, é acrescentado o literal “\_sign” no nome de arquivo de entrada.

### **C. Configura Diretório de Schema**

Após a instalação do AssinadorRS, a configuração aponta para o diretório Schema, disponível com a versão inicial dos Schemas XML. O AssinadorRS utiliza os Schemas dos Projetos NF-e e CT-e.

Eventualmente o Comitê Gestor dos Projetos NF-e e/ou CT-e libera novas versões dos Schemas. Neste caso, a atualização dos Schema para uso do AssinadorRS pode ser feita pelo Operador em uma das formas que seguem:

- Inclui no diretório Schema, a nova versão do Schema desejado;
- Cria um novo diretório para recepcionar as novas versões dos Schemas e configura o AssinadorRS para utilizar este novo diretório.

### **D. Seleciona Certificado**

Seleciona o Certificado que será utilizado na assinatura.

Nota: Os Diretórios e Certificados configurados serão mantidos para as próximas execuções do programa.

### **E. Função: Assinatura DF-e / Assinatura Lote / Assinatura de outros documentos XML**

O arquivo previamente selecionado na Área de Entrada será assinado com o Certificado configurado e um novo

arquivo, com os dados da assinatura XML, será disponibilizado na área de saída. Será acrescentado o literal “\_sign” no nome do arquivo de entrada para compor o nome do arquivo no diretório de saída.

O mesmo processo de assinatura de DF-e pode ser comandado para um Lote de DF-e, gerando um arquivo Lote de saída, com todos os Documentos Fiscais assinados individualmente.

A área de LOG apresenta informações sobre as operações comandadas.

#### **F. Função: Valida de SCHEMA e Assinatura DF-e / Lote / Outros documentos Xml**

O arquivo previamente selecionado na Área de Saída terá validado o Schema e a assinatura, utilizando o Certificado Digital presente no mesmo arquivo XML que está sendo verificado.

São verificados também os dados básicos do Certificado, como a data de início da validade e a data de expiração.

É verificada também toda a Cadeia de Certificação referente ao Certificado Digital, utilizando os Certificados das AC de teste presentes na área de armazenamento de Certificados do Windows.

A validação da Assinatura não está considerando a consulta a Lista de Certificados Revogados (LCR). Esta função necessita de acesso a internet e nem sempre o equipamento que está executando o programa AssinadorRS tem este acesso disponibilizado de forma direta (normalmente o equipamento não tem acesso a internet ou possui o acesso controlado por um “proxy”).

O mesmo processo de validação da assinatura do DF-e pode ser comandado para um Lote de DF-e, verificando a assinatura de todos os DF-e constantes no Lote.

A área de LOG apresenta informações sobre as operações comandadas.

Se for selecionado um arquivo na Área de Entrada, será validado o Schema e, se existente, será validada também a assinatura.

#### **G. Função: Gera Lote**

Para a geração do Lote de DF-e é necessário selecionar previamente os arquivos de DF-e que irão compor o Lote. Conforme a seleção pode ser gerado um Lote de Documentos na Área de Entrada (DF-e não assinados), ou um Lote de Documentos na Área de Saída (DF-e assinados).

Faz parte do nome do arquivo de Lote um número aleatório para evitar a geração de arquivos com o mesmo nome.

#### **H. Função: Visualizar Arquivo**

Os arquivos previamente selecionados serão visualizados em janelas específicas para cada arquivo.

#### **I. Função: Atualiza Áreas de Entrada e de Saída (“Refresh”)**

O acionamento desta função causa a atualização das informações sobre os arquivos visualizadas nas Áreas de Entrada e Saída.

#### **J. Função: Outras**

O acionamento do **botão direito do mouse** sobre as Áreas de Entrada e Saída disponibiliza o acesso as funções de <Selecionar Todos> arquivos, <Desmarcar Todos> ou <Remover> um determinado arquivo selecionado.

---

## A. CONSIDERAÇÕES TÉCNICAS

### A01. VÍNCULO ASSINATURA COM DADOS

Conforme o padrão do W3C, a associação da assinatura XML com os dados que forem assinados pode ser feita das formas que seguem:

- <Enveloped>: tag de assinatura após os dados;
- <Enveloping>: os dados são envelopados dentro da assinatura;
- <Detached>: a assinatura compõe um arquivo XML externo.

O modelo adotado no Projeto Nota Fiscal Eletrônica é o <Enveloped>.

### A02. CADEIA DE CERTIFICAÇÃO

A conferência completa da assinatura compreende os passos:

- conferência da assinatura do arquivo utilizando o Certificado do Contribuinte;
- conferência do Certificado do Contribuinte;
- conferência dos demais Certificados envolvidos na Cadeia de Certificação.

Os Certificados podem estar presente ou não no arquivo XML recebido, conforme as opções:

- <none>: Certificado não incluso no arquivo XML;
- <EndCertOnly>: incluso no arquivo somente o Certificado do Contribuinte (Certificado que assinou);
- <ExcludeRoot>: todos os Certificados da cadeia de certificação são inclusos no XML, menos o Certificado de Root (ICP-Brasil);
- <WholeChain>: todos os Certificados da cadeia de certificação são inclusos no XML.

O modelo adotado no AssinadorRS é o “EndCertOnly”.

Os demais Certificados da Cadeia de Certificação deverão estar residentes na área de **Armazenamento de Certificados** do equipamento que fará a conferência das assinaturas.

### A03. X509 Data Elements

O Certificado Digital que efetuou a assinatura da NF-e consta no arquivo XML e já contém os principais elementos do padrão X509, inclusive o valor da Chave Pública, tornando desnecessária a sua representação individualizada. Não são incluídos no arquivo XML assinado os elementos abaixo:

```
<X509SubjectName>
<X509IssuerSerial>
  <X509IssuerName>
  <X509SerialNumber>
<X509SKI>

<KeyValue>
  <RSAKeyValue>
    <Modulus>
    <Exponent>
```

Também não deve ser incluído o elemento <X509CRL> no arquivo XML assinado, já que a implementação dos Projetos NF-e e CT-e pela SEFAZ deverá sempre verificar a Lista de Certificados Revogados no momento da conferência da Assinatura.

A supressão destes elementos leva a redução do tamanho do arquivo da NF-e assinada.

### A04. PreserveWhiteSpaces

Opcionalmente, devem ser eliminados os espaços e caracteres de tabulação na Nota Fiscal assinada, com a inclusão da propriedade:

```
preserveWhiteSpace = false
```

Esta opção leva a redução do tamanho do arquivo da NF-e assinada.

## **A05. Assinatura Parcial do Arquivo XML**

O Projeto prevê a assinatura parcial do arquivo XML do DF-e, somente para a TAG <infNFe> ou <infCTe>. Esta TAG engloba todos os dados de interesse das SEFAZ, previstos no layout regulamentado.

As vantagens desta implementação são:

- Permite a inclusão de campos no DF-e que não serão assinados, podendo ser enviados ou não para o Fisco;
- Permite a verificação das assinaturas dos DF-e ainda na estrutura de Lote (caso contrário, primeiro o Lote deve ser “desmanchado”, para permitir a verificação individual das assinaturas);
- Permite a assinatura dos DF-e dentro da estrutura de Lote, o que pode ser interessante para as empresas, por questões de performance.

Para efetuar esta assinatura é utilizada a URI, referenciando o atributo “Id” da TAG <infNFe> ou <infCTe>.

## **A06. Transformação**

O processo de assinatura digital primeiro passa pela geração de um resumo (“digest”) a ser assinado.

Antes da geração deste “digest” são aplicadas transformações sobre os dados a serem resumidos e o AssinadorRS implementa as transformações previstas no Projeto da NF-e, na forma:

```
<Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />  
<Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315" />
```