

Sistema Nacional Nota Fiscal de Serviço



Manual para emissão da NFS-e Via

Anexo II - Guia para utilização das API's V1.0

Histórico de Versões

Versão	Data	Alterações da Versão
1.0.0	18/09/2025	Criação do documento
1.0.1	28/10/2025	Atualização do documento para o modelo de APIs Síncronos.
1.0.2	12/12/2025	Atualização do documento para incluir informações sobre a produção restrita.

Resumo do documento

Descrição	Este documento contempla informações sobre a utilização das API's de Recepção e Consulta de processamento de documentos eletrônicos de NFS-e Via relacionados as Concessionárias emissoras desses documentos.
------------------	---

Sumário

Manual das Concessionárias – Sistema Nacional NFS-e Via.....	1
Guia para utilização das API's.....	1
Versão 1.0.1 – Outubro de 2025	1
Histórico de Versões	2
Resumo do documento	2
1. Definições Nota Fiscal Eletrônica de Exploração de Vias e Eventos.....	4
1.1. Nota Fiscal Eletrônica de Exploração de Vias - NFS-e Via e Evento de Cancelamento	4
1.1.1 Descrição	4
1.1.2 Assinatura.....	4
1.1.3 Padrão de Documento XML	4
1.1.4 Esquema (Schema) para Arquivos XML na NFS-e Via	4
1.1.5 Padrão de Comunicação.....	5
1.1.6 Padrão de Certificado Digital	5
1.1.7 Padrão de Assinatura Digital.....	5
2. Receptor Público Nacional NFS-e Via – (Ambiente Nacional NFS-e Via)	6
2.1. API Recepção NFS-e Via.....	6
2.1.1 Descrição	6
2.1.2. Métodos	7
2.1.3. Ambiente de homologação.....	8
Link do ambiente de homologação	8
2.1.4. Ambiente de Produção Restrita.....	8
Link de Produção Restrita.....	8
2.2. API Consultas NFS-e Via.....	8
2.2.1 Descrição	8
2.2.2. Métodos	8
2.2.3. Ambiente de homologação.....	9
Link do ambiente de homologação	9
2.2.4. Ambiente de Produção Restrita.....	9
Link de Produção Restrita.....	9
Considerações Finais	10

1. Definições Nota Fiscal Eletrônica de Exploração de Vias e Eventos

1.1. Nota Fiscal Eletrônica de Exploração de Vias - NFS-e Via e Evento de Cancelamento

1.1.1 Descrição

As informações serão fornecidas pelas Concessionárias por meio de arquivo(s) XML. O XML de NFS-e Via e seus Eventos deverão ser enviado através de uma API REST (modo síncrono) ao Ambiente Nacional da NFS-e Via.

O processamento dos documentos será executado de forma síncrona, recebidos e validados via API REST. Além disso, o sistema dispõe de serviços específicos para consultas, permitindo obter informações sobre o processamento dos arquivos eletrônicos enviados pelas Concessionárias e o resultado da sua validação tanto no momento da transmissão quanto em momento posterior através do protocolo ou da chave de acesso do documento.

1.1.2 Assinatura

Os arquivos XML deverão ser assinados digitalmente, conforme a legislação brasileira, para garantir a integridade dos dados e a autoria do emissor.

ATENÇÃO: Os documentos eletrônicos deverão ser assinados digitalmente utilizando o e-CNPJ da Concessionária (raiz).

1.1.3 Padrão de Documento XML

A especificação do documento XML adotada é a recomendação W3C para XML 1.0, disponível em <http://www.w3.org/TR/REC-xml>.

A codificação dos caracteres será em UTF-8 e assim, todos os documentos XML devem ser iniciados com a seguinte declaração:

```
<?xml version="1.0" encoding="UTF-8"?>
```

1.1.4 Esquema (Schema) para Arquivos XML na NFS-e Via

A estrutura dos arquivos XML recebidos pelo Ambiente Nacional da NFS-e Via é definida e verificada por meio de um Esquema (Schema), uma linguagem que estabelece as regras para a estruturação do documento XML. O Schema descreve os elementos, sua organização e as regras de preenchimento de conteúdo, garantindo a obrigatoriedade de cada elemento ou grupo de informações.

Representação Física do Schema

O Schema é representado fisicamente por um arquivo com extensão XSD (XML Schema Definition). Este arquivo define quaisquer elementos que podem ou não estar presentes no XML, bem como as regras que governam a estrutura do documento.

Validação da Estrutura XML

A validação da estrutura XML é realizada por um analisador sintático (parser), que verifica se a mensagem atende às definições e regras estabelecidas no Schema. Qualquer divergência entre a estrutura do XML e o Schema resultará em um erro de validação.

Localização da Definição do XML

A definição do XML para NFS-e Via encontra-se detalhada no documento "LeiauteRN_NFSeVia&Eventos-ANNFSeVia."

Disponibilidade dos Schemas

Os Schemas (XSD) que definem os arquivos XML aceitos estão disponíveis no Portal XXXXX. [Endereço: <https://www.portalxxxxx.com.br/schemas>]

Tipos de Schema

Os seguintes tipos de Schema estão disponíveis:

1. Documento Eletrônico – NFS-e Via
 - Define a estrutura do XML para a NFS-e Via.
2. Documento Eletrônico – Evento de Cancelamento
 - Contém os Schemas para os eventos de negócio relacionados ao cancelamento, previstos para serem enviados ao Ambiente Nacional da NFS-e Via.

Esta organização visa garantir que os arquivos XML sejam consistentes e seguros, atendendo às exigências legais e operacionais do sistema NFS-e Via.

1.1.5 Padrão de Comunicação

A comunicação será baseada em APIs REST (modo síncrono), disponibilizadas pelo Serpro.

O canal físico de comunicação utilizado será a Internet, utilizando o protocolo HTTPS (TLS 1.2 ou superior) com autenticação mútua. Além de garantir um canal de comunicação seguro, essa configuração permite a identificação mútua do servidor e do cliente por meio de certificados digitais."

1.1.6 Padrão de Certificado Digital

O certificado digital utilizado no Ambiente Nacional de NFS-e Via deverá ser emitido por Autoridade Certificadora credenciada pela Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil.

O certificado digital deverá ser do tipo A1 ou A3. Certificados digitais de tipo A1 ficam armazenados no próprio computador utilizado. Certificados digitais do tipo A3 são armazenados em dispositivos portáteis invioláveis do tipo smart card ou token, que possuem um chip com capacidade de realizar a assinatura digital. Este tipo de dispositivo é bastante seguro, pois toda operação é realizada pelo chip existente no dispositivo, sem qualquer acesso externo à chave privada do certificado digital.

Para que um certificado seja aceito na função de transmissor de solicitações este deverá ser do tipo e-aplicação, e-CNPJ (e-PJ). Os certificados digitais podem ser utilizados tanto nas conexões SSL de transmissão, quanto para a assinatura dos eventos.

Transmissão: antes de ser iniciada a transmissão de solicitações ao sistema, o certificado digital do solicitante é utilizado para reconhecer o transmissor e garantir a segurança do tráfego das informações na Internet.

Assinatura de documentos: para garantir o não repúdio e a integridade das informações, os documentos eletrônicos enviados são assinados digitalmente seguindo a especificação descrita no item “Padrão de Assinatura Digital” e nas orientações estabelecidas neste manual.

Os Certificados Digitais utilizados no acesso aos serviços disponibilizados pelo sistema e na assinatura dos arquivos XML enviados deverão atender aos seguintes critérios:

Critério	Mensagem	Efeito
Certificado de Transmissão não informado	E100	Rejeição
Certificado de Transmissão inválido	E101 e E102	Rejeição
Autoridade Certificadora Inválida	E103	Rejeição
Não foi possível verificar o não repúdio do Certificado de Transmissão	E104	Rejeição
Certificado de Transmissão expirado	E105	Rejeição
Certificado de Transmissão e-CPF	E106	Rejeição
Não foi possível acessar a Lista de Certificados Revogados	E107	Rejeição
Erro na cadeia de certificado	E108	Rejeição
Certificado de Transmissão Revogado	E109	Rejeição
CNPJ do Certificado de Transmissão não autorizado	E206	Rejeição

1.1.7 Padrão de Assinatura Digital

O sistema utiliza um subconjunto do padrão de assinatura XML, definido pelo <http://www.w3.org/TR/xmlsig-core/>.

A assinatura digital do documento eletrônico deverá ser realizada na tag do XML que contém o atributo "ID" e deve atender aos seguintes padrões adotados:

- **Padrão de assinatura:** XML Digital Signature, utilizando o formato Enveloped (<http://www.w3.org/TR/xmlsig-core/>)
- **Certificado digital:** emitido por AC credenciada no ICP-Brasil (<http://www.w3.org/2000/09/xmlsig#X509Data>)
- **Cadeia de certificação:** EndCertOnly (Incluir na assinatura apenas o certificado do usuário final)
- **Tipo do certificado:** A1 ou A3
- **Tamanho da chave criptográfica:** compatível com os certificados A1 e A3 (1024 e 2048 bits).
- **Função criptográfica assimétrica:** RSA(<http://www.w3.org/2001/04/xmlsig-more#rsa-sha256>)
- **Função de message digest:** SHA-2 (<http://www.w3.org/2001/04/xmlenc#sha256>)
- **Codificação:** Base64 (<http://www.w3.org/2000/09/xmlsig#base64>)
- **Transformações exigidas:** útil para realizar a canonicalização do XML enviado, para realizar a validação correta da assinatura digital. São elas:
 - Enveloped (<http://www.w3.org/2000/09/xmlsig#enveloped-signature>)
 - C14N (<http://www.w3.org/TR/2001/REC-xml-c14n-20010315>)

As informações necessárias à identificação do assinante estão presentes dentro do certificado digital, tornando desnecessária a sua representação individualizada no arquivo XML.

2. Receptor Público Nacional NFS-e Via – (Ambiente Nacional NFS-e Via)

O sistema NFS-e Via é um conjunto de serviços desenhados para a gestão de notas fiscais de serviços eletrônicas relacionadas à exploração de vias. Este documento descreve os métodos de API disponíveis para interação com o sistema.

2.1. API Recepção NFS-e Via

Protocolo de comunicação: TLS 1.0, TLS 1.1 e TLS 1.2 com autenticação mútua

Formato para troca de mensagens: JSON

Formato dos documentos da NFS-e Via: XML 1.0 (<https://www.w3.org/TR/REC-xml>)

Codificação de caracteres: UTF-8

Certificado digital: Emitido por Autoridade Certificadora ICP-Brasil, tipo A1 ou A3, CNPJ, com “Autenticação do Cliente”

Padrão de assinatura dos documentos XML: XMLDSIG (<https://www.w3.org/TR/xmlsig-core/>)

Padrão de compactação dos documentos XML para troca de mensagens: GZip com representação base64binary

2.1.1 Descrição

A API permite que as concessionárias transmitam documentos eletrônicos de NFS-e Via para o Ambiente Nacional. O processo é dividido em três serviços principais:

Serviços Disponíveis:

1. Recebimento e Validação do Arquivo XML de NFS-e Via:

Permite a recepção e o processamento do arquivo XML referente à NFS-e Via.

2. Recebimento e Validação do Arquivo XML de Cancelamento de NFS-e Via:

Permite a recepção e o processamento do arquivo XML referente ao Cancelamento de NFS-e Via.

3. Recebimento e Validação do Arquivo XML de NFS-e Via de Substituição e Cancelamento por Substituição:

Permite a recepção e o processamento do arquivo XML referente à NFS-e Via de Substituição acompanhado de seu respectivo cancelamento por substituição.

Processo de Recepção:

A API realiza uma série de validações para garantir a integridade e a conformidade das mensagens recebidas:

- Validação da Estrutura:
Verificação do formato correto do JSON enviado.
Análise dos campos que compõem a mensagem para garantir que estejam de acordo com as especificações da aplicação.
- Validação do Certificado de Transmissão:
Verificação da validade e autenticidade do certificado digital utilizado para a transmissão.
- Resultados da Transmissão:
Rejeição: Acontece quando há erros na estrutura da mensagem ou no certificado de transmissão. Neste caso, a API retorna uma mensagem de erro detalhada.
Sucesso na Recepção: Retorna uma mensagem de sucesso, confirmando que a mensagem foi recebida e está pronta para ser processada no ambiente nacional.

Requisitos para Aceitação da Recepção:

Para que a mensagem JSON seja aceita pela API, são necessários:

1. Formato do JSON:

O JSON enviado deve estar de acordo com as especificações definidas pelo sistema.

2. CNPJ da Concessionária:

O CNPJ da concessionária deve estar cadastrado no ambiente destinado às concessionárias.

3. CNPJ do Certificado de Autenticação:

O CNPJ associado ao certificado de autenticação deve estar cadastrado no sistema ONE ou no ambiente das concessionárias, garantindo assim a autorização de transmissão.

A API é uma ferramenta essencial para a transmissão de documentos eletrônicos de NFS-e Via, oferecendo serviços específicos para atender às necessidades das concessionárias. Com um processo de validação rigoroso, a API garante a segurança e a conformidade das transações, permitindo que as concessionárias enviem e validem seus documentos de forma eficiente e segura.

Processo de Validação de Documentos Eletrônicos de NFS-e Via

A validação realizada sobre a NFS-e Via e seus eventos de Cancelamento e Cancelamento por Substituição durante a recepção dos documentos está compreendida em:

- Esquemas e Leiaute da NFS-e e eventos de Cancelamento e Cancelamento por Substituição;
- Regras de negócio aplicadas para a aceitação dos documentos eletrônicos de NFS-e via no Ambiente Nacional;

Para mais detalhes sobre as regras de validação, consulte o documento [LeiauteRN_NFS-eVia&Eventos-ANNFS-eVia](#).

2.1.2. Métodos

```
Example Value | Model
{
  "cnpjConcessionaria": "string",
  "identificador": "string",
  "notaFiscalViaXmlGZipBase64": "string",
  "eventoViaXmlGZipBase64": "string"
}
```

a) POST – /nfsev

Finalidade: Receber e validar de forma síncrona a Nota Fiscal de Serviço eletrônica de Exploração de Via (NFS-e Via).

Funcionalidade: Este método recebe uma requisição JSON contendo:

- Cabeçalho: CNPJ da concessionária e chave de acesso do documento.
- Corpo: Arquivo XML da NFS-e Via compactado em GZip e representado em base64binary (campo: notaFiscalViaXmlGZipBase64).

O sistema retorna uma mensagem com o resultado da recepção/validação (código de retorno e descrição do retorno), o protocolo de recepção do arquivo e a chave de acesso do documento enviado.

Para os casos de erro, a validação retorna o primeiro encontrado no documento e encerra nele o processo de validação da NFS-e Via.

b) POST – /cancelamento

Finalidade: Receber e validar de forma síncrona um Evento de Cancelamento de NFS-e Via.

Funcionalidade: Este método recebe uma requisição JSON contendo:

- Cabeçalho: CNPJ da concessionária e chave de acesso do documento.
- Corpo: Arquivo XML do Evento de Cancelamento de NFS-e Via compactado em GZip e representado em base64binary (campo: eventoViaXmlGZipBase64).

O sistema retorna uma mensagem com o resultado da recepção/validação (código de retorno e descrição do retorno), o protocolo de recepção do arquivo e o identificado do evento enviado.

Para os casos de erro, a validação retorna o primeiro encontrado no documento e encerra nele o processo de validação do evento.

c) POST – /substituicao

Finalidade: Receber e validar de forma síncrona a NFS-e Via Substituta e seu respectivo Evento de Cancelamento por Substituição.

Funcionalidade: Este método recebe uma requisição JSON contendo:

- Cabeçalho: CNPJ da concessionária e chave de acesso do documento.
- Corpo: Arquivo XML da NFS-e Via Substituta compactado em GZip e representado em base64binary (campo: notaFiscalViaXmlGZipBase64) e arquivo XML do Evento de Cancelamento por Substituição compactado em GZip e representado em base64binary (campo: eventoViaXmlGZipBase64).

O sistema retorna uma mensagem com o resultado da recepção/validação (código de retorno e descrição do retorno), o protocolo de recepção do arquivo e chave de acesso da NFS-e Via Substituta.

Para os casos de erro, a validação é executada iniciando-se pelo evento de cancelamento por substituição e em seguida pela NFS-e Via substituta, sendo retornado o primeiro erro encontrado e encerrando nele o processo de validação rejeitando ambos os documentos pelo mesmo motivo.

Validações Dados JSON:

Mensagem	Código	Tipo
Chave de acesso no metadado é diferente da chave de acesso no documento.	1144	Rejeição

CNPJ da concessionária no metadado é diferente do CNPJ da concessionária no documento.	1145	Rejeição
CNPJ da concessionária no metadado é diferente do CNPJ da concessionária no documento vinculado.	1146	Rejeição

Validações Gerais:

Erros não tratados pela aplicação serão retornados com os códigos e mensagens indicados abaixo (com exceção do erro 9997). Tais ocorrências podem decorrer de indisponibilidades temporárias e, caso persistam, deverão ser encaminhadas para análise técnica.

Mensagem	Código	Tipo
Falha no processamento da requisição.	9996	Rejeição
Requisição duplicada a chave de acesso já existe na base de dados.	9997	Rejeição
Falha no processamento da requisição.	9998	Rejeição
Falha no processamento da requisição.	9999	Rejeição

2.1.3. Ambiente de homologação

Foi disponibilizada uma Swagger em ambiente de homologação destinada a testes por parte das Concessionárias durante a homologação do sistema.

Link do ambiente de homologação

<https://hom-cert-api-nfsevia.np.estaleiro.serpro.gov.br/recepcao/swagger/index.html>

2.1.4. Ambiente de Produção Restrita

Foi disponibilizada uma Swagger em ambiente de produção restrita destinada a testes por parte das Concessionárias com o objetivo de manter o sistema em produção funcionando de forma confiável e segura e permitindo mudanças apenas de forma controlada e rastreável.

Link de Produção Restrita

<https://producaorestrita.certificado.api.via.nfse.gov.br/recepcao/swagger/index.html>

2.2. API Consultas NFS-e Via

Protocolo de comunicação: TLS 1.0, TLS 1.1 e TLS 1.2 com autenticação mútua

Formato para troca de mensagens: JSON

Formato dos documentos da NFS-e Via: XML 1.0 (<https://www.w3.org/TR/REC-xml>)

Codificação de caracteres: UTF-8

Certificado digital: Emitido por Autoridade Certificadora ICP-Brasil, tipo A1 ou A3, CNPJ, com “Autenticação do Cliente”

Padrão de assinatura dos documentos XML: XMLDSIG (<https://www.w3.org/TR/xmlsig-core/>)

Padrão de compactação dos documentos XML para troca de mensagens: GZip com representação base64binary

2.2.1 Descrição

A API de Consultas NFS-e Via é uma ferramenta projetada para que as concessionárias consultem informações relacionadas ao envio e validação de seus documentos eletrônicos (NFS-e Via) em um ambiente nacional. Essa API oferece três serviços principais, descritos a seguir:

- Consultar Alíquota Efetiva por Trechos sob Concessão;
- Consultar Resultado por Protocolo;
- Consultar Resultado por Chave de Acesso;

CNPJ do Certificado de Autenticação: Deve estar cadastrado no ambiente das concessionárias para autorização de consultas.

2.2.2. Métodos

a) GET – /Aliquotas/efetiva/cnpj/{cnpj}/trecho/{codigoTrecho}/dataReferencia/{dataReferencia}

Recupera a alíquota efetiva de um trecho sob concessão de uma Concessionária em uma determinada data de referência.

A Concessionária informa um dos seus trechos sob concessão em que ela deseja consultar a alíquota efetiva de todo o trecho em uma determinada data.

b) GET – /Consulta/protocolo

Consulta o resultado da recepção ou da validação de um documento eletrônico de NFS-e Via enviado ao Ambiente Nacional através do seu protocolo de retorno de recepção.

A Concessionária informa o protocolo que é retornado no momento da recepção dos documentos eletrônicos de NFS-e Via para consultar o resultado da recepção ou o resultado da validação de um documento.

O documento eletrônico de NF-e Via somente é aceito no Ambiente Nacional quando a validação do documento retorna sucesso. Qualquer outro retorno indica a rejeição do documento.

c) GET – /Consulta/chaveacesso

Consulta o resultado da recepção ou da validação de um documento eletrônico de NFS-e Via enviado ao Ambiente Nacional basendo-se na chave de acesso do documento.

A Concessionária informa a chave de acesso de um documento eletrônico de NFS-e Via para consultar o resultado da recepção ou o resultado da validação de um documento.

O documento eletrônico de NF-e Via somente é aceito no Ambiente Nacional quando a validação do documento retorna sucesso. Qualquer outro retorno indica a rejeição do documento.

Como um documento com a mesma chave de acesso pode ser enviado mais de uma vez para corrigir problemas de envios anteriores, o retorno da consulta por chave de acesso ocorre da seguinte forma:

Passo1 – Sucesso:

Verificação se o documento da chave informada possui registro de validação com sucesso na base nacional da NFS-e Via. Se sim, a consulta termina e são retornados os dados enviados na consulta mais a situação de “Documento validado com sucesso no Ambiente Nacional da NFS-e Via.”

Caso não seja encontrado nenhum resultado, a consulta passa para o próximo passo.

Passo2 – Rejeição:

Verificação se o documento da chave informada possui registro de erros de rejeição na base nacional da NFS-e Via. Se sim, a consulta termina e são retornados os dados enviados na consulta e o erro de rejeição registrado após a validação desse documento.

Caso não seja encontrado nenhum resultado, a consulta passa para o próximo passo.

Passo3 – Não recepcionado:

Verificação se o documento da chave informada possui registro de erros de recepção na base nacional da NFS-e Via. Se sim, a consulta termina e são retornados os dados enviados na consulta e o erro de recepção registrado quando o documento foi rejeitado nas validações de recepção.

Caso não seja encontrado nenhum resultado, deverá ser retornado que não consta nenhum registro desse documento bno Ambiente Nacional da NFS-e Via.

2.2.3. Ambiente de homologação

Foi disponibilizada uma Swagger em ambiente de homologação destinada a testes dessas consultas por parte das Concessionárias durante a homologação do sistema.

Link do ambiente de homologação

<https://hom-cert-api-nfsevia.np.estaleiro.serpro.gov.br/concessionarias/swagger/index.html>

2.2.4. Ambiente de Produção Restrita

Foi disponibilizada uma Swagger em ambiente de produção restrita destinada a testes por parte das Concessionárias com o objetivo de manter o sistema em produção funcionando de forma confiável e segura e permitindo mudanças apenas de forma controlada e rastreável.

Link de Produção Restrita

<https://producaorestrita.certificado.api.via.nfse.gov.br/concessionarias/swagger/index.html>

Considerações Finais

Referências Técnicas:

Para mais informações sobre os esquemas e layouts, consulte o documento "[LeiauteRN_NFSeVia&Eventos-ANNFSeVia](#)".

Este guia está estruturado para facilitar a compreensão e o uso da API, garantindo que as concessionárias possam consultar e validar seus documentos de forma eficiente e segura.

