MDFe
Manifesto Eletrônico de Documentos Fiscais

PAA
Provedor de Assinatura e Autorização

Projeto Manifesto Eletrônico de Documentos Fiscais

Nota Técnica **2022.002**

Versão 1.02 – abril 2026

ENCAT
Encontro Nacional de Coordenadores e Administradores Tributários Estaduais

Receita Federal

Sumário

Histórico de Alterações / Cronograma 3
1 Provedor de Assinatura e Autorização 4
2 Geração de XML com envio ao Ambiente de Autorização 4
3 Padrão de Certificado Digital para Assinatura Avançada 4
1. Chave Privada RSA (PrivateKey): 5
2. Chave Pública RSA (PublicKey): 5
4 Assinatura RSA e Geração do DFe pelo PAA 5
5 Credenciamento de contribuintes 6
6 Série de emissão dos documentos 6
7 Estrutura das informações do PAA no XML dos DFe 6
8 Fluxo simplificado de funcionamento do PAA 7
9 Regras de Validação 8
Validações da Assinatura Digital do DFe 8
Validações do MDFe 8
Validações do Registro de Eventos (parte geral) 8
Validações do PAA (Sempre que informado infPAA em MDFe e Evento) 8

Histórico de Alterações / Cronograma

Versão	Histórico de atualizações	Implantação Homologação	Implantação Produção
1.01	• Consolidação das Regras de Validação relacionadas ao PAA	07/2026	08/2026

1 Provedor de Assinatura e Autorização

O contribuinte emitente de Documento Fiscal Eletrônico poderá utilizar os serviços de um Provedor de Assinatura e Autorização de Documentos Fiscais Eletrônicos - PAA com a finalidade de realizar comunicações com os sistemas de autorização de uso de documentos fiscais eletrônicos providos pelas administrações tributárias, em nome do contribuinte.

O ambiente de autorização das Administrações Tributárias através do Portal Nacional dos Documentos Fiscais Eletrônicos irá permitir a vinculação entre contribuintes que se enquadrarem nesse perfil (devidamente identificados na plataforma gov.br do governo federal) com Provedores de Assinatura e Autorização previamente homologados pela Coordenação do ENCAT.

O contribuinte deverá utilizar ferramenta de emissão de documento fiscal fornecida pelo PAA, preferencialmente na internet e com identificação do usuário.

2 Geração de XML com envio ao Ambiente de Autorização

O PAA receberá o pedido de emissão no formato que seu software estiver construído e providenciará a geração do XML do documento fiscal eletrônico preenchendo o grupo infPAA. Neste grupo será alimentada a tag SignaturaValue assinando o atributo Id do DFe com a chave criptográfica no padrão RSA fornecida pela administração tributária. O DFe também deverá receber a assinatura digital qualificada com certificado ICP-Brasil do PAA.

O PAA deverá transmitir o XML do DFe para o ambiente de autorização onde será submetido a todas as regras de validação estabelecidas no MOC. O documento poderá ser autorizado ou rejeitado, devendo o PAA guardar o protocolo de autorização e atuar nos casos em que houver rejeição.

3 Padrão de Certificado Digital para Assinatura Avançada

O certificado digital utilizado para assinatura avançada das mensagens seguirá padrão RSA (com par de chaves) gerados pela Plataforma de Emissão Simplificada para o usuário contribuinte que efetuar seu credenciamento e vinculação com o Provedor de Assinatura e Autorização no portal da SEFAZ Virtual RS identificando-se pelo usuário e senha da plataforma gov.br.

O PAA poderá obter o par de chaves pública e privada do seu usuário diretamente com ele ou obter de forma automatizada acessando o serviço DFeDistPAA descrito no Manual de Orientações do PAA (MOPAA).

Os certificados seguirão a especificação OpenSSL e serão gerados de forma única para a relação de cada PAA com o contribuinte vinculado no portal. A especificação produz um par de chaves (pública e privada) no formato PEM RSA 1024 bits.

As chaves são transformadas na estrutura RSA para assinatura digital XML com a seguinte definição:

1. Chave Privada RSA (PrivateKey):

#	Campo	Ele	Pai	Tipo	Ocor.	Descrição/Observação
Priv01	RSAKeyValue	G	Raiz	-	1-1	Chave Privada RSA
Priv02	Modulus	E	Priv01	Base64	1-1	
Priv03	Exponent	E	Priv01	C	1-1	Informar “AQAB”
Priv04	P	E	Priv01	Base64	1-1	
Priv05	Q	E	Priv01	Base64	1-1	
Priv06	DP	E	Priv01	Base64	1-1	
Priv07	DQ	E	Priv01	Base64	1-1	
Priv08	InverseQ	E	Priv01	Base64	1-1	
Priv09	D	E	Priv01	Base64	1-1	

2. Chave Pública RSA (PublicKey):

#	Campo	Ele	Pai	Tipo	Ocor.	Descrição/Observação
Pub01	RSAKeyValue	G	Raiz	-	1-1	Chave Pública RSA
Pub02	Modulus	E	Pub01	Base64	1-1	
Pub03	Exponent	E	Pub01	C	1-1	Informar “AQAB”

4 Assinatura RSA e Geração do DFe pelo PAA

A empresa usuária do serviço de Provedor de Assinatura e Autorização deverá solicitar o vínculo a um Provedor homologado no portal da SEFAZ Virtual RS, o resultado dessa solicitação entregará um par de chaves RSA (chave pública e chave privada) para o emitente.

Com a chave privada, a aplicação do PAA deverá assinar o conteúdo do atributo Id do MDFe / Evento (convertido para array de bytes) com padrão de assinatura assimétrica RSA SHA1 originando um SignatureValue no formato base64.

A chave pública deverá ser informada no grupo RSAKeyValue no padrão XML Signature para chaves RSA.
Passos a executar:

1. Responsável pela empresa deverá acessar o portal DFe da SVRS com seu CPF (login plataforma gov.br)
2. Solicitar o vínculo com o Provedor de Assinatura e Autorização disponibilizado pelo portal.
3. Obter no portal o par de chaves RSA (chave privada e chave pública)
4. Assinar o conteúdo da tag Id do DFe com a chave RSA (SHA1 base64) do usuário do PAA
5. Informar a chave pública no padrão XML Signature no grupo RSAKeyValue
6. Assinar o DFe com certificado X509 padrão ICP-Brasil do PAA
7. PAA deverá transmitir o DFe para o serviço de autorização da SVRS

A qualquer tempo o Emitente poderá solicitar o término do vínculo e utilização do PAA acessando o portal da SVRS. A administração tributária e o PAA também poderão comandar o encerramento do vínculo.

5 Credenciamento de contribuintes

Para o credenciamento, o PAA irá consultar o cadastro de emissores de DFe para validar se existe alguma restrição ou se o contribuinte já está credenciado.

Se o contribuinte não estiver credenciado, o portal do PAA irá direcionar o contribuinte para que este faça o credenciamento na sua UF de origem. Se houver alguma restrição, o contribuinte será informado que há restrição de emissão na sua UF de origem.

Após o credenciamento para emissão de DFe, estará disponível a utilização de PAA para este contribuinte.
Até o final de 2026, ou assim que operacional e tempestivamente disponíveis, serão utilizadas na solução do PAA, as informações cadastrais disponibilizadas pelo ambiente nacional de dados previsto no Art. 59 da LC 214/2025.

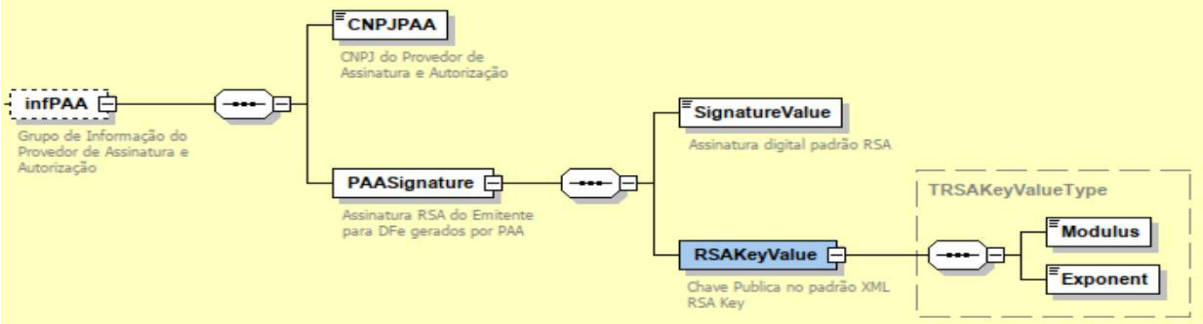
6 Série de emissão dos documentos.

Visando viabilizar a utilização de software emissor próprio e a emissão via PAA ou até mais de um PAA pelo contribuinte, é necessário fazer o controle da utilização da série do documento a fim de evitar duplicidade de documentos com mesma série e número.
Desta maneira, ao estabelecer o vínculo do PAA, o portal da SVRS irá atribuir àquele vínculo uma série específica que será utilizada pelo PAA para emitir os documentos daquele contribuinte.
A faixa de séries destinadas ao uso da emissão pelo PAA está designada entre 970 e 979, lembrando que cada série permitirá a emissão de até 999.999.999 documentos fiscais eletrônicos.

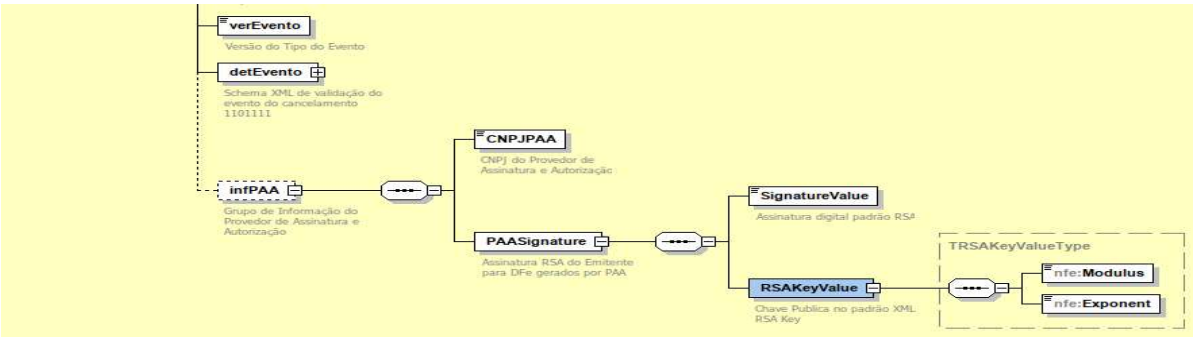
7 Estrutura das informações do PAA no XML dos DFe

Grupo/Elemento	Pai	Descrição	Elem	Tipo	Ocorr	Tam.	Observação
infPAA	**infMDFe**	**Grupo de Informação do Provedor de Assinatura e Autorização**	**G**		**0 - 1**		
CNPJPAA	infPAA	CNPJ do Provedor de Assinatura e Autorização	E	C	1 - 1	14	
PAASignature	infPAA	Assinatura RSA do Emitente para DFe gerados por PAA	G		1 - 1		
SignatureValue	PAASignature	Assinatura digital padrão RSA	E	C	1 - 1		Converter o atributo Id do DFe para array de bytes e assinar com a chave privada do RSA com algoritmo SHA1 gerando um valor no formato base64.
RSAKeyValue	PAASignature	Chave Pública no padrão XML RSA Key	G		1 - 1		
Modulus	RSAKeyValue		E	C	1 - 1		
Exponent	RSAKeyValue		E	C	1 - 1		

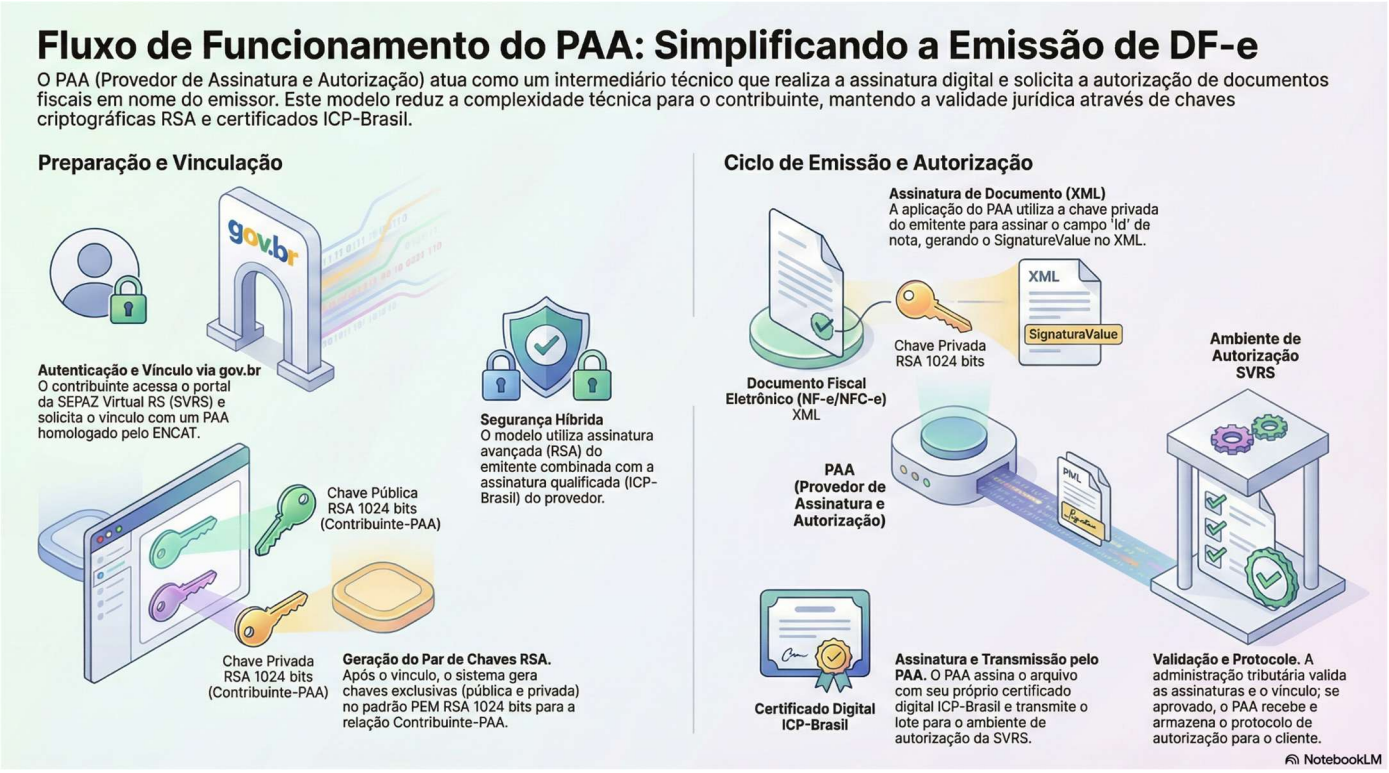
Esquema gráfico do leiaute contemplando o PAA.



Esquema gráfico do leiaute do evento contemplando o PAA.



8 Fluxo simplificado de funcionamento do PAA



9 Regras de Validação

Validações da Assinatura Digital do DFe

#	Regra de Validação	Aplic.	cStat	Efeito	Mensagem
F03	Se Certificado conter CNPJ do emitente: CNPJ-Base do Emitente difere do CNPJ-Base do Certificado Digital **Exceção:** Se a forma de emissão do MDFe for Regime Especial da Nota Fiscal Fácil, o CNPJ de assinatura será o e-CNPJ da SVRS para o serviço de recepção ou para os eventos do emitente (por exemplo: Cancelamento e encerramento) **Exceção 2**: Se o MDFe / Evento possuir indicação de uso do Provedor de Assinatura e Autorização (grupo: infPAA) esta regra não será aplicada.	Obrig.	213	Rej.	Rejeição: CNPJ-Base do Emitente difere do CNPJ-Base do Certificado Digital

Validações do MDFe

Regra de Validação	Aplic.	cStat	Efeito	Mensagem
Se o grupo de informações do Provedor de Assinatura e Autorização estiver informado (grupo: infPAA), o Processo de emissão (tag:ide/procEmi) deve ser 4- emissão de MDFe por Provedor de Assinatura e Autorização – PAA	Obrig.	910	Rej.	Rejeição: processo de emissão incompatível com PAA
Se o grupo de informações do Provedor de Assinatura e Autorização NÃO estiver informado (grupo: infPAA), o Processo de emissão (tag:ide/procEmi) deve ser DIFERENTE de 4- emissão de MDFe por Provedor de Assinatura e Autorização – PAA	Obrig.	911	Rej.	Rejeição: processo de emissão inválido para o MDFe
Se o grupo de informações do Provedor de Assinatura e Autorização e estiver informado (grupo: infPAA): A série de emissão do MDFe deverá estar na faixa 970-979 e atribuída ao vínculo entre o PAA e o emitente do MDFe	Obrig.	912	Rej.	Rejeição: Emissão por PAA com série inválida
IE Emitente deve ser informada (zeros ou nulo) **Exceção**: A IE não será informada se a forma de emissão (tpEmis) do MDFe for Regime Especial da Nota Fiscal Fácil (3) **Exceção 2:** Se MDFe gerado por PAA (grupo: infPAA) com procEmi =4, a IE do Emitente é opcional (MEI não inscrito na UF ou TAC Pessoa Física)	Obrig.	229	Rej.	Rejeição: IE do emitente não informada

Validações do Registro de Eventos (parte geral)

Regra de Validação	Aplic.	cStat	Efeito	Mensagem
O Processo de emissão do MDFe relacionado ao evento deve ser 4- emissão de MDFe por Provedor de Assinatura e Autorização – PAA	Obrig.	910	Rej.	Rejeição: processo de emissão incompatível com PAA
Se o grupo de informações do Provedor de Assinatura e Autorização estiver informado (grupo: infPAA): A série de emissão do MDFe deverá estar na faixa 970-979 e atribuída ao vínculo entre o PAA e o emitente do MDFe	Obrig.	912	Rej.	Rejeição: Emissão por PAA com série inválida

Validações do PAA (Sempre que informado infPAA em MDFe e Evento)

#	Regra de Validação	Aplic.	cStat	Efeito	Mensagem
PAA01	Se o grupo de informações do Provedor de Assinatura e Autorização estiver informado (grupo: infPAA), o CNPJ do PAA dever ser válido (zeros, DV)	Obrig.	914	Rej.	Rejeição: CNPJ do PAA inválido
PAA02	Se o grupo de informações do Provedor de Assinatura e Autorização estiver informado (grupo: infPAA): Verificar se o CNPJ do PAA (tag: CNPJPAA) existe na relação de Provedores de Autorização e Assinatura homologados pelo ENCAT	Obrig	915	Rej.	Rejeição: Provedor de Assinatura e Autorização não existe na base da SEFAZ
PAA03	Se o grupo de informações do Provedor de Assinatura e Autorização estiver informado (grupo: infPAA): Verificar se o Emitente (tag: CNPJ/CPF grupo emit) possui vínculo ativo com o PAA (tag: CNPJPAA)	Obrig.	916	Rej.	Rejeição: Emitente não associado ao PAA
PAA04	Se o grupo de informações do Provedor de Assinatura e Autorização estiver informado (grupo: infPAA):	Obrig.	917	Rej.	Rejeição: Emissão por PAA deve ser assinada pelo CNPJ do Provedor de Assinatura

	O CNPJ do certificado de assinatura DEVE ser igual ao CNPJ do PAA				
PAA05	Se o grupo de informações do Provedor de Assinatura e Autorização estiver informado (grupo: infPAA): Validar assinatura RSA (tag:SignatureValue) com a chave pública do emitente (grupo: RSAKeyValue)	Obrig.	959	Rej.	Rejeição: Assinatura RSA inválida