Projeto Conhecimento de Transporte Eletrônico

Nota Técnica **2024.003**

Consolidação da especificação do PAA

Versão 1.00 – setembro de 2024

ENCAT
Encontro Nacional de Coordenadores e Administradores Tributários Estaduais

Sumário

Histórico de Alterações / Cronograma

Versão	Histórico de atualizações	Implantação Homologação	Implantação Produção
1.00	• Consolidação das Regras de Validação relacionadas ao PAA		

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.
O Provedor de Assinatura e Autorização poderá optar pelos seguintes modelos de autorização:

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.

Plataforma de Emissão Simplificada (PES): Nas hipóteses de emissão contempladas no Manual de Orientações do Provedor de Assinatura e Autorização v1.00 (disponível em https://dfe-portal.svrs.rs.gov.br/pes) o PAA poderá optar por utilizar os serviços da plataforma de emissão, sistema no qual o PAA deverá enviar um pedido de emissão aos webservices descritos na plataforma contendo dados comerciais da prestação do serviço, delegando ao sistema PES a geração do XML e posterior autorização do documento fiscal. Nesse modelo ampliado da Nota Fiscal Fácil, o PAA deverá gerar a

assinatura do contribuinte da mesma forma utilizando a chave RSA fornecida pela Administração Tributária e assinar o pedido de emissão com seu certificado digital. O XML final do documento fiscal, gerado pela PES, terá a assinatura RSA do contribuinte na tag SignatureValue (grupo infPAA), o pedido de emissão do PAA na tag xSolic (grupo NFF) assinado pelo PAA e a assinatura qualificada com o certificado digital da SVRS na assinatura padrão do DFe.

2 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 a operação ObterDadosTAC do serviço PESAdmin da Plataforma de Emissão Simplificada.

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:

2.1 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	

2.2 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”

3 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 CTe / 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 devera 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.

Observação: O processo de assinatura e envio do pedido de emissão na plataforma de emissão simplificada está disciplinado no Manual de Orientações do PAA – MOPAA disponível em https://dfe-portal.svrs.rs.gov.br/pes.

4 Estrutura das informações do PAA no XML do DFe

Grupo/Elemento	Pai	Descrição	Elem	Tipo	Ocorr	Tam.	Observação
infPAA	**infCte**	**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		

5 Regras de Validação (CTe e CTe Simplificado)

5.1 Grupo E: Validações da Assinatura Digital do DFe

#	Regra de Validação	Aplic.	cStat	Efeito	Mensagem
E03	Se Certificado conter CNPJ do emitente: CNPJ-Base do Emitente deverá ser o mesmo CNPJ-Base do Certificado Digital **Exceção**: Se a forma de emissão do CTe 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 de emitente (por exemplo: Cancelamento e comprovante de entrega) **Exceção 2:** O evento Prestação de Serviço em desacordo poderá ser assinado pelo certificado digital da SVRS/PROCERGS quando usuário estiver identificado pela plataforma gov.br, nesse caso essa regra não deverá ser aplicada. **Exceção 3:** Se o CTe ou CTe Simplificado (modelo 57) / Evento possuir indicação de uso do Provedor de Assinatura e Autorização (grupo: infPAA preenchido) esta regra não será aplicada.	Obrig.	213	Rej.	Rejeição: CNPJ-Base do Emitente difere do CNPJ-Base do Certificado Digital

5.2 Grupo E-2: Validações do PAA

#	Regra de Validação	Aplic.	cStat	Efeito	Mensagem
PAA00	Se o grupo de informações do Provedor de Assinatura e Autorização estiver informado (grupo: infPAA), o ambiente de autorização do CTe deverá ser o da SEFAZ Virtual RS	Obrig.	916	Rej.	Rejeição: Ambiente de autorização inválido para emissão pelo PAA.
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.	909	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	911	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.	912	Rej.	Rejeição: Emitente não associado ao PAA
PAA04	Se o grupo de informações do Provedor de Assinatura e Autorização estiver informado (grupo: infPAA) e o CNPJ do certificado de assinatura for da SVRS: o tipo de emissão do CTe deve ser Regime Especial da Nota Fiscal Fácil (tpEmis-3)	Obrig.	910	Rej.	Rejeição: Emissão por PAA deve ser do tipo e emissão Nota Fiscal Fácil quando gerado pela Plataforma de Emissão
PAA05	Se o grupo de informações do Provedor de Assinatura e Autorização estiver informado (grupo: infPAA) e o CNPJ do certificado de assinatura for diferente da SVRS, o CNPJ do certificado de assinatura DEVE ser igual ao CNPJ do PAA		915	Rej.	Rejeição: Emissão por PAA deve ser assinada pelo CNPJ do Provedor de Assinatura
PAA06	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.	914	Rej.	Rejeição: Assinatura RSA inválida

5.3 Validação do CTe

G105	IE Emitente deve ser informada (zeros ou nulo) **Exceção:** A IE não será informada se a forma de emissão (tpEmis) do CTe for Regime Especial da Nota Fiscal Fácil (3) **Exceção 2:** Se CTe gerado por PAA (grupo: infPAA) a IE do Emitente é opcional (MEI não inscrito na UF ou TAC Pessoa Física)	Obrig.	229	Rej.	Rejeição: IE do emitente não informada

5.4 Validações do evento de cancelamento

O02	Emitente deve estar habilitado na base de dados para emissão do CTe **Exceção**: Esta regra não será aplicada quando a forma de emissão do CTe (tpEmis) for Regime Especial da Nota Fiscal Fácil (3) ou quando CTe gerado por PAA	Obrig.	203	Rej.	Rejeição: Emissor não habilitado para emissão do CTe