

Comunicado Técnico: Padronização de Assinatura Digital (XML Digital Signature)

Prezado Desenvolvedor,

Para garantir a integridade e o sucesso na validação das assinaturas digitais no novo Web Service de emissão de NFS-e (IssWebWSNacional), estamos estabelecendo uma diretriz técnica quanto ao algoritmo de canonicalização utilizado nos documentos XML enviados.

Recomendação de Algoritmo

Solicitamos que todas as assinaturas digitais passem a utilizar, preferencialmente, o **Exclusive Canonicalization Algorithm**:

- **Identificador:** <http://www.w3.org/2001/10/xml-exc-c14n#>

Por que utilizar o Exclusive Canonicalization?

Como nossa comunicação é baseada no protocolo **SOAP**, o documento XML assinado trafega dentro de um "envelope" (Body). O uso do algoritmo de canonicalização *inclusivo* pode causar falhas na validação da assinatura se o ambiente de recepção herdar namespaces ou atributos do envelope SOAP original.

Ao utilizar o modo **Exclusive**, garantimos que:

- A validação considere **apenas os elementos internos** ao trecho assinado.
- Seja evitada a quebra da assinatura por mudanças no contexto XML externo (como prefixos de namespace do envelope).
- Haja maior interoperabilidade entre diferentes plataformas e bibliotecas de segurança.

Exemplo de implementação no XML

Certifique-se de que a tag <CanonicalizationMethod> em seu XML reflita esta configuração:

```
<Reference URI="#ID_DO_ELEMENTO">  
  <Transforms>  
    <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />  
    ...  
  </Transforms>  
  ...  
</Reference>
```

Nota: Pedimos que revisem suas rotinas de assinatura o quanto antes para evitar rejeições intermitentes em ambientes de produção.