serpro.gov.br

Receita Integra
Documentação Técnica

Versão do Documento – 1.4

Última Atualização - 17/07/2026

Sumário

Receita Integra

A plataforma Receita Integra tem como objetivo padronizar o acesso externo às soluções de interoperabilidade de dados disponibilizadas para entidades e usuários externos à Receita Federal.

A iniciativa busca estabelecer um modelo único de integração, promovendo governança, rastreabilidade, segurança e conformidade no consumo de serviços. Para isso, foram adotados protocolos amplamente reconhecidos e consolidados no mercado, como o OAuth 2.0, utilizado para autorização segura e controle de acesso, garantindo que apenas aplicações devidamente autenticadas e autorizadas possam consumir os recursos disponibilizados.

Esse documento tem como objetivo descrever tecnicamente os aspectos técnicos e de segurança implementados, bem como as estruturas de dados envolvidas nesse compartilhamento.

Autenticação e Autorização (OAuth 2.0)

As APIs disponibilizadas utilizam o padrão OAuth 2.0, conforme a RFC 6749, com uso de Bearer Tokens (RFC 6750) e TLS (HTTPS) para proteção do transporte das informações.

O modelo adotado é o Client Credentials Flow, indicado para comunicação máquina-a-máquina (M2M), sem interação de usuário final.

Credenciais de Acesso

A credencial de acesso é obtida por meio do serviço "Gerar Credencial de Acesso para API", disponível no Portal Serviços da Receita Federal (https://serviços.receitafederal.gov.br) e Portal Nacional da Tributação de Bens e Serviços (https://consumo.tributos.gov.br).

Para gerar a credencial, o usuário precisa estar autenticado com a conta gov.br e, caso não seja utilizado certificado digital e-CNPJ, representar a pessoa jurídica (representante ou procurador) para quem a credencial será gerada.

Cada empresa receberá um conjunto de credenciais composto por:

- client_id
- client_secret

Essas credenciais são utilizadas exclusivamente para obtenção do token de acesso junto ao Authorization Server. Os tokens tem duração de 1 (uma) hora e existe um limite de 2 (dois) tokens por hora. Deverá ser implementado um cache para reutilização do token.

Envio do Token

Após a obtenção do token, todas as chamadas devem incluir o cabeçalho HTTP:

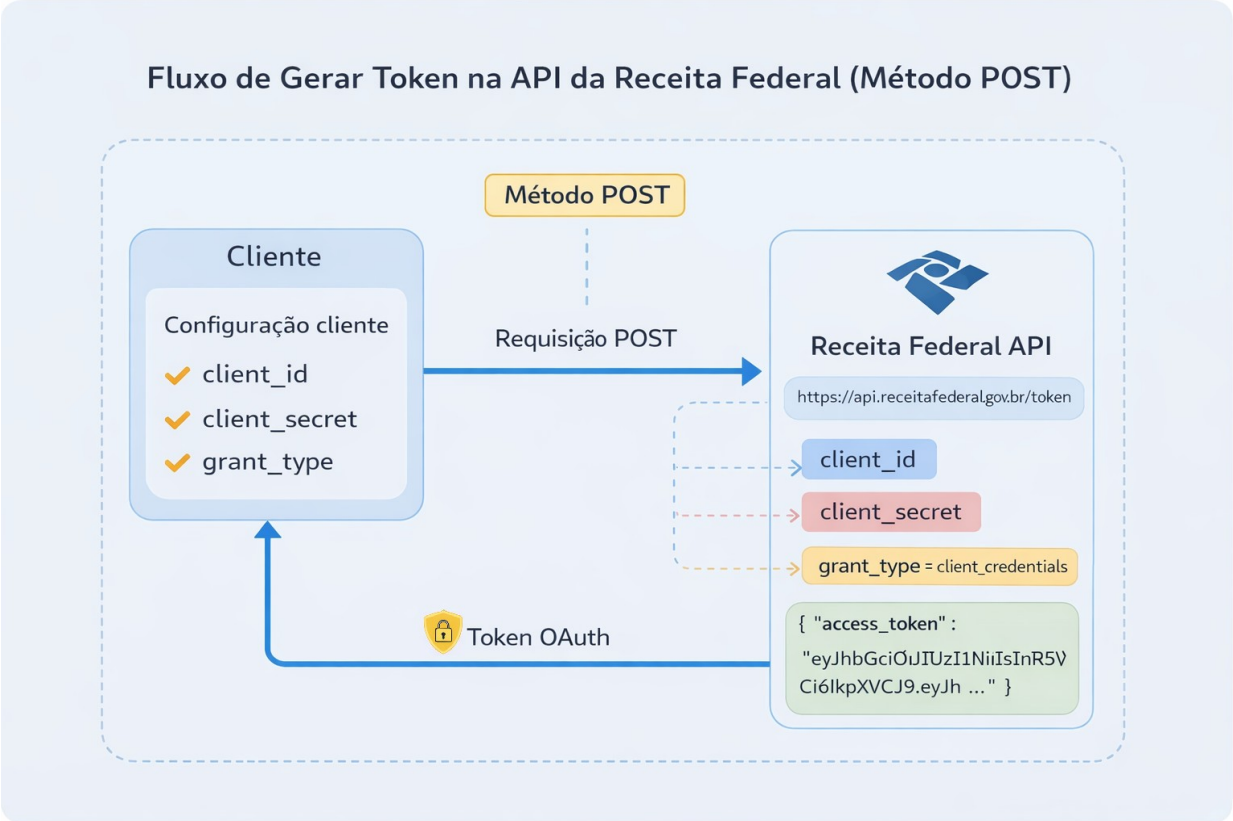
```
Authorization: Bearer <access_token>
```

Tokens enviados fora desse padrão ou ausentes resultarão em erro de autenticação.

Ambientes

Ambiente	Authorization Server (OAuth)
Produção	`https://api.receitafederal.gov.br/token`

Diagrama



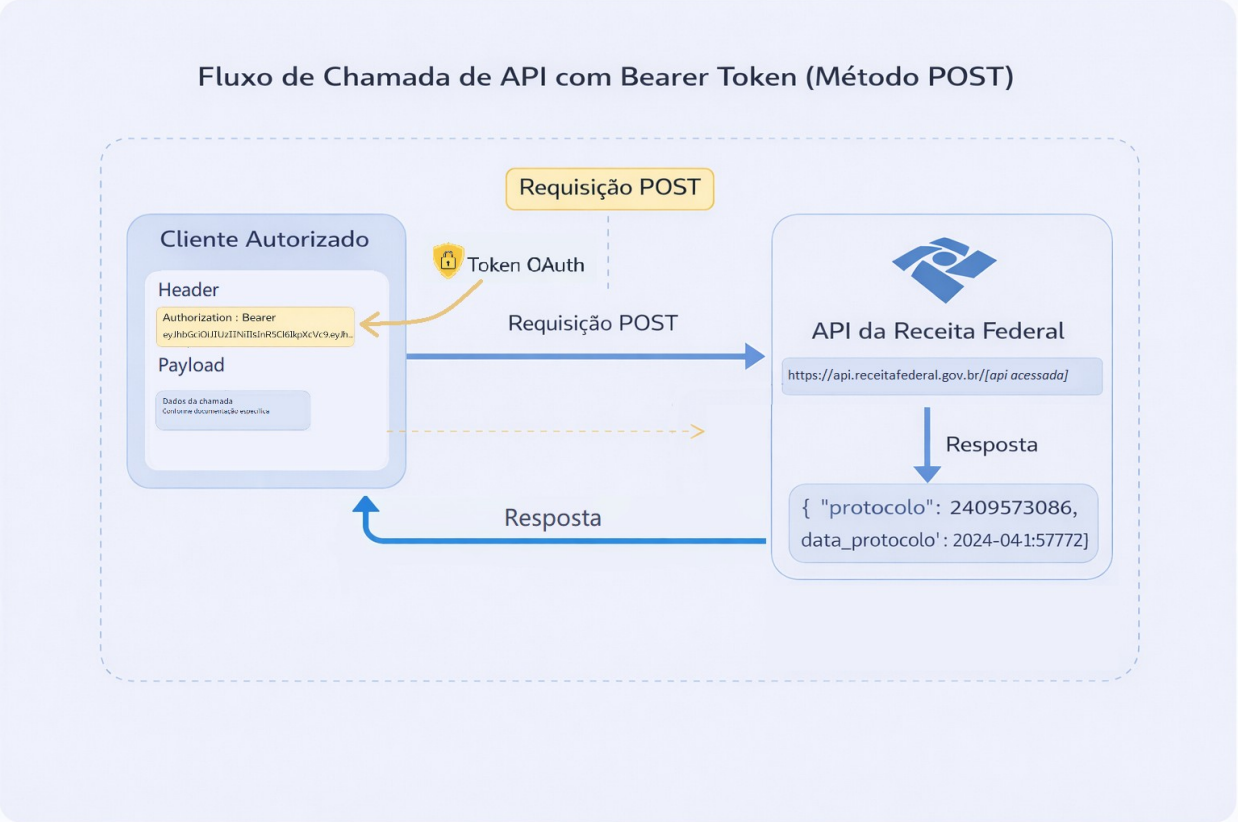


Tabela de Erros

A solução adota códigos de status HTTP padronizados para sinalização de erros, os quais podem ser retornados tanto pela camada de gerenciamento de APIs (API Gateway) quanto pelos serviços backend, conforme o estágio de processamento da requisição.

Código HTTP	Descrição	Possível Causa
400	Bad Request	Requisição malformada ou parâmetros inválidos
401	Unauthorized	Token de acesso ausente, inválido ou expirado
403	Forbidden	Token válido, porém, sem escopo ou permissão para acesso ao recurso
404	Not Found	Endpoint inexistente ou recurso não disponível
429	Too Many Requests	Limite de requisições excedido, conforme políticas de rate limit configuradas
500	Internal Server Error	Erro interno durante o processamento da requisição

Aspectos de Segurança

O acesso às APIs é protegido por meio do protocolo OAuth 2.0, utilizando o fluxo client_credentials, garantindo autenticação segura entre sistemas (machine-to-machine).

A obtenção do token de acesso ocorre exclusivamente via método HTTP POST, sobre conexão HTTPS, assegurando a confidencialidade e integridade das credenciais de autenticação. O Bearer Token emitido possui validade inicialmente configurada para 60 (sessenta) minutos e deve ser encaminhado em todas as requisições subsequentes no cabeçalho HTTP Authorization, no formato:

```
Authorization: Bearer <token>
```

Essa abordagem evita a exposição de informações sensíveis em URLs ou corpos de mensagens. Antes de processar qualquer requisição, a API realiza a validação completa do token, incluindo verificação de assinatura, prazo de expiração e escopos autorizados.

Como resposta às requisições válidas, a API retorna exclusivamente um identificador de protocolo, não expondo dados sensíveis no payload de resposta.

Recomenda-se que o gerenciamento de credenciais e tokens seja realizado exclusivamente em ambientes de backend, com adoção de cofres seguros (secret vaults), controle de acesso restrito e políticas de rotação periódica de credenciais, em conformidade com as boas práticas de segurança da informação e normas vigentes.