



GESTÃO · INTEGRAÇÃO · TECNOLOGIA

PLAYBOOK DE OPERAÇÕES

Configuração de Certificado para API Bradesco

Integração de Boleto via API com autenticação mTLS

Este POP descreve o procedimento padrão para preparar os arquivos de certificado necessários para uma nova implantação da integração de Boleto do Bradesco via API, utilizando autenticação mTLS.

Configuração de Certificado para API Bradesco

Ao final do procedimento serão gerados os arquivos certificado.crt, o certificado público utilizado pela API, e certificado.key, a chave privada correspondente. O arquivo .pfx original deve ser mantido guardado de forma segura como backup. Observação: em alguns casos o sistema pode aceitar o certificado em formato PEM com extensão .crt.

mTLS

AUTENTICAÇÃO

Certificado digital A1

.CRT e .KEY

SAÍDA

Backup .PFX protegido

Portal Developers

CREDENCIAIS

Client ID e Client Secret

Fluxo de Requisição

Exportar

Exportar .PFX com
chave privada



Gerar

Gerar .CRT/.PEM e
.KEY



Configurar

Informar caminhos
no sistema



Testar

Token OAuth e
registro do boleto

Preparação dos Certificados

1

Exportar o certificado do Windows

Abrir o gerenciador de certificados do Windows e localizar o certificado digital correto da empresa. Botão direito → Todas as Tarefas → Exportar.

Selecionar "Sim, exportar a chave privada" e o formato Troca de Informações Pessoais – PKCS nº 12 (.PFX).

Incluir os certificados no caminho de certificação, se disponível, definir uma senha forte para proteger o .PFX e salvar, por exemplo, como pfxEmpresa.pfx.

2

Organizar a pasta de trabalho

Criar a pasta C:\cert\NOME_CLIENTE\ e copiar o arquivo .PFX para ela, ou trabalhar temporariamente em uma pasta segura.

3

Gerar o certificado .CRT

No Prompt de Comando, na pasta do arquivo .PFX, executar o comando abaixo.

Será solicitada a senha definida para o arquivo .PFX. Alternativamente, gerar em formato PEM.

COMANDO

```
01 openssl pkcs12 -in pfxEmpresa.pfx -clcerts -nokeys -out certificado.crt
02 openssl pkcs12 -in pfxEmpresa.pfx -clcerts -nokeys -out certificado.pem
```

4

Gerar a chave privada .KEY

A opção -nodes gera a chave privada sem senha. Isso pode ser necessário quando o componente da integração não possui campo para informar a senha da chave privada.

COMANDO

```
01 openssl pkcs12 -in pfxEmpresa.pfx -nocerts -nodes -out certificado.key
```

Configuração e Validação

5

Estrutura final da pasta

A pasta C:\cert\NOME_CLIENTE\ deve conter certificado.crt, certificado.key e o pfxEmpresa.pfx como backup protegido.

6

Configurar no sistema

No cadastro da integração no sistema BR Sistemas, informar o Client ID, o Client Secret, o Certificado API (caminho completo do .CRT/.PEM) e o Certificado Privado API (caminho completo da chave .KEY).

7

Validar os arquivos

Validar o certificado e a chave privada com o OpenSSL.

COMANDO

```
01 openssl x509 -in C:\cert\NOME_CLIENTE\certificado.crt -noout -subject -issuer -dates
02 openssl pkey -in C:\cert\NOME_CLIENTE\certificado.key -noout -check
```

8

Testar a autenticação

Realizar o teste da API. O resultado esperado é HTTP 200 OK com access_token.

COMANDO

```
01 POST https://openapi.bradesco.com.br/auth/server-mtls/v2/token
```

Pontos importantes

- ✓ 401 – SSL with client authentication is required: certificado mTLS não configurado ou não apresentado na conexão
- ✓ fopen: No such file or directory: verificar caminho, nome e extensão dos arquivos .crt e .key
- ✓ 403 Forbidden após token: verificar permissão da aplicação e vínculo do contrato
- ✓ Valor decimal inválido: valores monetários com no máximo duas casas decimais

Checklist de Validação

E-mail Bradesco

- ✓ Confirmar o e-mail cadastrado

Portal Developers

- ✓ Cadastrar ou acessar a empresa

Aplicação

- ✓ Habilitar a aplicação/API correspondente

Credenciais

- ✓ Obter Client ID e Client Secret

Certificado A1

- ✓ Exportar com chave privada

Arquivo .PFX

- ✓ Gerar protegido por senha

Certificado .CRT

- ✓ Gerar a partir do .PFX

Chave privada .KEY

- ✓ Gerar a partir do .PFX

Pasta de certificados

- ✓ Criar C:\cert\NOME_CLIENTE\

Caminhos no sistema

- ✓ Configurar certificado e chave

Token OAuth

- ✓ Testar a obtenção do token mTLS

Registro do boleto

- ✓ Testar o registro do boleto

Valores monetários

- ✓ Usar no máximo duas casas decimais

Backup seguro

- ✓ Guardar .PFX e senhas em local seguro

Logs

- ✓ Nunca registrar Client Secret ou chave privada