Milersoft

PIX SICOOB

Configuração do pagamento digital PIX com o banco SICOOB

Para iniciar a configuração do PIX é necessario que o proprietario da loja entre no site https://developers.sicoob.com.br e efetue o cadastro para uso da API.

Após efetuar o cadastro anote as informações:

- **Nome do cooperado:**
- **Client ID:**
- **Geração do access token: https://auth.sicoob.com.br/auth/realms/cooperado/protocol/openid-connect**
- **URL: https://apis.sicoob.com.br/cooperado/pix/api/v2**

Agora deve ser gerado o certificado **PEN** e **KEY** conforme se encontra no manual da SICOOB.

Como extrair a chave pública (.PEM) do seu certificado

Realizar o download dos seguintes arquivos “openssl” através do endereço http://downloads.sourceforge.net/gnuwin32/openssl-0.9.8h-1-setup.exe

- Extrair os arquivos em uma pasta desejada, de preferência na raiz, exemplo: **“C:\openssl”**
- Abra o Prompt de comando do Windows. Para isso basta digitar “**cmd**” e pressionar Enter na barra de pesquisa ou na opção executar (teclas **Win+R**):
- Crie uma pasta temporária para armazenar os certificados, exemplo **c:\openssl\certificados**
Nota: lembrar de copiar o arquivo certificado.pfx para esta nova pasta.
- Dentro do **CMD**, acessar a pasta bin onde o openssl foi extraído, exemplo:
cd c:\openssl\bin
- Executar o comando para extração da chave privada certificado.**key** que será fornecida à equipe de desenvolvimento (ou terceirizado):
openssl pkcs12 -in c:\openssl\certificados\certificado.pfx -nocerts -out c:\openssl\certificados\certificado.key
Nota: neste passo será solicitado a senha do arquivo certificado.pfx e em seguida, será necessário informar uma nova senha exclusiva para o certificado.key. Exemplo do arquivo gerado:
-Executar o comando para extração da chave pública certificado.**pem** que será fornecida à equipe de desenvolvimento e ao Sicoob:
openssl pkcs12 -in c:\openssl\certificados\certificado.pfx -clcerts -nokeys -out c:\openssl\certificados\certificado.pem
Nota: neste passo também será solicitado a senha do arquivo certificado.pfx. Exemplo do certificado

gerado:
- Validar o algoritmo md5 para validar as chaves:
openssl x509 -noout -modulus -in c:\openssl\certificados\certificado.pem | openssl md5
Anotar o resultado.
openssl rsa -noout -modulus -in c:\openss\certificados\certificado.key | openssl md5
Anotar o resultado.
Nota: Se os códigos md5 não forem iguais, ou a senha foi informada indevidamente durante a geração dos certificados e precisará reiniciar o procedimento.
- Salvar os arquivos gerados na pasta c:\siga do servidor e em cada PDV.

-Abra o servidor, entre em configuração do sistema e preencha as informações em **Forma de Pegamentos Digitais**;
Preencher os campos:
- Nome do Banco: SICOOB
- Base URL: **https://api.sicoob.com.br/pix/api/v2**
- OAuth URL: **https://auth.sicoob.com.br/auth/realms/cooperado/protocol/openid-connect**
- Chave PIX: "Preencher chave PIX da loja"
- Recebedor: "Preencher com a informação do 1º processo, campo **Nome do cooperador**"
- Cidade: "Preencher com a cidade do cliente"
- APP Key: "Deixar **Vazio**, não preencher"
- Client ID: "Preencher com a informação do 1º processo, campo **Client ID**"
- Client Secret: "Deixar **Vazio**, não preencher"
- Tipo de Certificado: Deixa selecionado "**Certificado/Chave**"
- Certificado: Selecionar o certificado .**PEN** que foi gerado no processo acima.
- Chave Privada: Selecionar o certificado .KEY que foi gerado no processo acima.