Guia Técnico Integrações

API Pix Sicredi

Sumário

1. Apresentação

O Pix é um arranjo de pagamentos que possibilita pagar e transferir, 24 horas por dia, 365 dias no ano, inclusive aos finais de semana e feriados, com liquidação imediata. A API Pix permitirá integração com diversos negócios que desejam oferecer o Pix como forma de pagamento, automatizando o processo de recebimento com segurança, rapidez e maior facilidade.

2. Objetivo

Este guia tem como objetivo estabelecer as recomendações e condições de negócio para adesão e implementação da API Pix no Sicredi, bem como indicar os principais requisitos técnicos, detalhando as informações relativas a acesso, autenticação e integração, servindo de base aos integradores técnicos para desenvolvimento desta aplicação no ambiente de automação comercial dos associados.

3. Público-alvo da solução de integração

Associados PJ que buscam realizar integração da API Pix junto ao Sicredi, a fim de viabilizar a automatização de recebimento de cobranças em casos de negócio focados em pagamentos imediatos e com vencimentos futuros.

4. Funcionalidades da API Pix

- Gerenciamento de Cobrança
    - Criar Cobrança
    - Revisar cobrança
    - Consultar Cobrança
    - Consultar Lista de Cobranças
- Gerenciamento de Pix recebidos
    - Solicitar devolução
    - Consultar devolução
    - Consultar Pix
    - Consultar Pix Recebidos
- Gerenciamento de Notificações
    - Configurar o Webhook Pix
    - Callback

- Exibir informações acerca do Webhook Pix
- Cancelar o Webhook Pix

5. Jornada de adesão e implementação Sicredi

Por jornada de adesão, entende-se o processo por meio do qual um usuário recebedor passa a utilizar os serviços de um PSP específico. Do ponto de vista da API Pix, tal processo deve incluir o fornecimento de credenciais de acesso (Client_ID e Client_Secret) e de certificados ao usuário recebedor. O Sicredi, como PSP participante do arranjo Pix, tem autonomia para definir a jornada de adesão para os seus associados, utilizando os canais que julgar mais adequados.

O usuário que deseja integrar-se com a API Pix no Sicredi deve, como premissa seguir as seguintes orientações:

- Possuir chave(s) Pix vinculada(s) a conta corrente ou poupança no Sicredi.
- Possuir dados de telefone celular e e-mail atualizados no seu cadastro junto à cooperativa.
- Possuir todas as configurações do seu software de automação e conciliação de pagamentos de acordo com as especificações e detalhamentos indicados no link do Manual de Padrões para Iniciação do Pix do Banco Central do Brasil, constante na seção - Documentação do Bacen em relação à API Pix.

6. Passo a passo da jornada no Sicredi

Como primeiro passo, o associado deve entrar em contato com sua cooperativa, solicitando a adesão para integração com a API Pix no Sicredi.

Neste contato, serão esclarecidas ao associado as etapas do processo de integração, sendo fornecido o presente documento, que deve ser o guia para que a empresa realize o desenvolvimento necessário, incluindo funcionalidades e requisitos de segurança, tornando-se assim apta para o processo de integração ao arranjo Pix.

Ainda para a adesão, a cooperativa necessitará, junto ao associado, coletar algumas informações a fim de subsidiar análises para o atendimento da demanda. Estes dados deverão ser informados em formulário específico, conforme fluxo interno junto ao time responsável pelo apoio às Integrações de API.

Após realizada toda a análise de negócio pela cooperativa, um termo de adesão deverá ser assinado entre as partes.

Finalizada esta etapa de adesão, ocorrerão marcos de implementação técnica via Internet Banking.

7. Implementação via Internet Banking

Atenção: os passos a seguir devem ser realizados no Internet Banking pelo associado com acesso à conta e com perfil de usuário "Master".

1. **Upload de arquivo CSR (Certificate Signing Request)**
   - Acessar o Internet Banking *https://www.sicredi.com.br/* com os dados de cooperativa e conta, clicar no menu **Outros Serviços / Acesso API Pix / Gerenciar Certificados** e realizar o *upload* do arquivo CSR (*Certificate Signing Request*).

O arquivo enviado será recebido pelo Sicredi e avaliado dentro do nosso perímetro de segurança. Com as informações validadas, dentro do prazo informado no IB, será disponibilizado o certificado digital assinado, necessário para a correta implementação.

No **Anexo I** deste Guia, está disponível um passo-a-passo com as instruções técnicas necessárias para a geração deste arquivo.

2. **Download do certificado digital assinado pelo Sicredi**
   - Acessar o Internet Banking *https://www.sicredi.com.br/* com os dados de cooperativa e conta, clicar no menu **Outros Serviços / Acesso API Pix / Gerenciar Certificados** e realizar o *download* dos arquivos disponibilizados:
     - ✓ Certificado Digital .CER
     - ✓ Cadeia de Certificados Completa Sicredi .CER

Observação: Caso os arquivos mencionados acima forem disponibilizados com conteúdo DER, pode ser necessária a realização de conversão do conteúdo, visto que algumas aplicações de mercado, como por exemplo, **Postman** *e* **cURL**, utilizam no formato **PEM**.
Como exemplo, segue comando para este processo:

```
openssl x509 -inform der -in certnew.cer -out certificate.pem
```

3. **Geração das credenciais de acesso padrão OAUTH2.0 (*Client_id* e *Client_Secret*)**

   - Acessar o Internet Banking *https://www.sicredi.com.br/* com os dados de cooperativa e conta, clicar no menu **Outros Serviços / Acesso API Pix / Gerar Credenciais**, e na lista **Certificado/Provedor**, selecionar o **certificado aprovado** e o Ambiente Virtual*, dando o 'aceite' aos Termos de Uso para avançar e informar os dados de assinatura eletrônica para o *Client_ID* e o *Client_Secret* sejam concedidos.

***Ambiente Virtual:**

- **Homologação** (ambiente de testes e validações): Selecionando este ambiente, as credenciais (*Client_id* e *Client_Secret*) serão disponibilizadas para uso em URL de homologação. O acesso a este ambiente deve ser direcionado para testes, caso o responsável técnico pela integração julgue necessário realizar validações do seu sistema, antes de realizar o acesso em produção.
- **Produção** (ambiente de armazenamento de dados): Selecionando este ambiente, as credenciais (*Client_id* e *Client_Secret*) serão disponibilizadas para uso em URL de produção. O acesso a este ambiente é direcionado diretamente para ambiente produtivo.

Os testes não são obrigatórios. A escolha do ambiente fica a critério do associado, conforme orientações do responsável técnico da integração. Caso opte-se pela realização de homologação, orientamos testes conforme seção **9. Testes Opcionais**, deste guia.

Ambas as URLs estão descritas na seção **8. Fluxo de Requisições da API Pix Sicredi** deste guia.

8. Fluxo de Requisições da API Pix Sicredi

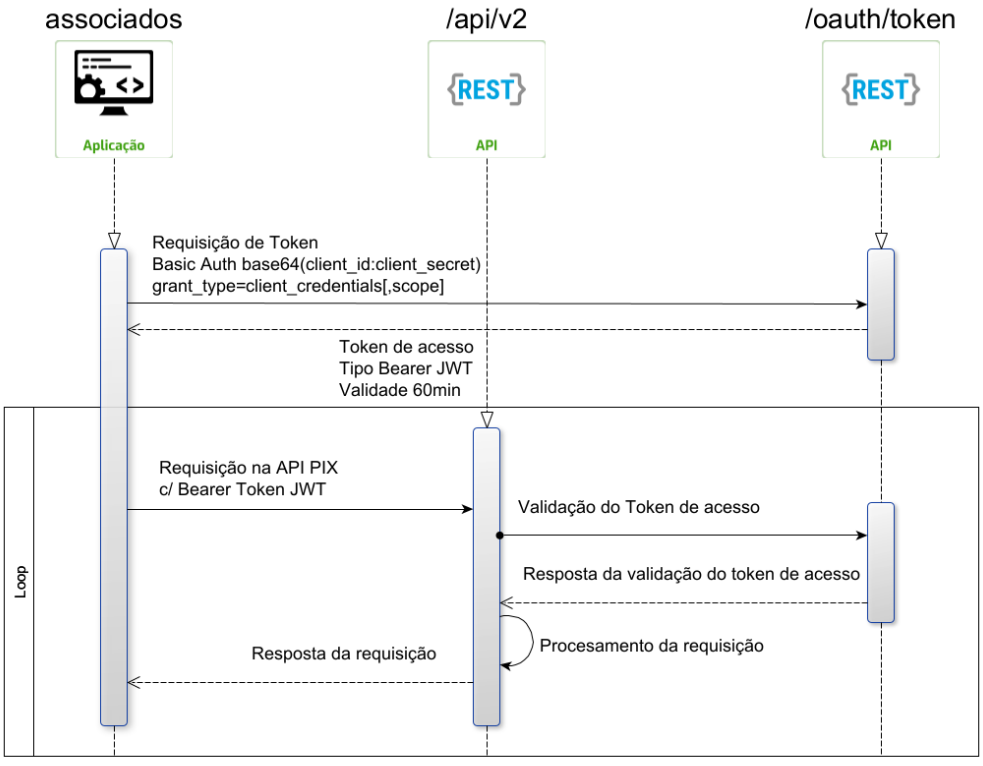
Como orientação inicial, informamos que **todas as chamadas da API Pix devem ser feitas utilizando criptografia TLS** com autenticação mútua no estabelecimento da conexão, de posse dos seguintes itens:

- Certificado digital *.CER* (disponibilizado através do Internet Banking Sicredi);
- Chave *APLICACAO.KEY* gerada pra fazer a requisição do certificado;
- Cadeia completa (disponibilizado através do Internet Banking Sicredi).

Importante:

- Recomendamos que seja realizado um entendimento por parte do responsável técnico sobre **conexões mTLS**, que é o padrão utilizado pelo Banco Central na API Pix.
- Para auxiliar na configuração das chamadas da API, caso seja utilizada a ferramenta **Postman**, temos o **Anexo II**, contendo o passo-a-passo de configuração mTLS nesta ferramenta, e o **Anexo III**, indicando instruções de uso de uma collection de requisições da API Pix Sicredi.

A API Pix Sicredi segue o fluxo de autenticação *OAuth 2.0-Client Credentials Flow*, como especificado pelo Bacen, como apresentado no diagrama abaixo.



Primeiramente, é necessário realizar a requisição do token de acesso (/oauth/token), com as credenciais Client Id e Client Secret. Utilizando esse token de acesso, a aplicação do associado estará apta a realizar requisições no servidor de recursos (/api/v2).

Abaixo, recomendações que devem ser seguidas para a chamada da API Pix utilizando o contexto da documentação do Bacen, disponíveis pelo link https://bacen.github.io/pix-api/#/.

- **Servidor de autenticação – para requisitar o token de acesso:**

Deverá ser gerado um *token* no padrão JWT a partir do Servidor de Autorização da API Pix (padrão OAuth2) utilizando suas credenciais de acesso (*client_id:client_secret*), requisitando o endpoint *POST /oauth/token*.

Seguem detalhes sobre a requisição para geração do token JWT:

POST /oauth/token	
HEADER	
Key	Value
Authorization	Basic Base64(client_id:client_secret)
Content-type	application/x-www-form-urlencoded

O valor do *Authorization Header* deve conter o valor "*Basic*", seguido do *client_id* e *client_secret*, separados pelo caracter **:** (dois-pontos) e codificadas em base 64.

BODY	
Key	Value
grant_type	client_credentials
scope	cob.read+cob.write+pix.read

O campo *scope* deve conter a lista de escopos (acessos) desejados no momento da geração do *token* JWT. A separação dos escopos deve ser por um espaço em branco.

Exemplos:

- **Homologação:** https://api-pix-h.sicredi.com.br/oauth/token

```
curl --location --request POST 'https://api-pix-h.sicredi.com.br/oauth/token' \
--header 'Content-Type: application/x-www-form-urlencoded' \
--header 'Authorization: Basic Q0xJRU5UX0lEOkNMSUVOVF9TRUNSRVQ=' \
--data-urlencode 'grant_type=client_credentials' \
--data-urlencode 'scope=cob.write+cob.read+cobv.write+cobv.read+webhook.read+webhook.write'
```

- **Produção:** https://api-pix.sicredi.com.br/oauth/token

```
curl --location --request POST 'https://api-pix.sicredi.com.br/oauth/token' \
--header 'Content-Type: application/x-www-form-urlencoded' \
--header 'Authorization: Basic Q0xJRU5UX0lEX1BST0RVQ0FPOkNMSUVOVF9TRUNSRVRfUFJPRFVDQU8=' \
--data-urlencode 'grant_type=client_credentials' \
--data-urlencode 'scope=cob.write+cob.read+cobv.write+cobv.read+webhook.read+webhook.write'
```

- **Servidor de recursos – para realizar o acesso aos recursos da API Pix:**

Após ter adquirido o token de acesso com os escopos dos recursos desejados (*endpoints*), basta utilizá-lo para receber a autorização na construção das requisições, como nos exemplos abaixo:

- **Homologação:** *https://api-pix-h.sicredi.com.br/api/v2*

```
curl --location --request GET 'https://api-pix-h.sicredi.com.br/api/v2/cob/rbkPASL2pV4X7bIlD746zeMOX' \
--header 'Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9[...]'
```

- **Produção:** *https://api-pix.sicredi.com.br/api/v2*

```
curl --location --request GET 'https://api-pix.sicredi.com.br/api/v2/cob/rbkPASL2pV4X7bIlD746zeMOXI' \
--header 'Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9[...]'
```

9. Testes opcionais

Para concluir a homologação, orientamos a geração de *3 QR Codes* válidos.

Como evidência, deve ser realizado o envio de 3 códigos Pix Copia e Cola (a sequência de caracteres que representa o *QR Code*) para o email *integracoes_pix@sicredi.com.br* com o assunto padrão: Testes Homologação CNPJ XXXXXXXX.

Para estas validações, a cobrança deve ser criada com validade superior a 48h, com valores entre R$ 10,00 e 100,00 e o código Pix Copia e Cola deve ser enviado por completo, com todos os seus caracteres.

Para as demais funcionalidades (alteração, consulta, etc) não há necessidade de envio de evidências.

10. Documentação do Bacen em relação à API Pix

O Sicredi desenvolveu a API Pix conforme todos os requisitos constantes no **Manual de Padrões para Iniciação do Pix**, que é a documentação do Bacen regulamentada para todos os PSPs:

- **Link do Manual de Padrões para Iniciação do Pix:** https://www.bcb.gov.br/content/estabilidadefinanceira/pix/Regulamento_Pix/II_ManualdePadroesparaIniciacaodoPix.pdf

Para o desenvolvimento das chamadas da API, o responsável técnico deve basear-se na documentação da API Pix abaixo, que contém todos os parâmetros de entrada e saída e os *endpoints* com as funcionalidades disponibilizadas pela API.

- **Especificação baseada em formato Swagger (Open API)**: https://bacen.github.io/pix-api
- **Especificação Open API 3.0**: https://github.com/bacen/pix-api/releases/download/2.6.2/spec.html

No processo de integração, a API Pix não é responsável por gerar as imagens do QR Code. Desta forma, há duas possibilidades:

1. Utilizar o campo 'pixCopiaECola', recebido nas respostas dos *endpoints* cob e cobv, como entrada no software utilizado para geração da imagem do QR Code.
2. Gerar uma nova entrada, seguindo os padrões descritos no Manual do BR Code: https://www.bcb.gov.br/content/estabilidadefinanceira/spb_docs/ManualBRCode.pdf

11. Recomendações

Abaixo algumas recomendações gerais do Sicredi de boas práticas de integração da API Pix.

- Alteração de valor da cobrança

Para o campo JSON de nome *valor.modalidadeAlteracao*, mencionado na seção 1.6. Iniciação do Pix via QR Code Dinâmico da documentação do Bacen - Manual de Padrões para Iniciação do Pix, recomendamos sempre utilizar no preenchimento do campo o valor '0', a fim de evitar alterações indevidas do valor da cobrança por parte do pagador.

- Pix Saque e Pix Troco

As indicações referentes ao desenvolvimento de Pix Saque e Pix Troco constam detalhadas a partir da versão 2.5.0 da documentação do Bacen - Manual de Padrões para Iniciação do Pix.

ISPB do facilitador de serviço de saque – Nos parâmetros de: *retirada.saque.prestadorDoServicoDeSaque* e *retirada.troco.prestadorDoServicoDeSaque* devem ser sempre indicados como número de IPSB Sicredi, o código **01181521**.

- Sistema Operacional

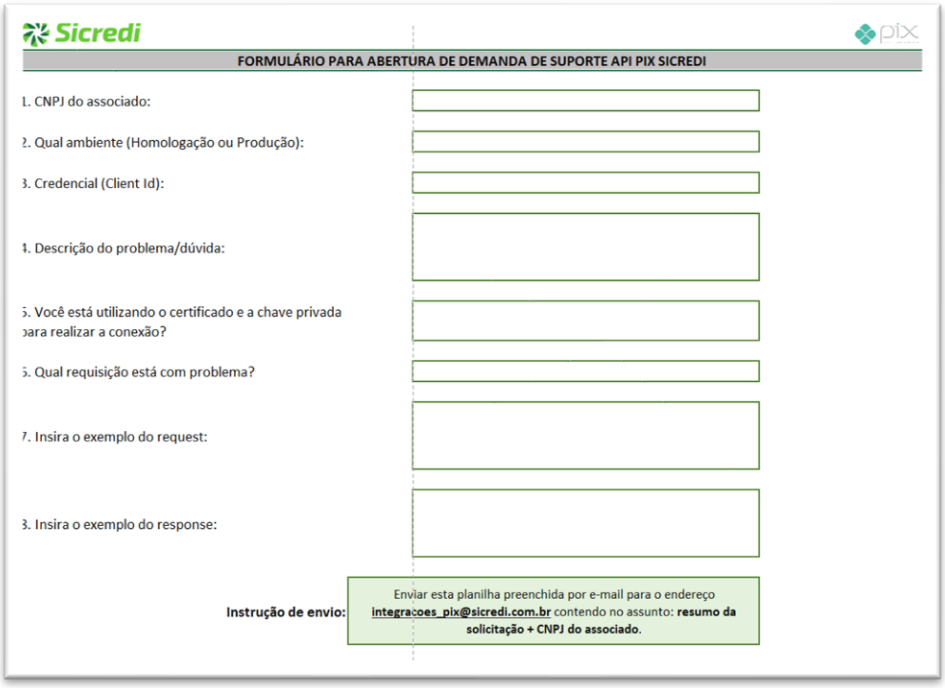
No caso de ser utilizado o sistema operacional Windows Server, a recomendação do Sicredi é de que seja de uma versão atualizada, que possua suporte da Microsoft. Nesse sentido, recomendamos a utilização de versões do Windows Server 2016 em diante.

- Arrecadação Híbrida

As indicações referentes ao desenvolvimento de Arrecadação Híbrida constam detalhadas no **Manual de Integrações API Pix - Arrecadação/Recebimento com Utilização do Pagamento Instantâneo PIX Modelo QR Dinâmico** e deve ser solicitado para área responsável Recebimentos PJ, pelo e-mail homologacoes_recebimentos@sicredi.com.br.

12. Suporte

O Sicredi possui um canal exclusivo para esclarecimentos e apoio em todo o processo de integração com a **API Pix**. Havendo necessidade de suporte, o integrador técnico deve enviar um e-mail para integracoes_pix@sicredi.com.br, com o formulário abaixo* preenchido:



Sicredi

pix

FORMULÁRIO PARA ABERTURA DE DEMANDA DE SUPORTE API PIX SICREDI

1. CNPJ do associado:	
2. Qual ambiente (Homologação ou Produção):	
3. Credencial (Client Id):	
4. Descrição do problema/dúvida:	
5. Você está utilizando o certificado e a chave privada para realizar a conexão?	
6. Qual requisição está com problema?	
7. Insira o exemplo do request:	
8. Insira o exemplo do response:	
Instrução de envio:	Enviar esta planilha preenchida por e-mail para o endereço **integracoes_pix@sicredi.com.br** contendo no assunto: **resumo da solicitação + CNPJ do associado.**

*Este formulário é encaminhado juntamente com o e-mail de Boas-Vindas ao associado.

Nos casos de demanda sobre **Arrecadação Híbrida**, o suporte a ser acionado deve ser o e-mail homologacoes_recebimentos@sicredi.com.br.

Anexo I - Geração de certificado CSR para uso API Pix

1º passo

Gerar o arquivo de chave (.key)

Utilizando o software OPENSSL, em ambiente de linha de comando, autenticado como usuário Administrador, execute o comando a seguir:

openssl genrsa -des3 -out APLICACAO*.key* 2048

Recomendações:

- Algoritmo da chave: **RSA (genrsa);**
- Tamanho da chave: **2048 ou mais**;
- Criptografia da senha da chave privada: **AES256 ou *Triple DES*** (**-aes256 ou -des3**).

Neste passo será solicitada uma frase secreta para gerar o arquivo de chaves, conforme abaixo:

- *Enter pass phrase for* APLICACAO*.key*:
- *Verifying - Enter pass phrase for* APLICACAO*.key*:

Informe um valor qualquer para a frase secreta, e anote-o para ser usado no passo seguinte:

2º passo

Gerar a requisição do certificado (.csr) através da chave (.key) gerada no passo anterior
Utilizando o software OPENSSL, em ambiente de linha de comando, autenticado como usuário Administrador, execute o comando a seguir:

openssl req -new -key APLICACAO*.key -out* APLICACAO.csr

Neste passo será solicitada a frase secreta cadastrada no passo 1, ao digitá-la as seguintes informações serão solicitadas, preencha conforme padrão Sicredi abaixo:

- *Country Name (2 letter code) [AU]:* BR

- *State or Province Name (full name) [Some-State]:* Rio Grande do Sul

- *Locality Name (eg, city) [ ]:* Porto Alegre

- *Organization Name (eg, company) [Internet Widgits Pty Ltd]:* Confederacao Interestadual das Cooperativas Ligadas ao Sicredi

- *Organizational Unit Name (eg, section) [ ]:* API PIX Sicredi

- *Common Name (eg, YOUR name) [ ]: Utilizar o prefixo* ***api-pix-*** *+ Nome do Estabelecimento,* *Exemplo*: ***api-pix-****SUPERMERCADOABC*

- *Email Address [ ]:* [E-mail do Associado]

- *A challenge password [ ]:* Campo não setado

- *An optional company name [ ]:* Campo não setado

3º passo

Retirando a frase secreta

Dependendo do *Web Server* será necessário retirar a frase secreta da chave (*.key*) gerada no primeiro passo para que ela não seja solicitada no momento de algum *restart* do *Web Server.*

Para isso, execute os passos abaixo informando a senha definida no primeiro passo. Utilizando o software OPENSSL, em ambiente de linha de comando, autenticado como usuário Administrador, execute os comandos a seguir:

mv ***APLICACAO****.key* ***APLICACAO****_COMSENHA.key*
openssl rsa -in ***APLICACAO****_COMSENHA.key -out* ***APLICACAO****.key*

Anexo II – Manual Técnico Postman

Certificados Sicredi - Autenticação TLS mútua

O objetivo desse anexo é auxiliar o público que tem posse de certificados Sicredi no processo de autenticação TLS mútua usando a ferramenta Postman.

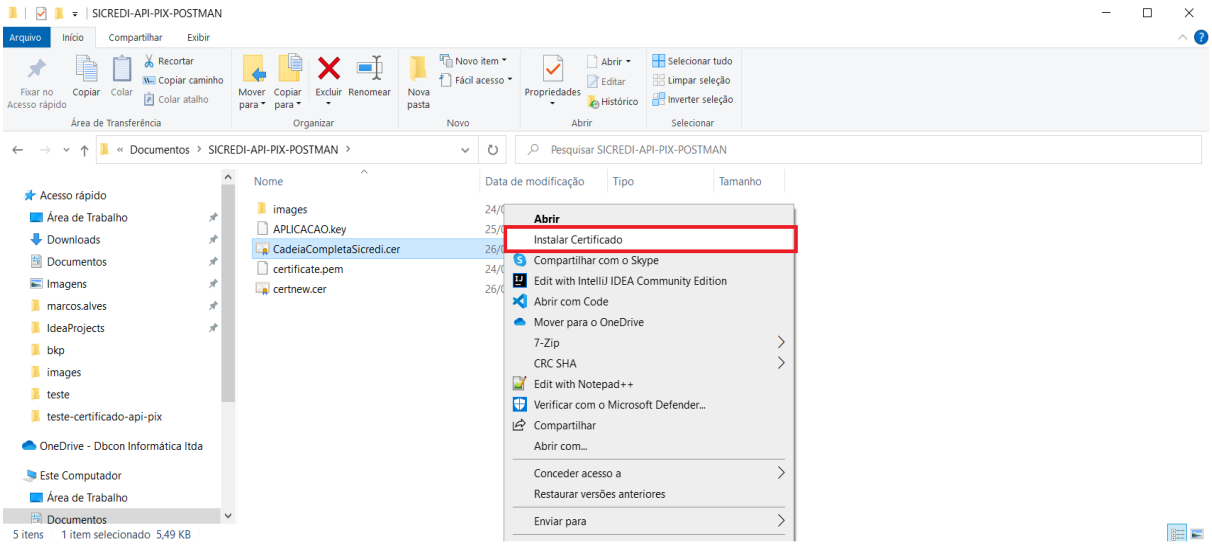
O Postman (até a confecção desse documento) aceita apenas certificados no formato .PEM, em contrapartida, o Sicredi disponibiliza o certificado no formato .DER. Logo, para uma conexão de sucesso usando o Postman é necessária a conversão do certificado para o formato requerido.

Nos próximos passos, seguiremos demostrando como realizar essa conversão, e como utilizar as credenciais SSL (certificado e chave) para a autenticação mútua no Postman.

1º passo

Você deve ter recebido a cadeia certificadora completa do Sicredi (CA), primeiramente, deve-se instalar esse certificado na wallet do sistema.

Exemplo Windows:

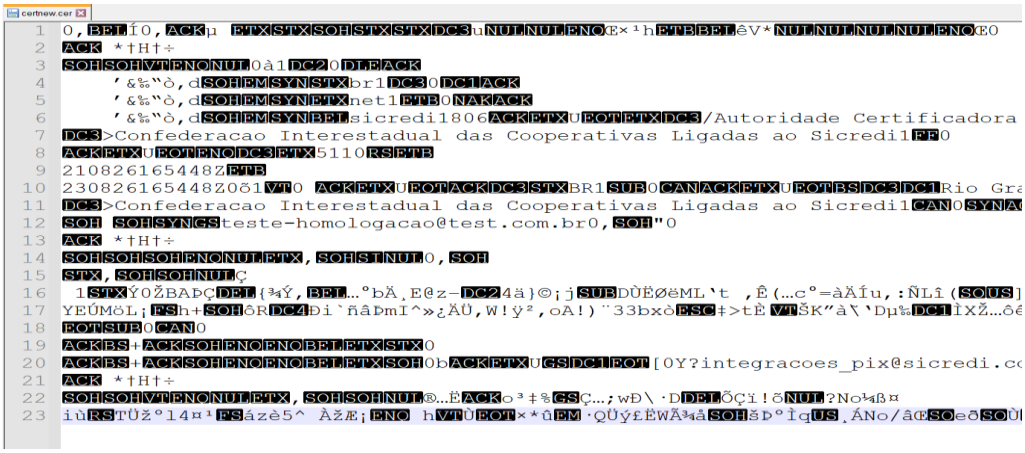


O assistente de instalação será aberto, basta prosseguir confirmando as informações.

2º passo

Verifique se o certificado recebido está no formato .DER

Exemplo: Abra o arquivo em um editor de texto, e verifique se está ilegível (contendo informações em binário) como na imagem.

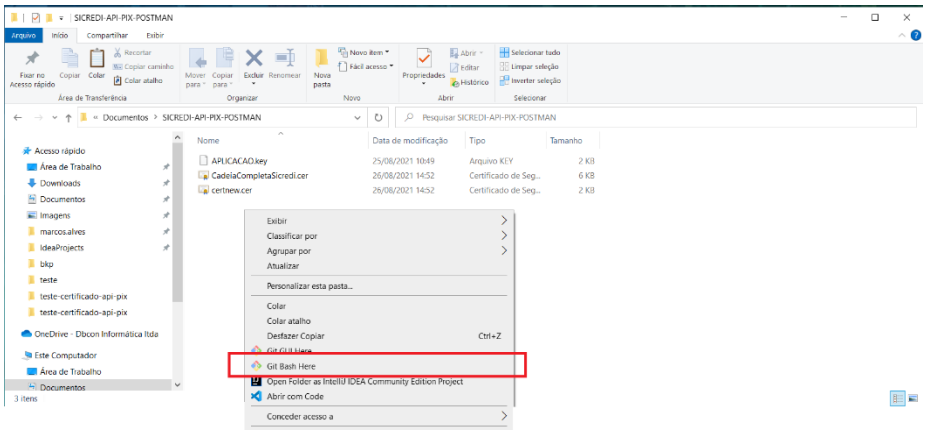


3º passo

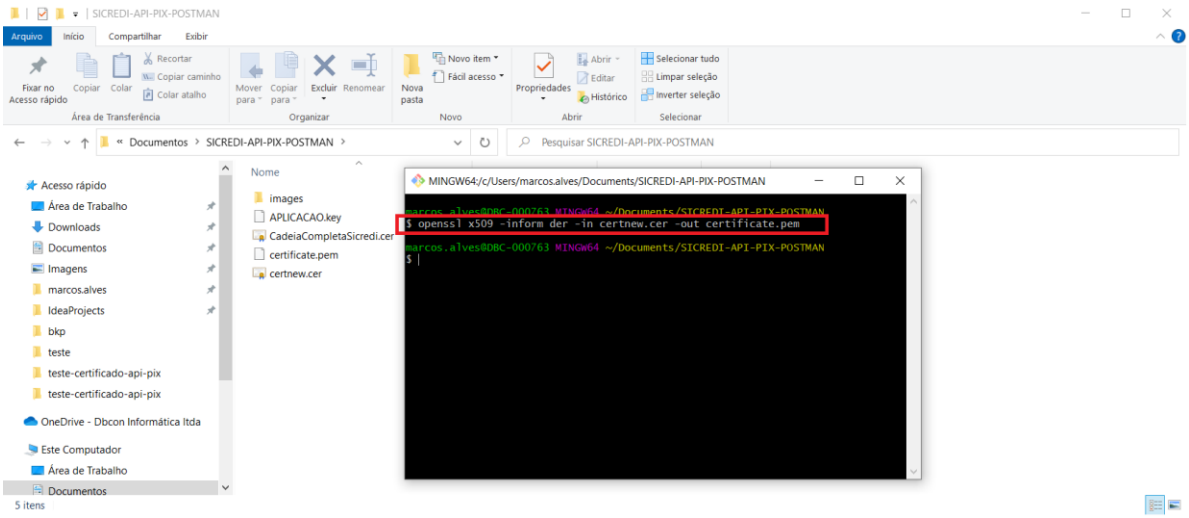
Utilize algum software SSL para realizar a conversão do certificado no formato .DER para .PEM

Exemplo Windows:

Neste exemplo, utilizamos uma versão do OpenSSL que está embutida na instalação do MINGW64 provinda pelo GIT.



O comando utilizado foi: openssl x509 -inform der -in certificado_original.cer -out certificado_novo.pem



4º passo

Após a conversão o formato do arquivo .PEM deve estar legível, sem informações em binário.

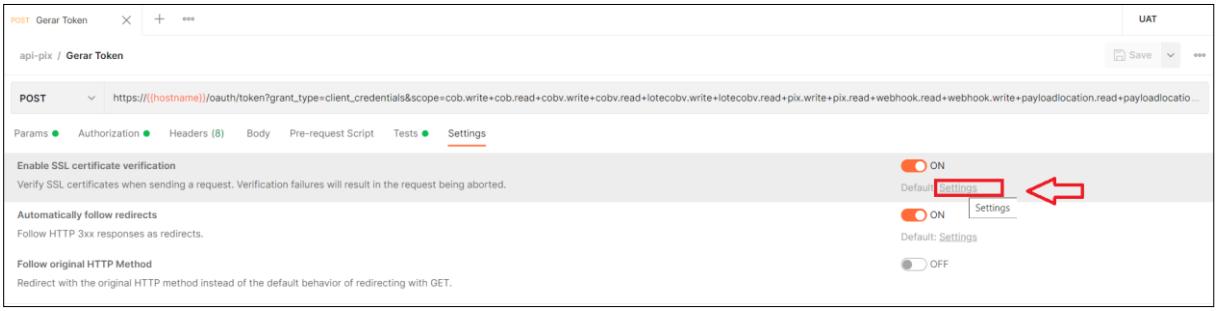
Exemplo:

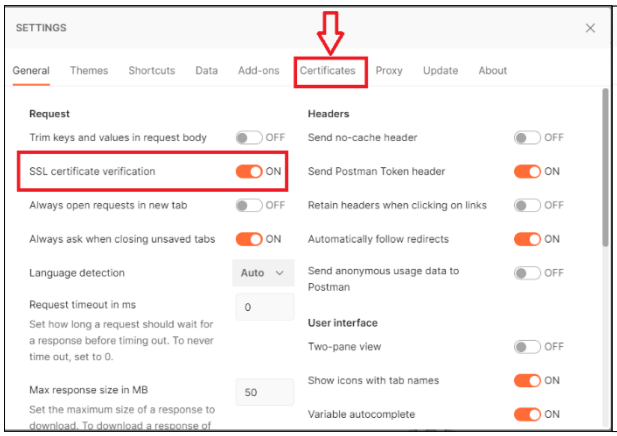
Abra o arquivo .pem gerado em um editor de texto, e verifique se está como na imagem.

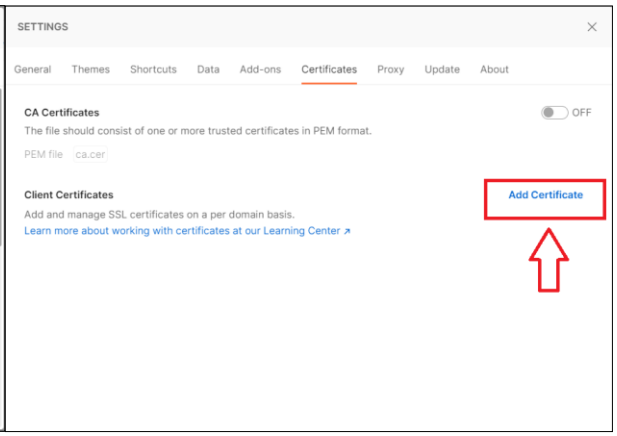
5° passo

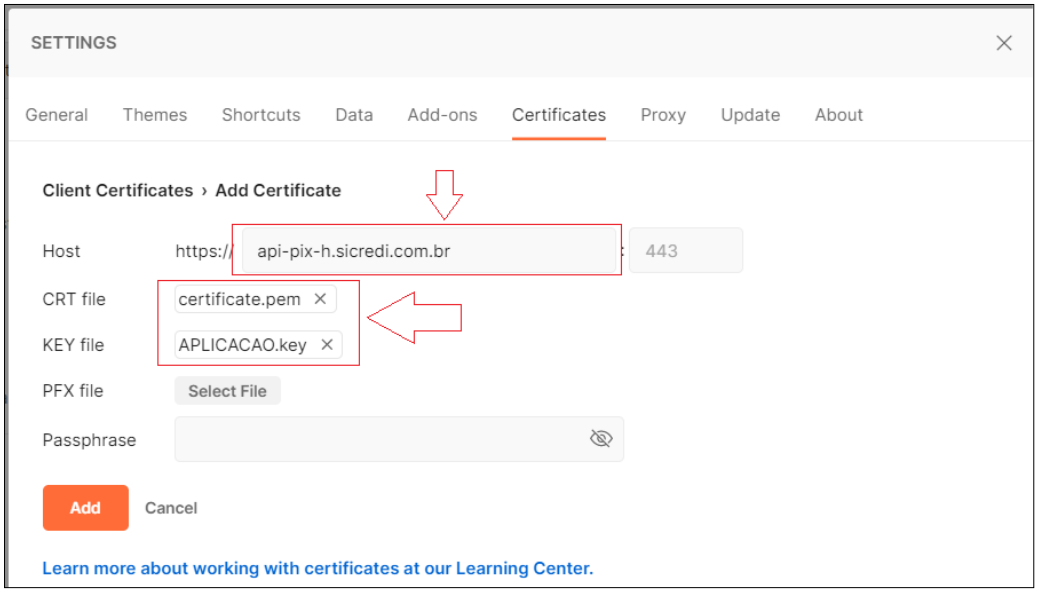
Em seguida, basta configurar o Postman para utilizar o certificado (.PEM) e a chave (.KEY).

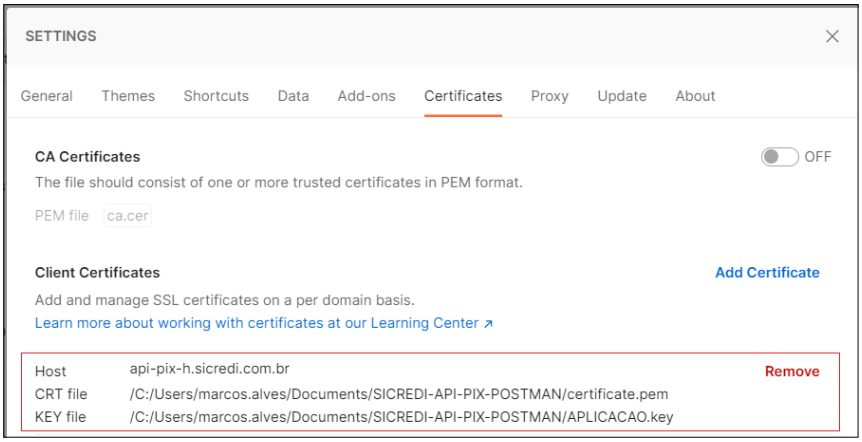
A seguir, seguem imagens ilustrando o processo:





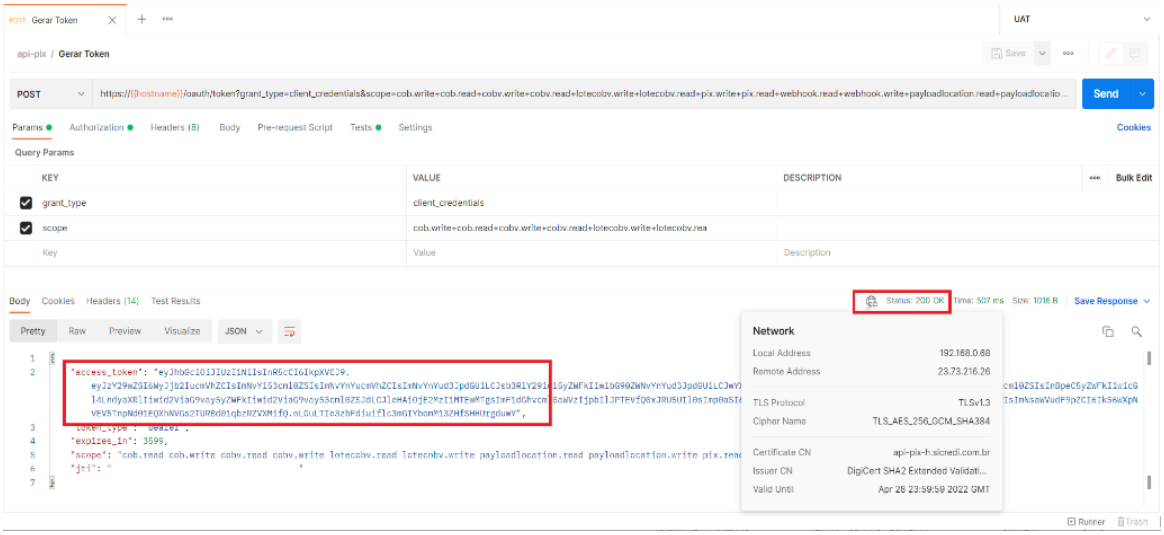






6º passo

Após as configurações, já será possível realizar chamadas autenticadas mTLS com o ambiente do Sicredi. Tanto para geração do token de acesso a API PIX, quanto para as criações de cobranças e demais funcionalidades da API. Exemplo:



Anexo III – Collection Postman

O Postman é um API Client que facilita aos desenvolvedores criar, compartilhar, testar e documentar APIs. Esta ferramenta pode ser baixada de forma gratuita no seguinte link:

https://www.postman.com/downloads/

No caso da API Pix, criamos uma *collection* com as principais requisições com o objetivo de facilitar o entendimento do integrador técnico nas etapas de desenvolvimento da integração com a API Pix.

O arquivo da *collection* com extensão ".json" é enviado no e-mail de Boas-Vindas que o associado recebe no início da sua jornada de integração com a API Pix:

- Api Pix Sicredi.postman_collection.json

Para melhor visualização da documentação no Postman, recomendamos que o usuário tenha o programa instalado em seu ambiente e que possua uma conta neste client. Caso seja necessário o reenvio do arquivo da collection ou alguma dúvida e/ou sugestão, favor solicitar através do e-mail integracoes_pix@sicredi.com.br.

Anexo IV – Erros Frequentes

Neste anexo, compilamos os erros mais frequentes retornados pela API Pix, a fim de otimizar a identificação e endereçamento de tratativas. Reforçamos que sejam seguidas as instruções do Guia Técnico de Integrações API Pix para que todas as chamadas sejam bem-sucedidas.

Códigos de erro padrões da API Pix

A API Pix retorna códigos de status HTTP para indicar sucesso ou falhas das requisições.

- **Status 2xx** indicam sucesso;
- **Status 4xx** indicam falhas causadas pelas informações enviadas pelo cliente ou pelo estado atual das entidades;
- **Status 5xx** indicam problemas no serviço no lado da API Pix.

A seguir, estão listados os tipos de erro e possíveis violações mais frequentes da API Pix Sicredi.

Status 400

O status 400 trata-se de uma crítica de negócio, e geralmente no corpo da mensagem consta a indicação do ponto que deve ser verificado – em violações ou em detalhes.

Abaixo destacamos os casos mais comuns:

➔ **Escopo solicitado na requisição não está liberado para a credencial.**

- **Orientação**: Quando é realizada a adesão à API Pix junto à cooperativa, o associado informa como deseja ter o recebimento Pix no Sicredi através da API Pix, assim os escopos são liberados de acordo com o que foi solicitado, em até 48 horas após a geração das credenciais.

  Modalidades de recebimento via API Pix e respectivos escopos:
  - ✓ **Cobrança Imediata:** escopos cob.write + cob.read;
  - ✓ **Cobrança com Vencimento:** escopos cobv.write + cobv.read + lotecobv.write + lotecobv.read.

  Nestes casos, é importante checar com o associado se o escopo que está sendo solicitado condiz com a forma que deseja receber o Pix e se as credenciais foram geradas há mais de 48 horas. Havendo necessidade de inclusão de mais escopos, o associado deverá solicitar à sua cooperativa a adição da modalidade de recebimento via API Pix correspondente.

➔ **Chave Pix utilizada no ambiente incorreto.**
- Orientação: Verificar se a chave Pix informada faz parte do ambiente correto. No caso de chaves aleatórias, por exemplo, não é possível utilizar a chave de produção no ambiente de homologação e vice-versa.

➔ **Crítica de thumbprint incorreto.**
- Orientação: o certificado enviado na requisição está diferente do que foi cadastrado para a credencial gerada no Internet Banking. Neste caso, o associado do Sicredi deverá refazer a geração das credenciais no canal de Internet Banking, selecionando o certificado correto assinado pelo Sicredi para a integração.

Status 401

➔ **"Cannot convert access token to JSON":**
- Descrição: Não foi possível converter o token de acesso para o formato esperado.
- Orientação: Enviar o token no mesmo formato que foi recebido, pois pode ter ocorrido uma codificação ou conversão de dados antes do envio.

➔ **"Full authentication is required to access this resource"**
- Descrição: Problema nas credenciais Client Id e/ou Client Secret utilizadas.
- Orientação: Confirmar se as credenciais utilizadas estão corretas e no formato válido, e se pertencem ao ambiente em que estão sendo informadas (homologação ou produção).

Status 403

➔ **"You don't have permission to access "http://api-pix.sicredi.com.br/" on this server."**

➔ **"You don't have permission to access "http://api-pix-h.sicredi.com.br/" on this server."**
- Descrição: Não foi possível realizar a autenticação mTLS.
- Orientação: Todas as chamadas da API Pix devem ser feitas utilizando criptografia TLS com autenticação mútua no estabelecimento da conexão, de posse dos seguintes itens:
  - Certificado digital .CER (disponibilizado através do Internet Banking Sicredi);
  - Chave APLICACAO.KEY gerada pra fazer a requisição do certificado;
  - Cadeia completa (disponibilizado através do Internet Banking Sicredi).

Observação: recomendamos utilizar a chave privada APLICACAO.KEY sem senha, pois algumas ferramentas podem não suportar este tipo de proteção.

Status 404

➔ **“Entidade não encontrada.”**

- Descrição: Não foi possível localizar o recurso solicitado ou o endpoint requisitado.
- Orientação: Validar as informações da requisição e o endpoint requisitado, conforme a documentação do Bacen, indicada neste Guia Técnico.

Status 500

➔ **“Condição inesperada ao processar requisição.”**

- Descrição: Quando o servidor retorna um código de erro (HTTP) 500, indica que encontrou uma condição inesperada e que o impediu de atender à solicitação. Essa resposta de erro é uma resposta genérica. Ou seja, é um erro não mapeado, não conhecido pelo sistema, não sendo possível determinar de imediato a sua causa raiz.
- Orientação: Encaminhar o formulário de suporte preenchido para avaliação técnica e investigação da causa raiz pelo time técnico da API Pix Sicredi.