
Guia Técnico Integrações

API Pix Sicredi

Sumário

1. Apresentação.....	3
2. Objetivo	3
3. Público-alvo da solução de integração.....	3
4. Funcionalidades da API Pix.....	3
5. Jornada de adesão e implementação Sicredi.....	4
6. Passo a passo da jornada no Sicredi	5
7. Implementação via Portal do Desenvolvedor	5
8. Fluxo de Requisições da API Pix Sicredi.....	8
9. Documentação Bacen em relação à API Pix	12
10. Webhook	13
11. Recomendações.....	15
12. Suporte	16
Anexo I – Passo-a-passo Portal Desenvolvedor.....	19
Anexo II – Postman e Collection	26
Anexo III – Erros Frequentes.....	33
Anexo IV – Geração Manual de Requisição (CSR) para assinatura de Certificado da API Pix Sicredi.....	39
Anexo V – Extra.....	41

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 Portal do Desenvolvedor do Sicredi.

7. Implementação via Portal do Desenvolvedor

Atenção: os passos a seguir devem ser realizados no Portal do Desenvolvedor pelo técnico do associado.

1. Primeiro acesso ao Portal Dev.

No primeiro acesso ao Portal do Desenvolvedor Sicredi (<https://developer.sicredi.com.br>), o técnico deverá realizar seu cadastro como usuário desenvolvedor no Portal e, após, solicitar a abertura de chamado (**Página Inicial > Suporte > Abra um chamado**) para acesso à API Recebimento do primeiro associado que o técnico está realizando a integração via Portal do Desenvolvedor Sicredi. Para as demais integrações atendidas por este usuário técnico, a solicitação via chamado permanecerá para que seja autorizada a sua atuação nos arquivos da conta especificada do CPF/CNPJ.

Para maiores detalhes e telas, consultar Anexo I – Passo a passo Portal do Desenvolvedor.

2. Geração de arquivo CSR (Certificate Signing Request) – Requisição para assinatura de Certificado.

Dentro do Portal do Desenvolvedor, já com o login efetuado, o técnico deverá abrir um Chamado (**Página inicial > Suporte > Abra um chamado**) requisitando o Acesso à API Pix para trocas de arquivos para o associado, onde deverá ser informado o CNPJ e o ID da adesão (Número de demanda da integração aberta pela cooperativa e informada ao associado no corpo do e-mail de boas-vindas)

O arquivo gerado (**Página Inicial > API's > Catálogo de APIs > API de Recebimento > Registrar Novo CSR**) para a conta informada do associado será recebido pelo Sicredi e avaliado dentro do nosso perímetro de segurança. Com as informações validadas, dentro do prazo informado, será disponibilizado o certificado digital assinado, necessário para a implementação.

Juntamente ao arquivo de Requisição (CSR) registrado no Portal do Desenvolvedor para a conta informada do associado, estará disponível (⋮) o arquivo de Chave Privada, que deverá ser baixado e armazenado em local seguro e organizado para posterior configuração da implementação na automação do associado.

Para maiores detalhes e telas, consultar Anexo I – Passo a passo Portal do Desenvolvedor.

3. Download do certificado digital assinado Sicredi

Técnico deve acessar o Portal do Desenvolvedor (<https://developer.sicredi.com.br>) com usuário e senha previamente criados, acessar **APIs > Catálogo de APIs > API Recebimento > API Pix > Geração de Certificado** inserindo os dados de Cooperativa e Conta para realizar o *download* dos arquivos disponibilizados:

- ✓ Certificado Digital .CER
- ✓ Cadeia de Certificados Completa Sicredi .CER
- ✓ webhook-sicredi.CER (**opcional**) – para autenticação do webhook)

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

Técnico deve acessar o Portal do Desenvolvedor <https://developer.sicredi.com.br/api-portal/> com usuário e senha previamente criados, acessar APIs > Catálogo de APIs > API Recebimento > Pix > Certificados e Credenciais, inserir Cooperativa e Conta do associado para listar os arquivos disponíveis e, sob o arquivo de certificado cnpj.CER, clicar em (⋮) para acessar Gerar Credenciais sobre este certificado específico (disponibilizado pelo Sicredi).

Esta credencial acessa o ambiente de produção.

Atenção:

Caso sejam necessários testes das funcionalidades no ambiente de **homologação**, o técnico deve solicitar ao endereço integracoes_pix@sicredi.com.br, o acesso para o ambiente informando o CNPJ do associado que está integrando. Com base nessa solicitação, retornaremos informando a chave a ser utilizada no ambiente de homologação.

A geração de credencial para o ambiente de **homologação** não está prevista para ser emitida via Portal do Desenvolvedor. Em razão disso, **apenas para credenciais do ambiente de homologação**, o técnico deve solicitar que o associado acesse o Internet Banking Sicredi (Página Inicial IB > Outros Serviços > Acesso à API Pix > Gerar Credenciais), em que estas devem ser geradas com base no Certificado assinado Sicredi disponível nesta seção indicando o ambiente de Homologação no momento de sua geração. Após validado o token para geração, o associado deverá copiar, colar e salvar as credenciais em um arquivo texto para enviá-las ao técnico.

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:

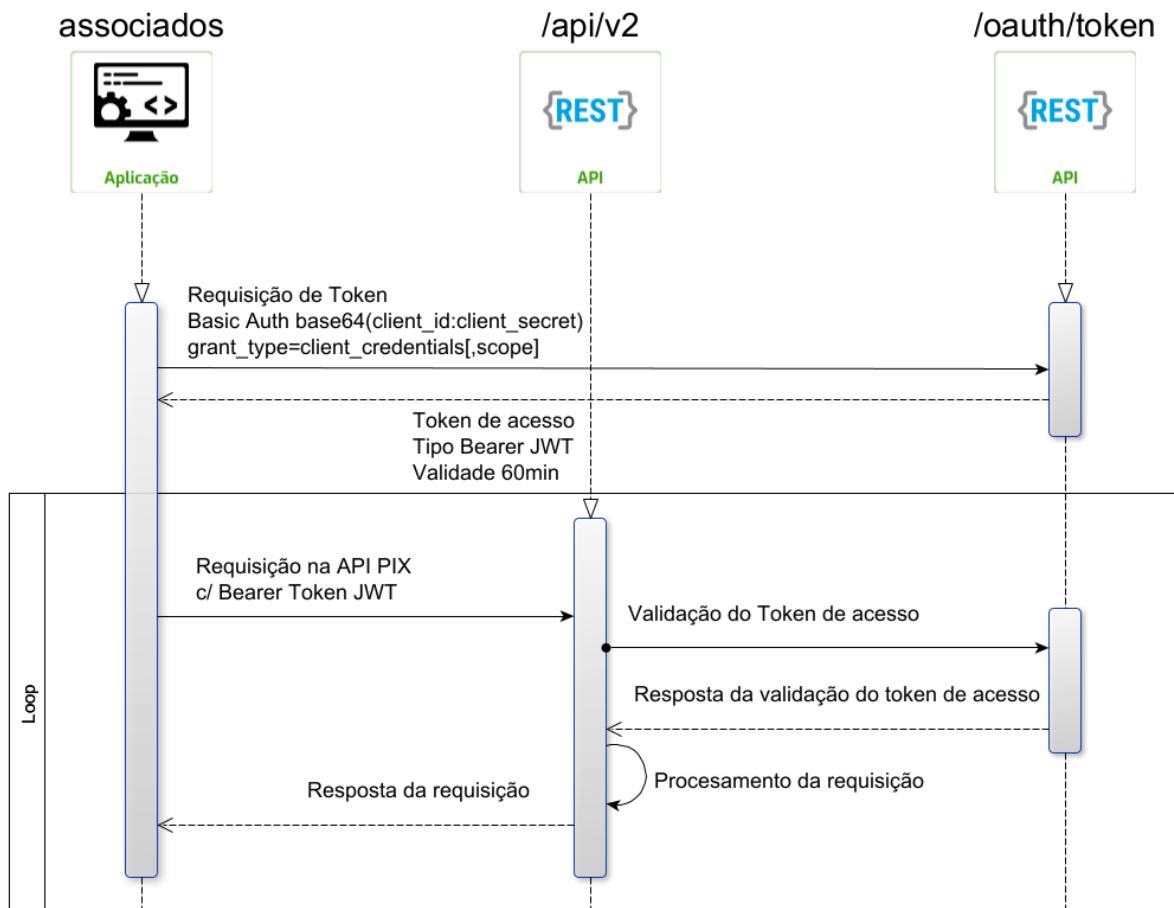
- Certificado digital *.CER* (disponibilizado através do Portal do Desenvolvedor);
- Chave *APLICACAO.KEY* gerada em conjunto com a requisição do certificado;
- Cadeia completa (disponibilizado através do Portal do Desenvolvedor).

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, indicamos que seja utilizada a ferramenta **Postman**, temos o **Anexo II**, contendo o passo-a-passo da configuração nesta ferramenta com instruções da 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 caractere : (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, ou ainda, o sinal de “+” entre cada um dos escopos a serem solicitados.

Exemplos:

- Ambiente de 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 Q0xJRU5UX01EX1BST0RVQ0FP0KNMSUV0VF9TRUNSRVRfUFJPRFVDQU8=' \
--data-urlencode 'grant_type=client_credentials' \
--data-urlencode 'scope=cob.write+cob.read+cobv.write+cobv.read+webhook.read+webhook.write'
```

Campos com a resposta da requisição de Token de acesso:

Campo	Tipo	Descrição
access_token	string	Token de acesso
token_type	string	Tipo do token (bearer)
expires_in	number	Tempo de expiração do token (milissegundos)
scope	string	Escopos liberados para o acesso
jti	string	Identificação do token

Por padrão o token expira em aproximadamente 60 minutos (3600 segundos).

- Resposta da requisição:

```
{
  "access_token": "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzY29wZSI6WyJjb2IucmVhZCIsImNvYi53cm10ZSIIsIndlYmhvb2sucmVhZCIsIndlYmhvb2sud3JpdGUiXSwiZXhwIjoxNjkxNjEyMjk1LCJhdXR0b3JpdGllcyI6WyJST0xFX0NMSUV0VCJdLCJqdGkiOiI5NTY5ZDNhNS03NzI1LTRjMjMtYjA1NS00Zjg5MDEwOTY2NDQiLCJjbGllbnRfaWQoIj0e116TVRFeU56TXdNREF4TVRrNk1EQXdNam80WVVzIn0.wtQFSFv8_-t9EIkijielVS8510gFBV3foMqsvMEq9ZY",
  "token_type": "bearer",
  "expires_in": 3599,
  "scope": "cob.read cob.write webhook.read webhook.write",
  "jti": "9569d3a5-7725-4c23-b055-4f8901096644"
}
```

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:

- Ambiente de Produção: <https://api-pix.sicredi.com.br/api/v2>

```
curl --location --request GET 'https://api-pix.sicredi.com.br/api/v2/cob/rbkPASL2pV4X7bI1D746zeMOXI' \
--header 'Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9[...]'
```

9. Documentação 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/2.6.3/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/ManualBRCCode.pdf

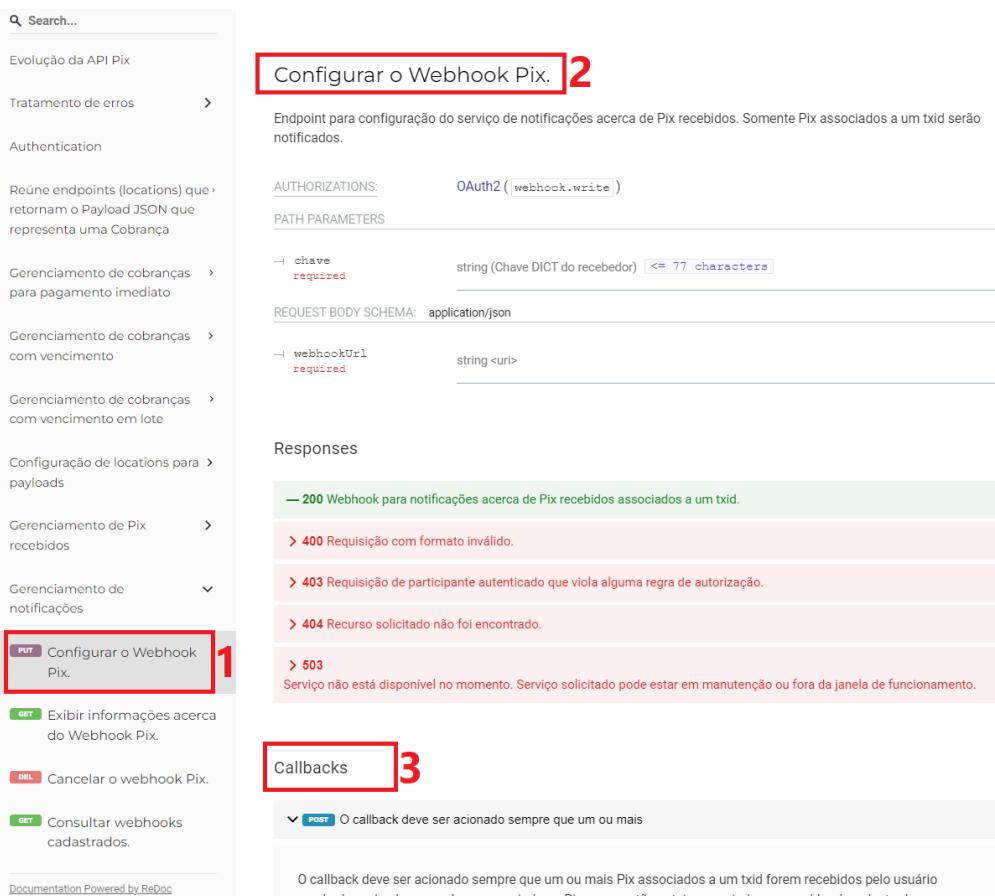
10. Webhook

O Webhook é um recurso que pode ser cadastrado através da integração com a API Pix, em que o Sicredi comunica ao sistema de automação do associado, imediatamente, a confirmação dos recebimentos de Pix, trazendo mais agilidade ao fluxo transacional.

Cadastro

O cadastro do Webhook **deve ser realizado pelo sistema integrado ou pelo técnico responsável pela integração da API Pix Sicredi.**

Para receber notificações de transações efetuadas através da API Pix, precisa ser criado um registro de Webhook, conforme documentação do Bacen, sendo necessária a utilização da chave Pix do associado (a mesma utilizada para geração da cobrança a qual se deseja receber a notificação):



The screenshot shows the API documentation for the Webhook Pix resource. On the left, there's a sidebar with navigation links like 'Evolução da API Pix', 'Tratamento de erros', 'Authentication', etc. A red box labeled '1' highlights the 'PUT Configurar o Webhook Pix.' link under the 'Gerenciamento de notificações' section. The main content area has a red box labeled '2' around the title 'Configurar o Webhook Pix.' and its description. It details the required 'chave' parameter (OAuth2) and the 'webhookUrl' parameter. Below this, a red box labeled '3' highlights the 'Callbacks' section, which describes the POST method for triggering callbacks when associated Pix are received.

Search...
Evolução da API Pix
Tratamento de erros >
Authentication
Reúne endpoints (locations) que retornam o Payload JSON que representa uma Cobrança
Gerenciamento de cobranças > para pagamento imediato
Gerenciamento de cobranças > com vencimento
Gerenciamento de cobranças > com vencimento em lote
Configuração de locations para payloads
Gerenciamento de Pix > recebidos
Gerenciamento de notificações
PUT Configurar o Webhook Pix. 1
GET Exibir informações acerca do Webhook Pix.
DELETE Cancelar o webhook Pix.
GET Consultar webhooks cadastrados.
Documentation Powered by ReDoc

Configurar o Webhook Pix. 2
Endpoint para configuração do serviço de notificações acerca de Pix recebidos. Somente Pix associados a um txid serão notificados.

AUTHORIZATIONS: OAuth2 (webhook.write)
PATH PARAMETERS
-> chave required string (Chave DICT do recebedor) <= 77 characters
REQUEST BODY SCHEMA: application/json
-> webhookUrl required string <uri>

Responses
— 200 Webhook para notificações acerca de Pix recebidos associados a um txid.
> 400 Requisição com formato inválido.
> 403 Requisição de participante autenticado que viola alguma regra de autorização.
> 404 Recurso solicitado não foi encontrado.
> 503 Serviço não está disponível no momento. Serviço solicitado pode estar em manutenção ou fora da janela de funcionamento.

Callbacks 3
▼ **POST** O callback deve ser acionado sempre que um ou mais Pix associados a um txid forem recebidos pelo usuário recebedor e desde que o objeto associado ao Pix em questão esteja associado a um webhook cadastrado

Fonte: Documentação Bacen. Disponível em: <https://github.com/bacen/pix-api/releases/download/2.6.3/spec.html>

A imagem acima demonstra as especificações do Bacen para configuração do Webhook. Na **marcação de nº 1** da imagem, é possível visualizar em qual o menu se encontra as orientações sobre a configuração do Webhook. Na **marcação nº 2**, encontram-se as especificações da requisição. E, na **marcação nº 3**, encontram-se as regras do retorno, indicando as regras de quando o *callback* será acionado, contendo as propriedades do objeto retornado.

Detalhes sobre a requisição para registro do Webhook:

PUT /webhook/{chave}	
Parâmetros	
Parâmetro	Descrição
<i>chave</i>	<i>Chave pix</i>
Body	
Esquema	Descrição
<i>webhookUrl</i>	<i>URI que irá receber a notificação (deve ser enviada no body do request)</i>

Autenticação TLS

O servidor cadastrado para receber as notificações de recebimento de Pix para a chave determinada, deve, no mínimo:

- Implementar TLS na porta 443, disponibilizando um certificado assinado por uma CA pública reconhecida (ex.: Digicert, Entrust, GlobalSign, etc...)
- Recomenda-se que o atributo CN do certificado seja o mesmo do nome de domínio do servidor
- A URL cadastrada deve utilizar o protocolo HTTPS: (https://nome_de_domínio_do_servidor...)
- Ter o certificado de cadeia completa do Sicredi instalado e configurado como confiável, o qual é disponibilizado no canal Portal do Desenvolvedor do Sicredi para o técnico do associado;
- **Opcionalmente**, o servidor da automação pode realizar a validação do certificado do Webhook (**webhook-sicredi.CER**), adicionando mais uma camada de segurança ao processo. Este certificado está disponível para download no portal do desenvolvedor junto aos demais arquivos da conta.

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**

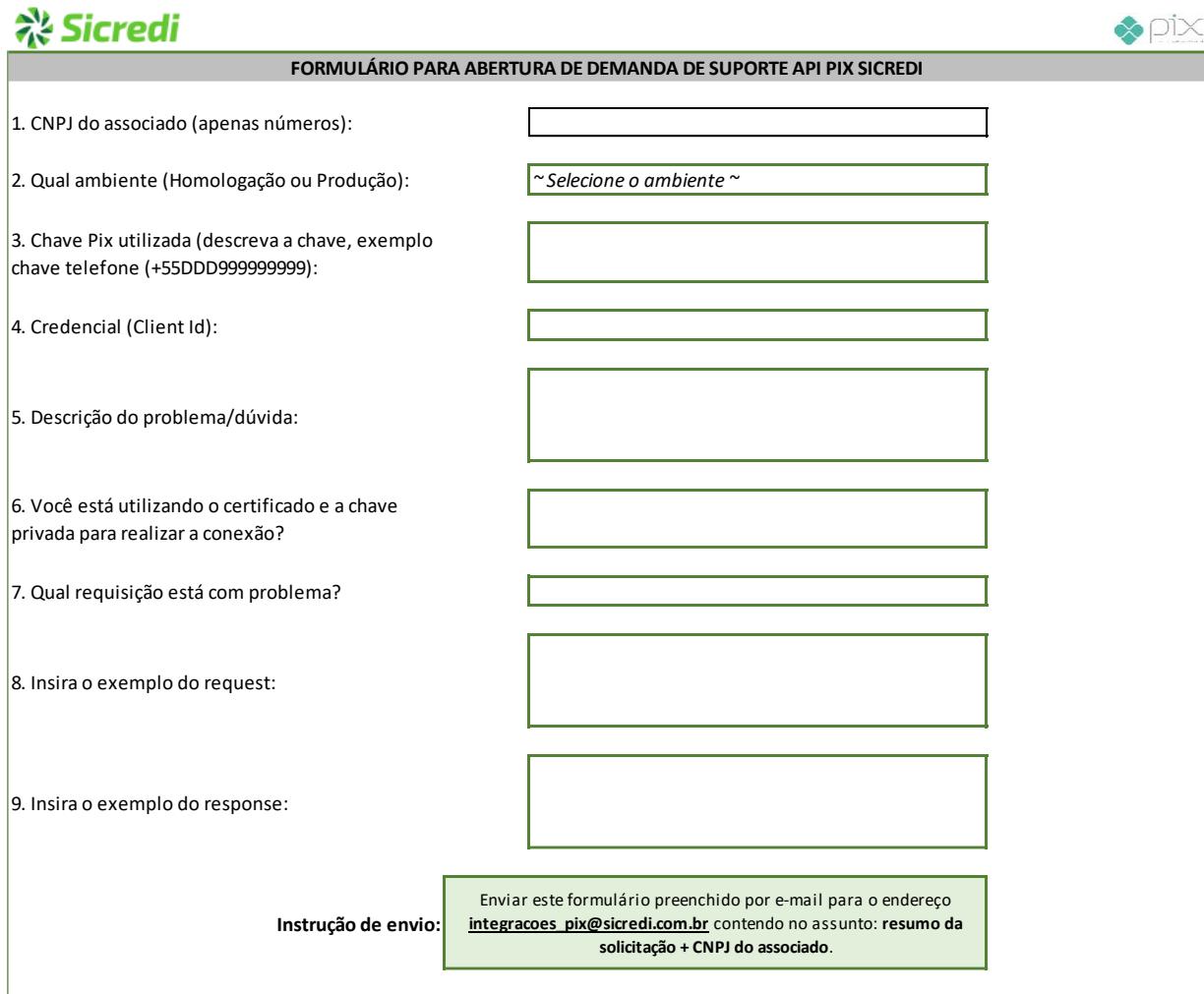
No caso de ser utilizado o sistema operacional Windows Server, a recomendação do Sicredi é de que seja de uma versão atualizada, que possua suporte da Microsoft. Nesse sentido, recomendamos a utilização de versões do Windows Server 2016 em diante.

- **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:



FORMULÁRIO PARA ABERTURA DE DEMANDA DE SUPORTE API PIX SICREDI

1. CNPJ do associado (apenas números):

2. Qual ambiente (Homologação ou Produção):

3. Chave Pix utilizada (descreva a chave, exemplo chave telefone (+55DDD9999999999)):

4. Credencial (Client Id):

5. Descrição do problema/dúvida:

6. Você está utilizando o certificado e a chave privada para realizar a conexão?

7. Qual requisição está com problema?

8. Insira o exemplo do request:

9. Insira o exemplo do response:

Instrução de envio: Enviar este formulário preenchido por e-mail para o endereço integracoes_pix@sicredi.com.br contendo no assunto: resumo da solicitação + CNPJ do associado.

Orientação para preenchimento dos itens 7, 8 e 9.

7. Qual requisição está com problema?

Neste campo deve ser informado o método do endpoint e a URL a qual destina a requisição desejada.

Por exemplo, na geração de cobrança:

HTTP Api Pix Sicredi / Cobrança / Criar cobrança

POST api-pix.sicredi.com.br/api/v2/cob

Neste caso, o método é **POST** e a URL é *api-pix.sicredi.com.br/api/v2/cob*.

Portanto, tomando como exemplo o caso acima, o campo de item 7 deve ser preenchido da seguinte forma: **POST:api-pix.sicredi.com.br**

8. Insira o exemplo do request

O Request é aquilo que está requerendo, em um caso como exemplo acima de criação de cobrança, é necessário incluir o .json da informação contida no Body da requisição. Ex:

```
{
  "calendario": {
    "expiracao": 3600
  },
  "devedor": {
    "cnpj": "12345678000195",
    "nome": "Empresa de Serviços SA"
  },
  "valor": {
    "original": "37.00",
    "modalidadeAlteracao": 1
  },
  "chave": "7d9f0335-8dcc-4054-9bf9-0dbd61d36906",
  "solicitacaoPagador": "Serviço realizado.",
  "infoAdicionais": [
    + { ... },
    + { ... }
  ]
}
```

9. Insira o exemplo do response

O Response, por sua vez, é a resposta que a API deu à requisição realizada, retornando o Status de sucesso/erro e demais detalhes. Ex:

```
{  
    "type": "https://pix.bcb.gov.br/api/v2/error/AcessoNegado",  
    "title": "Acesso Negado",  
    "status": 403,  
    "detail": "Requisição de participante autenticado que viola alguma regra de autorização."  
}
```

Este formulário está disponível no Portal do Desenvolvedor para download (<https://developer.sicredi.com.br/api-portal/pt-br/content/api-pix-documentacao>)

Atenção:

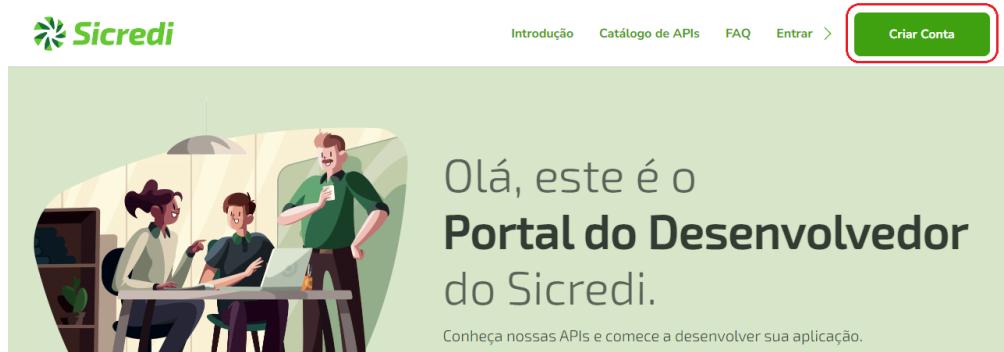
Nos casos de demanda sobre **Arrecadação Híbrida** (QRCode Dinâmico de Pix em boletos, carnês e demais documentos), o suporte a ser acionado deve ser o e-mail homologacoes_recebimentos@sicredi.com.br.

Anexo I – Passo-a-passo Portal Desenvolvedor

As etapas aqui indicadas exploram as atribuições a serem executadas pelo técnico integrador do associado através do Portal do Desenvolvedor, onde serão geradas todas as informações necessárias para a integração com a API Pix Sicredi de determinada conta.

Etapa 1: Acesso ao Portal Dev.

O técnico deverá acessar o Portal do Desenvolvedor Sicredi (<https://developer.sicredi.com.br>) e criar seu cadastro/conta de desenvolvedor em “Criar Conta”.



Após solicitação de criação de cadastro, receberá, no endereço informado, um e-mail para ativação da conta.

Etapa 2: Solicitação de acesso à API

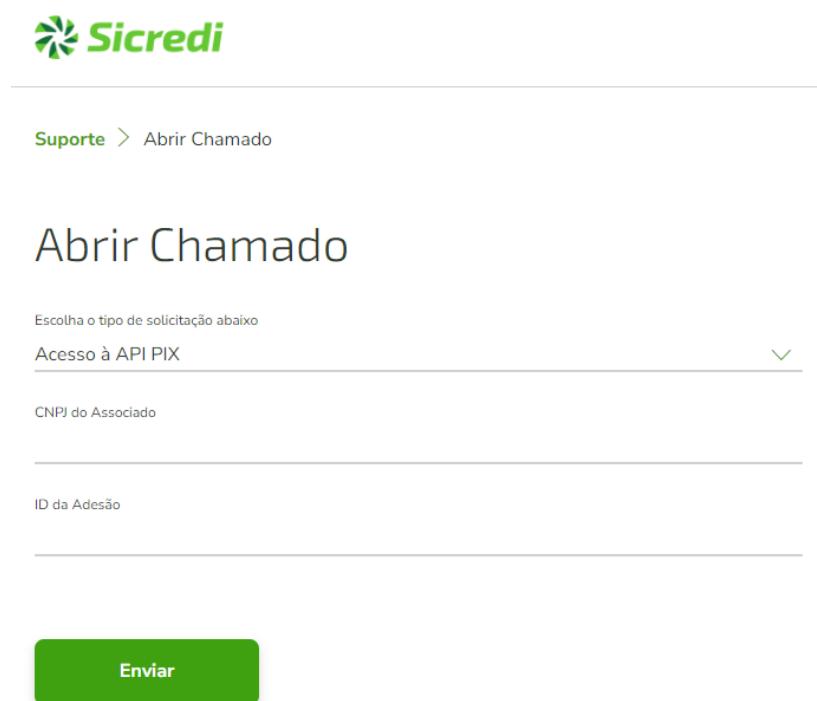
Ao efetuar o login no cadastro realizado no Portal do Desenvolvedor (Etapa 1), deverá ser solicitado o acesso à API da nova integração a ser realizada seguindo os passos abaixo:

Página Inicial Portal Dev. > Suporte > Abra um Chamado



<https://dev-sicredi.zendesk.com/hc/pt-br/requests/new>

Para integração à API Pix, o tipo de solicitação deverá ser selecionado “Acesso à API Pix” informando o CNPJ do associado e o ID de adesão (este encaminhado no e-mail de boas-vindas ao associado).

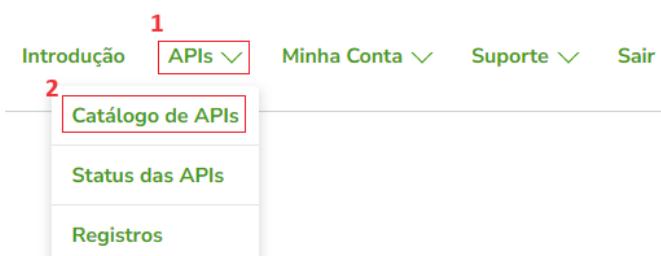


The screenshot shows a web form titled "Abrir Chamado". At the top, it says "Escolha o tipo de solicitação abaixo" and has a dropdown menu set to "Acesso à API PIX". Below the dropdown are two input fields: "CNPJ do Associado" and "ID da Adesão", both with placeholder text. At the bottom is a large green button labeled "Enviar".

O prazo de atendimento para resposta ao acesso solicitado é de 2 horas úteis, e o técnico receberá as atualizações da solicitação via e-mail.

Etapa 3: Geração de Certificado

Obtendo sucesso na solicitação da primeira integração a ser realizada via Portal do Desenvolvedor, o técnico terá acesso à *APIs de Recebimento* em *Catálogo de APIs*.



<https://developer.sicredi.com.br/api-portal/pt-br/content/catalogo-de-apis>



Em *APIs de Recebimento*, a troca de certificados e geração de credenciais ocorrem justamente em *Certificados e Credenciais*.

APIs de Recebimento

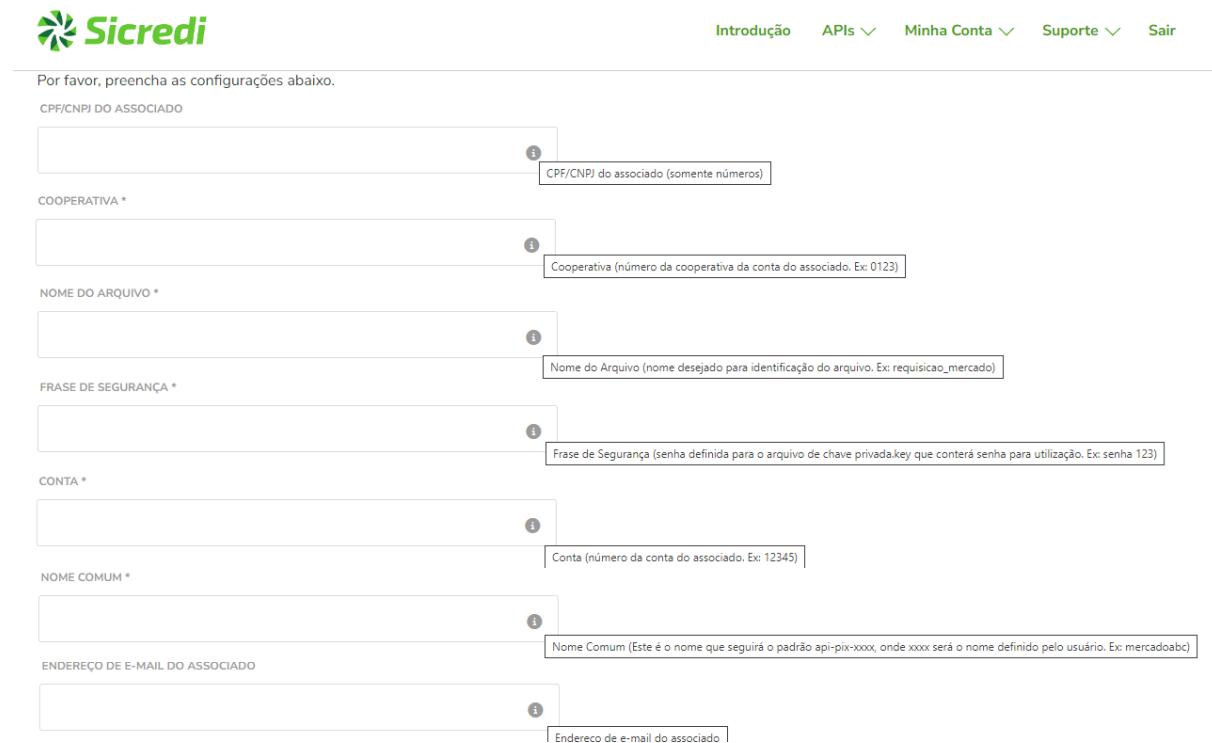
The screenshot shows a web-based API documentation interface for the Pix API. At the top right, there is a green button labeled 'V1.0.0'. Below it, the word 'Pix' is displayed next to a small hand icon. A subtitle reads 'Documentação para recebimento integrado através do Pix.' Underneath, there are two navigation links: 'Overview >' and 'Documentação >'. At the bottom of the main content area, there is a link 'Certificados e Credenciais >' which is highlighted with a red rectangular box.

Na tela seguinte já pode ser registrada a requisição de certificado (CSR) para a conta a ser integrada na API Pix clicando em “Registrar Novo CSR”.

The screenshot shows the Sicredi API portal. At the top, there is a navigation bar with the Sicredi logo, followed by links for 'Introdução', 'APIs', 'Minha Conta', 'Suporte', and 'Sair'. Below the navigation bar, there are two input fields: 'Cooperativa' (with placeholder 'Digite o número da cooperativa') and 'Conta' (with placeholder 'Digite o número da conta'). To the right of these fields is a green search icon. Further to the right is a green button with the text 'Registrar Novo CSR' enclosed in a red rectangular box.

https://developer.sicredi.com.br/api-portal/csr_certs/generate

Para registrar a requisição (CSR) deverá ser preenchido o formulário com as informações especificadas e detalhadas em cada campo no ícone **1**.



Por favor, preencha as configurações abaixo.

CPF/CNPJ DO ASSOCIADO

COOPERATIVA *

NOME DO ARQUIVO *

FRASE DE SEGURANÇA *

CONTA *

NOME COMUM *

ENDEREÇO DE E-MAIL DO ASSOCIADO

Após realizado o registro da requisição para a conta desejada, a tela abaixo surgirá para que o técnico já possa salvar o arquivo de Chave Privada (Com e Sem Senha).



Novo certificado *api-pix-testeyteste* criado com sucesso.

Para baixar o CSR, [click here](#).

To download the private key, [click here](#).

To download the private key without passphrase, [click here](#).

[Voltar para a lista](#)

*Recomendamos que os arquivos sejam salvos em pasta com nome que identifique o processo de integração desse associado, evitando que possam ocorrer trocas com arquivos de outros processos.

O acompanhamento da assinatura de certificado deve ser realizado através do acesso *APIs de Recebimento*, ou simplesmente clicando em “Voltar para a lista” na tela indicada acima.

A lista dos arquivos de cada conta liberada estará disponível a qualquer momento e por ela será realizada a geração das informações restantes: Download de Certificado Validado Sicredi; Download Chave Privada Sem Senha; Geração de Credencial de Produção.

Para este acesso, basta retomar em APIs > Catálogo de APIs > APIs de Recebimento e preencher os dados da conta a ser consultada.

Cooperativa	Conta	Registrar Novo CSR				
0116	471406					
Nome do Arquivo	Data de Importação	Data de Atualização	Usuário LDAP	Tipo	Status	⋮
testeyteste.csr	2024-02-18 00:52:11			CERTIFICADO_ORIGINAL	EM_PROCESSAMENTO	

<https://developer.sicredi.com.br/api-portal/pt-br/certificates>

O status “Em Processamento” indica que a requisição foi recebida pelo Sicredi e está sendo avaliada pela Segurança da Informação. Assim que validada, retornaremos o status “OK” contendo Certificado Validado Sicredi (.CER) para uso em conjunto com a Chave Privada (.KEY), a qual poderá ser baixada a partir da Requisição (CSR) anteriormente realizada conforme demonstração abaixo:

CadeiaCompletaSicredi.cer	2023-10-19 14:37:30	2023-10-19 14:37:30		CERTIFICADO_CADEIA	OK	
Certificado Validado Sicredi  certificado.cer	2023-10-19 14:37:19	2023-10-19 14:37:19		CERTIFICADO_VALIDADO	OK	
APLICACAO.csr	2023-10-19 14:33:08	2023-10-19 14:37:30		CERTIFICADO_ORIGINAL	OK	 
webhook-sicredi.cer	2023-07-17 14:10:47	2023-08-21 13:45:33		CERTIFICADO_ORIGINAL	OK	
webhook-sicredi.cer	2023-07-17 14:10:47	2023-08-21 13:45:33		CERTIFICADO_VALIDADO	OK	  Visualizar Certificado Download CSR Download Key Download Key (sem frase secreta)

Perceba que, após validada a requisição, foi disponibilizado o Certificado Validado (.CER) e que as operações em cima de cada arquivo podem ser realizadas conforme as opções que constam no ícone (⋮).

Etapa 4: Geração de Credencial de Produção

Com base no Certificado Validado (.CER) disponível na lista de arquivos da conta desejada, é possível a geração de credencial de produção (Client ID e Client Secret).

Cooperativa	Conta	Ações				
0116	471406					
Nome do Arquivo	Data de Importação	Data de Atualização	Usuário LDAP	Tipo	Status	⋮
CadeiaCompletaSicredi.cer	2024-02-18 01:44:33	2024-02-18 01:44:33	*** - ***	CERTIFICADO_CADEIA	OK	
Certificado Validado.cer	2024-02-18 01:44:21	2024-02-18 01:44:21	*** - ***	CERTIFICADO_VALIDADO	OK	 <div>Gerar nova Credencial Visualizar Certificado Download CER</div>
testeyteste.csr	2024-02-18 00:52:11	2024-02-18 01:44:33	*** - ***	CERTIFICADO_ORIGINAL	OK	

<https://developer.sicredi.com.br/api-portal/pt-br/certificates>

Insira o CPF/CNPJ do associado para a geração da credencial:

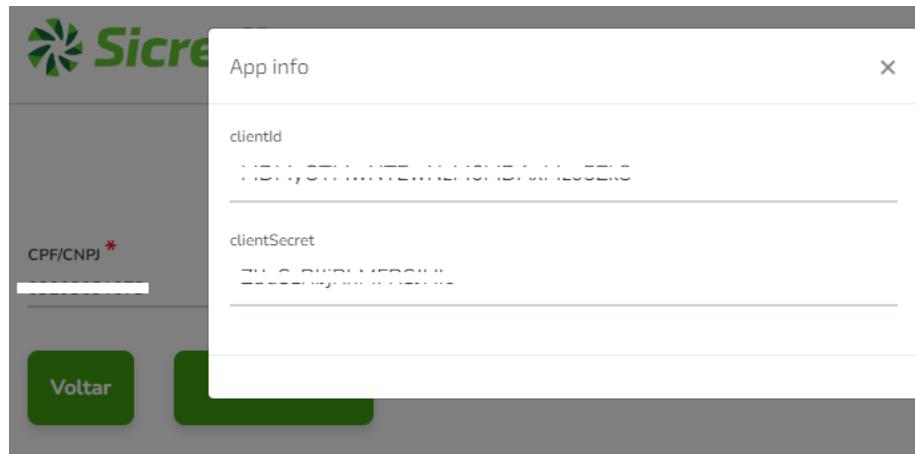


CPF/CNPJ *

 Voltar

 Registrar

Credencial Gerada com sucesso, podendo também ser consultada posteriormente no ícone () do certificado validado disponível na lista de arquivos da conta.



Pronto! Processo de geração de dados para integração com a API Pix concluído.

Anexo II – Postman e Collection

Certificados Sicredi - Autenticação TLS mútua

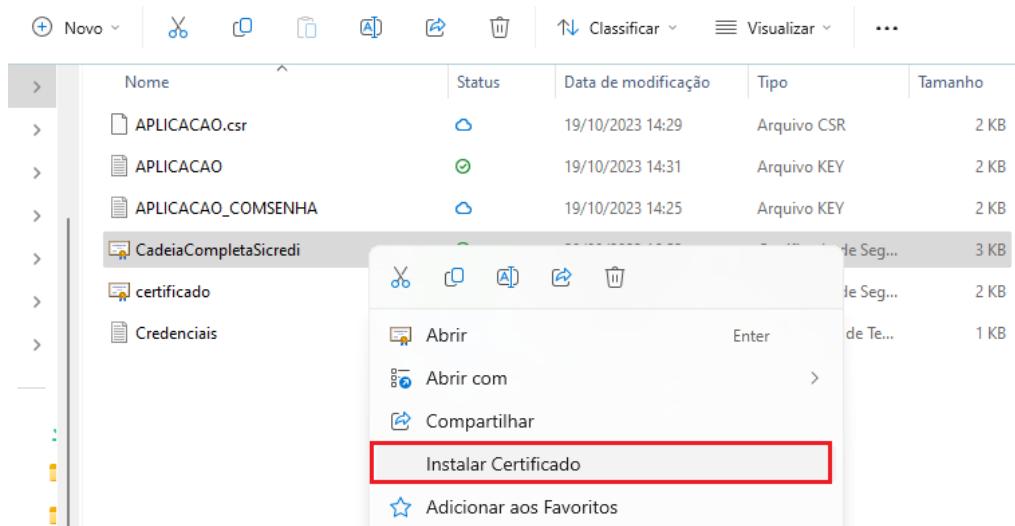
O objetivo desse anexo é auxiliar o público que tem posse de certificados Sicredi no processo de autenticação TLS mútua usando a ferramenta Postman.

O Postman (até a confecção desse documento) aceita apenas certificados com estrutura (PEM), e aqui ilustramos como verificar a estrutura do arquivo que possui e como utilizar as credenciais SSL (certificado e chave) para a autenticação mútua no Postman utilizando a Collection construída pelo Sicredi para facilitar a operação das requisições com a API Pix Sicredi.

Conferindo a estrutura do Certificado recebido e a chave privada

Você deve ter recebido a cadeia certificadora completa do Sicredi (CA), primeiramente, deve-se instalar esse certificado no wallet do sistema.

Exemplo Windows:



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

Após efetuar o download do Certificado validado Sicredi no Portal do Desenvolvedor, ele deve estar legível, sem informações em binário.

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



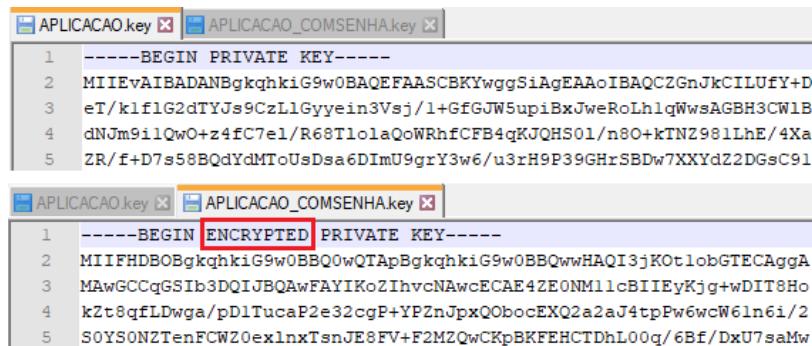
```
-----BEGIN CERTIFICATE-----  
MIIHzTCCBrWgAwIBAgITdQAByZxuWgXB+pWKgAAAAAFjDANBgkqhkiG9w0BAQsF  
ADCB4DESMBAGCgmSJomT8ixkARKwAmJyMRMwEQYKCZImiZPyLGQBGRYDbmV0MRCw  
FQYKCZImiZPyLGQBGRYHc2lJcmVkaTE4MDYGA1UEAxMvQXV0b3JpZGFkZSBZXJ0  
aWZpY2Fkb3JhIFN1Ym9yZGluYWRhIFNpY3J1ZGkgRzIxCzAJBgNVBAYTAKJSMUcw  
RQYDVQKExZ5Db25mZWRLcmFjYW8gSW50ZXJ1c3RhZHVhbCBkYXMgQ29vcGVyYXRp  
dmFzIExpZ2FkYXMyYW8gU2lJcmVkaTEMMaGCA1UEBRMDNTExMB4XDTExMDgyNjE2  
NTQ0FoXDTIzMDgyNjE2NTQ0OFowgfUxCzAJBgNVBAYTAKJSMRowGAYDVQQIExFS  
aW8gR3JhbmrLIGRvIFN1bDEVMBMGAAUEBxMMG9ydG8gQWx1Z3J1MUcwRQYDVQQK  
EZ5Db25mZWRLcmFjYW8gSW50ZXJ1c3RhZHVhbCBkYXMgQ29vcGVyYXRpdnFzIExp
```

Essa estrutura, indica que o arquivo possui o formato (PEM), o qual é recomendado para utilização nas mais diversas aplicações.

Caso o arquivo possua uma estrutura com informações em binário (ou diferente da apresentada na imagem acima) ele estará com a estrutura (DER) e deverá passar por uma conversão para garantir que via Postman e a aplicação a ser utilizada pelo associado o arquivo funcione da maneira desejada.

Atenção: é comum (até a data de criação deste Guia) que os arquivos de certificado baixados diretamente do Internet Banking possuam a estrutura contendo informações em binário (DER), exigindo tal conversão de (DER) para (PEM).

Quanto à **chave privada**, é recomendado o download da Chave Privada Sem Senha no Portal do Desenvolvedor. Abaixo telas de comparativo indicando a existência de senha no arquivo de chave privada .key quando existente a palavra ENCRYPTED no header do arquivo:



```
-----BEGIN PRIVATE KEY-----  
MIIEwAIBADANBgkqhkiG9w0BAQEFAASCBKYwggSiAgEAAoIBAQZGnJkCILUFY+D  
eT/k1f1G2dTYJs9CzLlGyyein3Vsj/1+GfGJW5upiBxJweRoLhlqWwsAGBH3CW1B  
dNjm9i1Qw0+z4fc7e1/R68T1olaQoWRhfCFB4qKJQHS01/n8O+kTNZ981LhE/4xa  
ZR/f+D7s58BQdYdMToUsDsaa6DimU9grY3w6/u3rH9P39GhrSBDw7XXYdZ2DGsC91  
-----BEGIN ENCRYPTED PRIVATE KEY-----  
MIIFHDBOBgkqhkiG9w0BBQ0wQTApBgkqhkiG9w0BBQwwHAQI3jK0tlobGTECAggA  
MAwGCCqGS1b3DQIJBQAwFAYIKoZIhvcNAwcECAE4ZEONM11cBIIEyKjg+wDIT8Ho  
kZt8qfLDwga/pDITucaP2e32cgP+YPZnJpxQObocEXQ2a2aJ4tpPw6wcW6ln6i/2  
SOYS0NZTenFCWZ0exlnxTsnJE8FV+F2M2QwCKpBKFEHCTDhL00q/6Bf/DxU7saMw
```

Instruções para a conversão do arquivo de certificado no Anexo V – Extra.



Primeiro acesso ao Postman e a importação da Collection API Pix Sicredi

O que é e para que serve o Postman?

O Postman é uma ferramenta popular usada por desenvolvedores e equipes de desenvolvimento de software para testar, documentar e colaborar em APIs (Application Programming Interfaces). Ele oferece uma interface gráfica amigável que permite enviar solicitações HTTP para APIs e receber as respostas correspondentes.

Portanto, possui ambiente para a documentação e execução de testes de APIs.

O que é e para que serve a Collection?

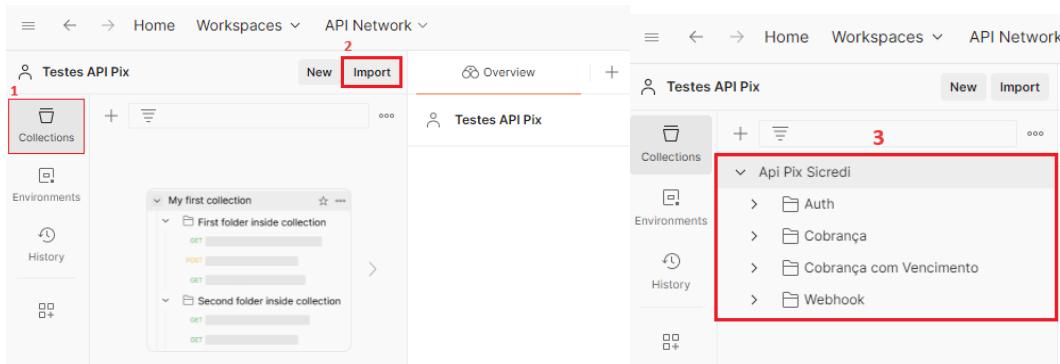
O Postman Collection é uma coleção de links de API, com seus respectivos métodos (POST, GET, PUT etc.) e demais configurações de envio como headeres, body, entre outros.

Essa Collection da API Pix o Sicredi gerou para teste e uso em sua realidade para dar exemplos prontos de uso para os associados.

Aqui neste documento, demonstraremos a configuração utilizando a Collection API Pix Sicredi para execução de testes da API Pix com o ambiente Sicredi.

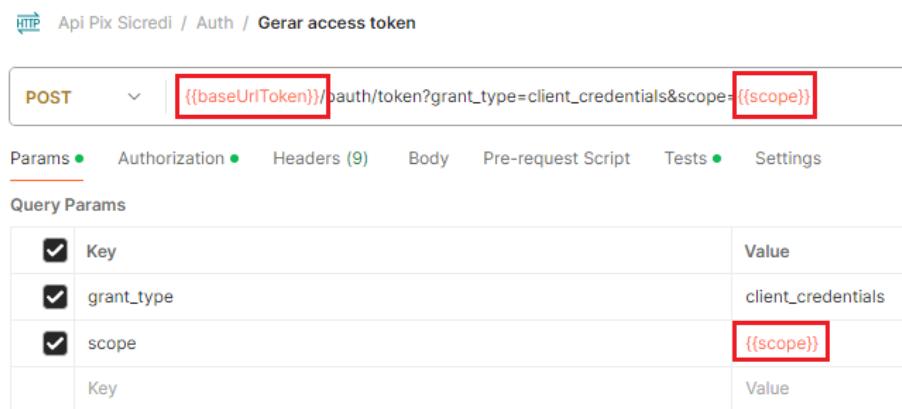
Dito isso, o Postman poderá ser baixado gratuitamente (<https://www.postman.com/downloads>) sendo necessário também um cadastro de conta gratuita para iniciar as configurações e testes. E o arquivo de *Collection API Pix Sicredi* com extensão “.json” está disponível na documentação do Portal do Desenvolvedor em (Página Inicial > APIs > Catálogo de APIs > API de Recebimento – Documentação)

Após realizado com sucesso o cadastro e logo ao obter o aplicativo do Postman em sua máquina e abri-lo, obterá a tela inicial, onde nela deverá ser realizada a importação da Collection API Pix Sicredi:



Em Collections (1) clique em “Import” (2) e realize a importação do arquivo collection.json. A importação do arquivo será realizada conforme demonstrado na tela acima (3).

Consultando brevemente as subpastas com as requisições estruturadas é possível identificar que existem `{strings}` que consomem/puxam informações da tela de *Variables*, a qual veremos abaixo como se dão as configurações dessas informações a serem inseridas automaticamente nos campos de `{string}`.



Key	Value
grant_type	client_credentials
scope	<code>{{{scope}}}</code>
Key	Value

Outro ponto, é que as demais requisições que exigem informações a serem registradas no Body da requisição, a Collection da API Pix Sicredi já possui a estrutura esperada pelo Bacen, devendo apenas ser alterados/informados os valores desejados.

POST {{baseUrl}}/api/v2/cob

Params Authorization Headers (10) Body Pre-request Script Tests Settings

none form-data x-www-form-urlencoded raw binary GraphQL JSON

```

1  {
2    "calendario": {
3      "expiracao": 3600
4    },
5    "devedor": {
6      "cnpj": "12345678000195",
7      "nome": "Empresa de Serviços SA"
8    },
9    "valor": {
10      "original": "0.13",
11      "modalidadeAlteracao": 1
12    },
13    "chave": "{{chavePix}}",
14    "solicitacaoPagador": "Serviço realizado."

```

Configurando as informações e credenciais do associado no Postman

Antes de acessar as subpastas das requisições da API Pix Sicredi (1) na Collection, deve-se configurar em *Variables* (2) as informações de endpoints URL (3) (produção e homologação), escopos (4) chave Pix (5) e credenciais (6) (Client ID e Client Secret), salvando-as (7) para posteriormente prosseguir com requisições. Abaixo tela exemplificando um cadastro teste:

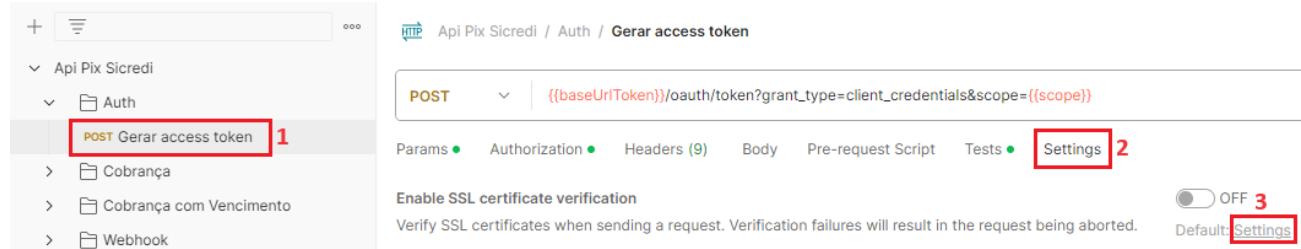
The screenshot shows the Postman interface with the collection 'Api Pix Sicredi' selected. The 'Variables' tab is active, indicated by a red box and the number '2'. The table lists variables with their initial and current values:

	Variable	Initial value	Current value
3	baseURL	https://api-pix-h.sicredi.com.br	https://api-pix-h.sicredi.com.br
3	baseURLToken	https://api-pix-h.sicredi.com.br	https://api-pix-h.sicredi.com.br
4	scope	cob.write+cob.read+webhook.read+webhook.write	cob.write+cob.read+webhook.read+webhook.write
5	chavePix		
6	clientId		
6	clientSecret		
	token	não preencher	não preencher
	txid	não preencher	não preencher
	dataInicio	não preencher	não preencher
	dataFim	não preencher	não preencher

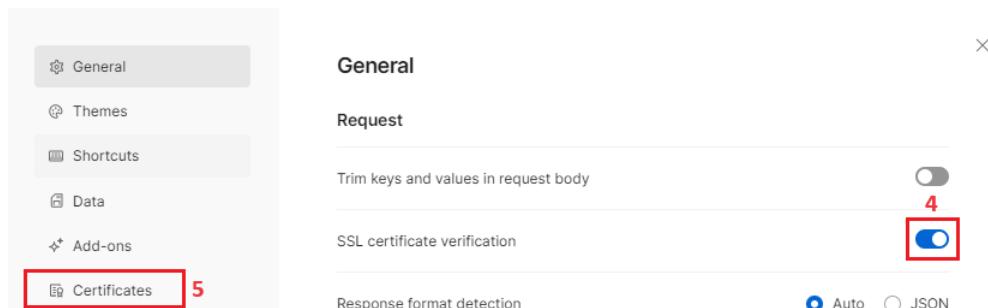
- Perceba que as informações preenchidas devem ser inseridas igualmente em ambas as colunas “Initial value” e “Current value”.

Configurando o Certificado e a Chave Privada que serão utilizados na autenticação mTLS na API Pix e gerando o token

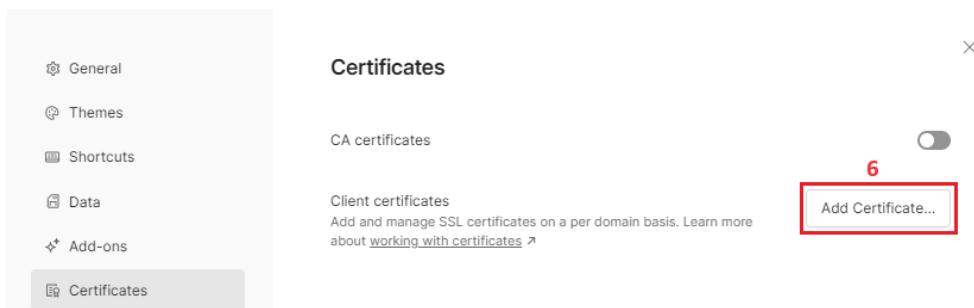
Agora, na primeira subpasta da Collection (Auth) em “Gerar access token” (1), clique em Settings (2) e em *Enable SSL certificate verification* clique em Settings (3).



Na tela aberta, habilite o *SSL certificate verification* (4) e clique em Certificates (5) para acessar o ambiente a ser inserido os arquivos de certificado e chave privada.



Adicione os arquivos (Certificado e Chave Privada.key) e defina a URL desejada para as requisições a serem realizadas.





Na tela de Add Certificate, insira o endpoint URL (7) do ambiente desejado (neste exemplo de produção: `api-pix.sicredi.com.br`), insira o arquivo de certificado (.CER) contendo estrutura (PEM) (8), insira a Chave Privada SEM SENHA (9) e clique em “Add” (10).

- [General](#)
- [Themes](#)
- [Shortcuts](#)
- [Data](#)
- [Add-ons](#)
- [Certificates](#)
- [Proxy](#)
- [Update](#)
- [About](#)

Add certificate

Host (required)

: 443

CRT file

7

KEY file

9

PDF file

Passphrase

⑩

10
[Add](#)
[Cancel](#)

Learn more about [working with certificates](#) ↗

Client certificates

Add and manage SSL certificates on a per domain basis. Learn more about [working with certificates](#) ↗

[Add Certificate...](#)

HOST	api-pix.sicredi.com.br
CRT file	/C:/Users/filippo_villa/OneDrive - Sicredi/Desktop/Certifica...
KEY file	/C:/Users/filippo_villa/OneDrive - Sicredi/Desktop/Certifica...

Pronto! Considerando essas configurações, a Collection está devidamente cadastrada levando em conta os dados corretos inseridos do associado apta a realizar a primeira requisição de token nessa mesma seção (API Pix Sicredi / Auth / Gerar access token) clicando em “Send” (11):

HTTP Api Pix Sicredi / Auth / Gerar access token Save ↻

Obtendo o response de *status 200 OK*, token gerado:

Anexo III – 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 Interações 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, no momento da 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. Havendo necessidade de inclusão de mais escopos, o associado deverá solicitar à sua cooperativa a adição da modalidade de recebimento via API Pix correspondente.

Exemplo de resposta status 400 (Escopo vazio):

```
1 [ {  
2   "type": "https://pix.bcb.gov.br/api/v2/error/RequisicaoInvalida",  
3   "title": "Requisição inválida.",  
4   "status": 400,  
5   "detail": "Escopo vazio (o usuário não tem permissão para solicitar escopos)"  
6 } ]
```

O detalhe (detail) do Response da requisição informa o ocorrido: Para esta credencial, os escopos/funcionalidades de cobrança não foram habilitados. Nesse caso deverá ser verificado junto ao associado se a solicitação de integração foi realizada para a cooperativa e se já foi atendida pela equipe responsável.

Exemplo de resposta status 400 (Escopo Negado):

```
1 [ {  
2   "type": "https://pix.bcb.gov.br/api/v2/error/RequisicaoInvalida",  
3   "title": "Requisição inválida.",  
4   "status": 400,  
5   "detail": "Escopo negado (o usuário não tem acesso ao escopo solicitado): cobv.read"  
6 } ]
```

O detalhe (detail) do Response da requisição informa o ocorrido: Esta credencial não possui os escopos de cobrança com vencimento (COBV) habilitados. Nesse caso deverá ser verificado pelo associado se o mesmo solicitou os escopos de cobrança com vencimento na demanda de integração aberta pela cooperativa.

➔ Chave Pix não encontrada

- **Orientação:** Verificar se a chave Pix informada já está cadastrada.

Exemplo de resposta status 400 (Chave Pix não localizada):

```
1  [
2      "type": "https://pix.bcb.gov.br/api/v2/error/CobOperacaoInvalida",
3      "title": "Cobrança inválida.",
4      "status": 400,
5      "detail": "A requisição que busca alterar ou criar uma cobrança para
6          pagamento imediato não respeita o schema ou está semanticamente errada.",
7      "correlationId": "fc105e34-12615826",
8      "violacoes": [
9          {
10              "razao": "Não foi localizada a chave informada",
11              "propriedade": "cob.chave"
12          }
13      ]
14 ]
```

Esse Response apresenta em Razão a violação ocorrida: Na tentativa de criação de cobrança, a chave Pix parametrizada não foi encontrada no PSP Sicredi, ou seja, não foi informada corretamente na configuração da API, ou ainda, não está devidamente cadastrada para o associado no Sicredi.

Recomenda-se verificar se a chave foi corretamente informada pelo técnico na configuração da API e se está cadastrada para o associado em sua conta Sicredi.

➔ Crítica de thumbprint incorreto.

- **Orientação:** falha na validação mTLS, o certificado não foi enviado na requisição, ou é diferente do que foi cadastrado com as credenciais Client_id e Client_secret que estão sendo utilizadas. Neste caso, deve-se revisar a configuração do uso do certificado na chamada. Pode ocorrer também de ter sido gerada a credencial com base no certificado incorreto. Neste caso, o técnico deverá refazer a geração das credenciais no Portal do Desenvolvedor, selecionando o certificado correto assinado pelo Sicredi para a integração.

Status 401

➔ “Cannot convert access token to JSON”:

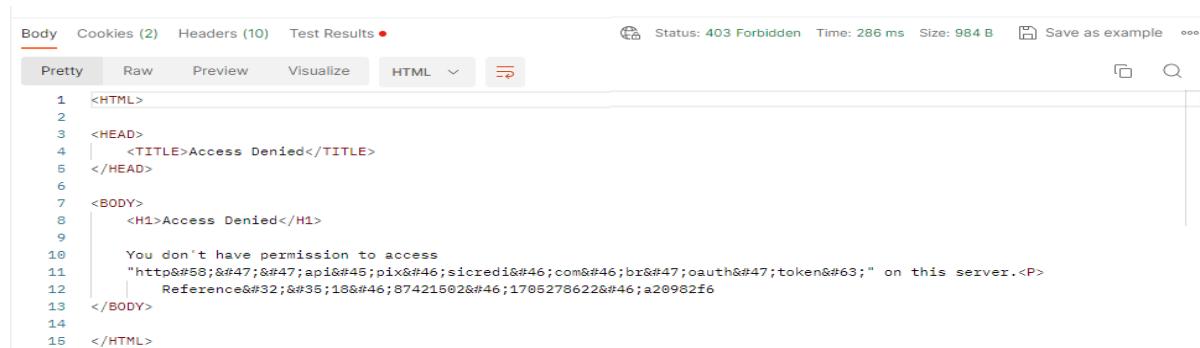
- **Descrição:** Não foi possível converter o token de acesso para o formato esperado.
- **Orientação:** Enviar o token no mesmo formato que foi recebido, pois pode ter ocorrido uma codificação ou conversão de dados antes do envio.

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 no Portal do Desenvolvedor);
 - Chave APPLICACAO.KEY gerada pra fazer a requisição do certificado;
 - Cadeia completa (disponibilizado no Portal do Desenvolvedor).

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

Exemplo de resposta status 403 (Acesso Negado):



```
Body Cookies (2) Headers (10) Test Results • Status: 403 Forbidden Time: 286 ms Size: 984 B Save as example ...  
Pretty Raw Preview Visualize HTML 🔍  
1 <HTML>  
2  
3 <HEAD>  
4 |   <TITLE>Access Denied</TITLE>  
5 </HEAD>  
6  
7 <BODY>  
8 |   <H1>Access Denied</H1>  
9  
10 You don't have permission to access  
11 "http://&#58;&#47;api&#46;pix&#46;sicredi&#46;com&#46;br&#47;oauth&#47;token&#63;" on this server.<P>  
12 Reference:&#32;&#35;18&#46;87421502&#46;1705278622&#46;a20982f6  
13 </BODY>  
14  
15 </HTML>
```

Mensagem mais frequente e comum para o erro 403 nas integrações e que também demanda maior análise técnica da causa raiz da impossibilidade de acesso.

Daqui, podemos ter diversas possibilidades, tais como:

- Certificado (CER) e Chave Privada (KEY) não correspondem um ao outro. No Anexo XXX Extras é possível verificar como conferir a relação entre os arquivos.
- Técnico está inserindo os arquivos incorretos. Ex: No lugar do Certificado (CER), está sendo inserida a Requisição (CSR).

- Técnico está inserindo os arquivos em formato diferente do disponibilizado via Portal do Desenvolvedor. No Anexo XXX Extras é possível verificar o formato e os comandos para conversão.

➔ “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.

```
1  {
2    "type": "https://pix.bcb.gov.br/api/v2/error/AcessoNegado",
3    "title": "Acesso Negado",
4    "status": 403,
5    "detail": "Full authentication is required to access this resource"
6 }
```

O detalhe (detail) do Response indica que há problema na Credencial (Client ID e Client Secret) fornecida pelo técnico na requisição, informando que todas as autenticações necessárias para realizar o acesso à requisição desejada precisam ser cumpridas, e neste caso está sendo válido apenas Certificado e Chave Privada, mas a credencial não está cumprindo o devido papel para concluir a autenticação mTLS.

Nesse caso, orientamos que o técnico reveja a credencial, pois pode haver erro de digitação e/ou outras inconsistências entre Client ID e Client Secret. Ou ainda, a credencial informada não pertencer ao ambiente (Produção ou Homologação) requisitado.

Não havendo solução encontrada, recomenda-se geração de nova credencial.

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.

Atenção:

Diante response de status 500, certificar-se de que esse é o Response real da API para a requisição solicitada. Há aplicações/sistemas que retornam em seu log o status 500, porém quando realizado o teste via Postman é apresentado um erro diferente do status 500, o qual estava “mascarado” pela impossibilidade de leitura/organização do retorno da API pela aplicação utilizada, retornando o erro genérico de status 500.

Portanto, a recomendação inicial é de que obtendo erro de status 500 em aplicações que não sejam o Postman, realize um teste da requisição desejada utilizando o Postman com suporte dos passos indicados no Anexo II – Postman e Collection.

Permanecendo o erro 500, siga a orientação indica na Descrição desta seção.

Anexo IV – Geração Manual de Requisição (CSR) para assinatura de Certificado da API Pix Sicredi

Atenção:

Este recurso, atualmente, não é o mais recomendado em vista da disponibilidade das funcionalidades através do Portal do Desenvolvedor, descrito anteriormente neste **Guia no item 7**.

No entanto, as orientações que aqui constam servem para atender a necessidade da troca de certificados para o associado em detrimento de qualquer indisponibilidade na utilização do Portal do Desenvolvedor visando atender emergencialmente as necessidades do associado.

1º passo

Gerar o arquivo de chave (.key)

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

winpty openssl genrsa -des3 -out CHAVE.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).
- Para maior compatibilidade de comandos em ambiente Windows é interessante prefixar todo o comando com **winpty**.

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

Enter pass phrase for CHAVE.key:

Verifying - Enter pass phrase for CHAVE.key:

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

2º passo

Gerar Requisição de Certificado (.csr).

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

```
winpty openssl req -new -key CHAVE.key -sha256 -out REQUISICAO.csr -subj  
'//C=BR/O=Confederacao Interestadual das Cooperativas Ligadas ao  
Sicredi/CN=api-parceiros-{NOME_PARCEIRO}.sicredi.net/ST=RS/L=Porto  
Alegre/jurisdictionCountryName=BR/OU=API Pix  
Sicredi/serialNumber=urn:cpfcnpj:{CPF_CNPJ_PARCEIRO}'
```

Recomendações:

- Obrigatoriamente o campo {NOME_PARCEIRO} deve ser substituído por nome contendo caracteres minúsculos. Em caso de integração individual, indicar nome principal da razão social do associado, e para geração de certificado para parceiro API Pix Sicredi indicar nome fantasia.
- O campo {CPF_CNPJ_PARCEIRO} deverá ser preenchido com CPF ou CNPJ do proprietário do certificado contendo apenas números. Ex: 12345678000123. Em caso de CPF, o comando “urn:cnpj” não deve ser alterado, permanecerá urn:cnpj ainda que seja informado CPF como resultado.
- Para maior compatibilidade de comandos em ambiente Windows é interessante prefixar todo o comando com **winpty**.

Neste passo será solicitada a frase secreta cadastrada no passo 1, ao digitá-la o arquivo de REQUISICAO.csr será gerado no diretório utilizado.

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 CHAVE.key CHAVE_COMSENHA.key  
winpty openssl rsa -in CHAVE_COMSENHA.key -out CHAVE.key
```

Anexo V – Extra

Extensão dos arquivos (.CER; .KEY; .PEM; .PFX etc)

Tenha cuidado ao renomear a extensão de arquivos. Isso não vai mudar o tipo de arquivo. Apenas software de conversão especial (ex: SSL) pode mudar um arquivo de um tipo para outro.

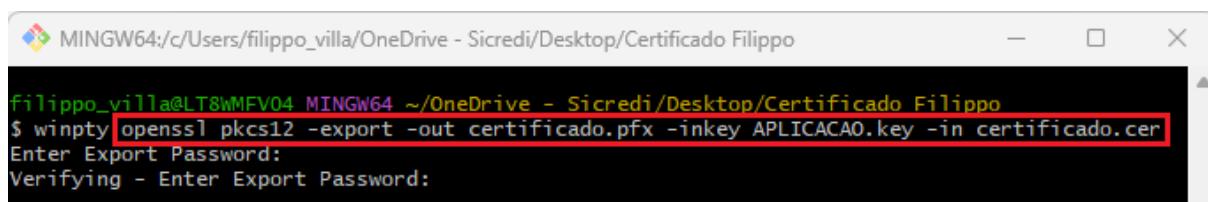
Conversão dos arquivos Certificado (.CER) e Chave Privada (.KEY) para Certificado (.PFX)

Existem aplicações que operam apenas com a configuração de um arquivo único de certificado com a extensão .PFX. No caso em que é apresentado neste documento, o Certificado (.PFX) convertido será basicamente a união dos arquivos de Certificado (.CER) e Chave Privada (.KEY), e por isso requer que esses arquivos possuam relação e, envolvendo o arquivo de chave privada (.KEY) – obrigatoriamente –, exigirá a criação de uma senha para o novo Certificado (.PFX), a qual será solicitada durante o processo de conversão a partir do comando descrito abaixo.

Utilizando um software SSL, introduza o comando abaixo para que o software identifique os arquivos de Certificado (.CER) e Chave Privada (.KEY) necessário para realizar a conversão em (.PFX):

```
openssl pkcs12 -export -out certificado.pfx -inkey privatekey.key -in certificado.cer
```

Os nomes dos arquivos descritos no comando podem mudar conforme nomenclatura que estes possuem na máquina onde está sendo processada a conversão.



A screenshot of a terminal window titled 'MINGW64:/c/Users/filippo_villa/OneDrive - Sicredi/Desktop/Certificado Filippo'. The command entered is: \$ winpty openssl pkcs12 -export -out certificado.pfx -inkey APLICACAO.key -in certificado.cer. Below the command, it says 'Enter Export Password:' and 'Verifying - Enter Export Password:'. The terminal window has a dark background with white text.

Será criado um arquivo de certificado (.PFX) no diretório onde o software SSL estiver sido operado.

 certificado.pfx  10/03/2024 21:58 Troca de Informações Pessoais 3 KB



Conversão da estrutura do arquivo Certificado de (DER) para (PEM)

Primeiramente é importante ressaltar que nesta conversão estamos falando da estrutura do conteúdo do arquivo, e não de sua extensão/tipo de arquivo, que permanece (.CER).

Há casos em que o download do arquivo de Certificado (.CER) tenha ocorrido diretamente no Internet Banking Sicredi, ou por algum outro motivo venha a apresentar a estrutura (DER) contendo informações codificadas, sendo possível verificar este cenário rapidamente abrindo o arquivo de certificado como texto:

Arquivo	Editar	Exibir
0,0;0,0§ 00000000000000'no{ÔÄr_oÿFò(zö0		
0 *tHt+:		
00		
0 00ž1		
0 00U0000BR100000U0000Rio Grande do Sul10000U0 0		
Porto Alegre10000U0		
0 SICREDI1:080000001Autoridade Certificadora Subordinada Sicredi 2040000		
24021804423Z#		
260217164302Z0r1		
0 00U0000BR100000U0000Rio Grande do Sul10000U0 0		
Porto Alegre10000U0		

Diante dessa estrutura conhecida como DER, existe a necessidade da conversão para PEM utilizando um software SSL e executando o seguinte comando:

```
openssl x509 -inform der -in certificado.cer -out certificado_novo.pem
```

Os nomes dos arquivos descritos no comando podem mudar conforme nomenclatura que estes possuem na máquina onde está sendo processada a conversão.

O novo arquivo PEM gerado deve possuir a estrutura visualmente identificada como na imagem:

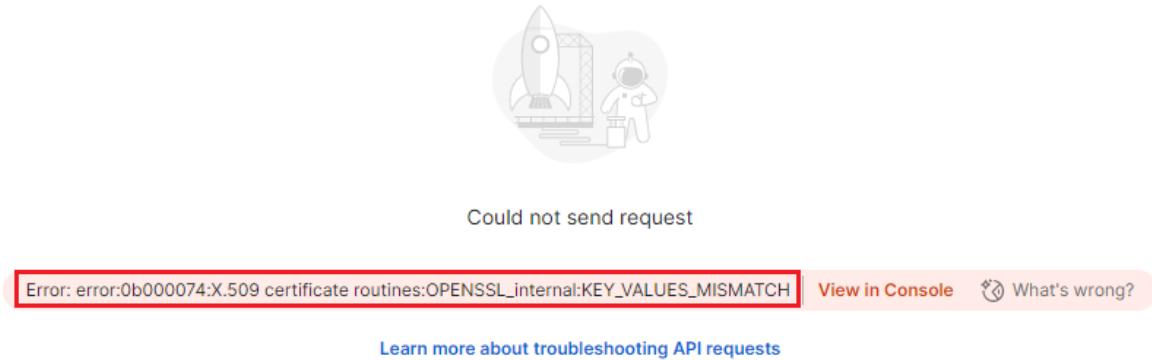
Arquivo Editar Exibir

-----BEGIN CERTIFICATE-----

MIIElwTCCAG6mgAwIBAgIUExVrX8cnK+3UYjMguOfbNwtDLKUwDQYJKoZIhvcaNAQELBQAwgY4xzcAJBgNVBAYTAKJSMRowGAYDVQQIEFsaw8gR3Jhbmr1IGRvIFN1bDEVMBMGAA1UEBcMUUG9ydG8QwLz331MRawDgYDVQQKEwdTSUNSRURJMtoOAYDVQDQEZFBdXRvcmlkYWR1IEN1cnRpZmJ1YWRvcmEgU3Vib3JkaW5hZGEGu21jcmVkaSAYMDQwB4XTD10MDIwOTESMjIwMVoXDTI2MDIwOTA3MjIzM沃czELMAKGA1UEBhMCQIxGjAYBgNVBAgTEVJpbjyBHCmfUzGUGzG8gU3VsMRUwEwDVQHExw0b3J0byBBbGVncmUxEDA0BgNVBAoTB1NJQ1JFREkxhZAdBgNVBAMFfMfwS1waXgtNDcx0TA4NjQwMDAx0DCwggeI1MA0GCScgS1b3DQEBAQUAA4IDwAwggeEKAoIBAQCcfa4NlwwY5E3PQT0bpnry6qYR0yWUYSVEDaSism7pkp45EvvnWZns+6XNMxu0zxbwa6KDZV3n12AAT7fsuPdxNtH/0+f+Pw0WkkpI#P1471YF+0hTxv/4m41FT+n/GF11RwUPF

Verificação de correspondência entre arquivos de Certificado (.CER) e Chave Privada (.KEY)

Essa verificação poderá ser realizada quando persistir erro ao acesso da API Pix e os testes indicados via *Postman* trouxerem a seguinte mensagem:



`KEY_VALUES_MISMATCH` indica que o Certificado e a Chave Privada não possuem correspondência, ou seja, não está sendo utilizada a Chave Privada que originou a requisição para assinatura deste Certificado disponibilizado pelo Sicredi.

Além da conclusão da mensagem já definida pelo *Postman*, poderá ser realizada uma conferência manual utilizando um software SSL.

Os comandos indicados retornarão o MD5 (algoritmo de digestão de mensagens), que é um protocolo criptográfico usado para autenticar mensagens, bem como verificação de conteúdo e assinaturas digitais. MD5 é baseado em uma função *hash* que verifica se um arquivo enviado corresponde ao arquivo recebido da instituição a quem você enviou.

Dessa forma, insira os comandos abaixo para obter o MD5 de cada um dos arquivos

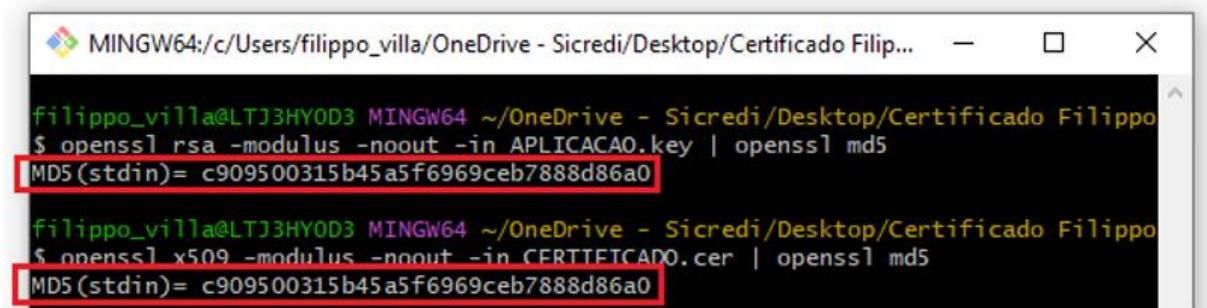
MD5 (stdin) da Chave Privada:

```
openssl rsa -modulus -noout -in name.key | openssl md5
```

MD5 (stdin) do Certificado:

```
openssl x509 -modulus -noout -in name.cer | openssl md5
```

Para que os arquivos de Certificado e Chave Privada possuam correspondência, deverão apresentar os mesmos códigos MD5:



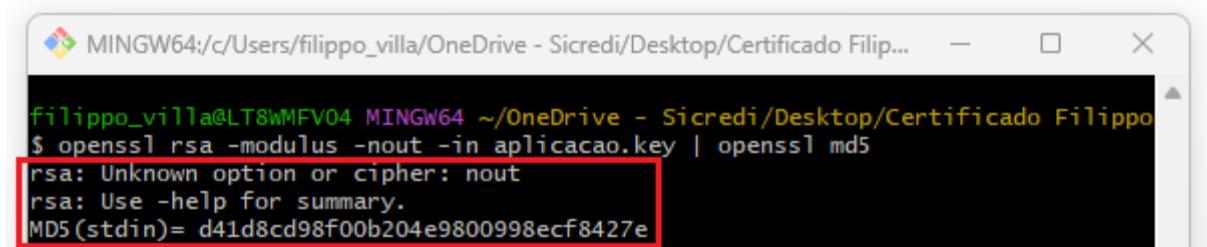
```
filippo_villa@LTJ3HY0D3 MINGW64 ~/OneDrive - Sicredi/Desktop/Certificado Filippo
$ openssl rsa -modulus -noout -in APPLICACAO.key | openssl md5
MD5(stdin)= c909500315b45a5f6969ceb7888d86a0

filippo_villa@LTJ3HY0D3 MINGW64 ~/OneDrive - Sicredi/Desktop/Certificado Filippo
$ openssl x509 -modulus -noout -in CERTIFICADO.cer | openssl md5
MD5(stdin)= c909500315b45a5f6969ceb7888d86a0
```

Caso os códigos sejam diferentes, indica que os arquivos não possuem correspondência e será necessário identificar onde está a chave privada correta que possui relação com o certificado disponível. Se não encontrado, deverá ser realizada nova requisição obtendo nova Chave Privada e Certificado assinado Sicredi.

Atenção:

É comum que o software SSL responda com um MD5 padrão quando não conseguir executar corretamente o comando desejado, então junto ao código MD5 também surge mensagem da incompatibilidade com o comando inserido. Será necessário revisar o comando inserido.



```
filippo_villa@LT8wMFV04 MINGW64 ~/OneDrive - Sicredi/Desktop/Certificado Filippo
$ openssl rsa -modulus -nout -in aplicacao.key | openssl md5
rsa: Unknown option or cipher: nout
rsa: Use -help for summary.
MD5(stdin)= d41d8cd98f00b204e9800998ecf8427e
```