

---

# **Guia Técnico Integrações**

## **API Pix Sicredi**

---

## Sumário

1. Apresentação .....	3
2. Objetivo .....	3
3. Público-alvo da solução de integração.....	3
3. Funcionalidades da API Pix.....	3
5. Jornada de adesão e implementação Sicredi.....	5
6. Passo a passo da jornada no Sicredi .....	6
7. Implementação via Portal do Desenvolvedor .....	6
8. Fluxo de Requisições da API Pix Sicredi.....	9
9. Documentação Bacen em relação à API Pix.....	12
10. Webhook.....	13
11. Recomendações.....	15
12. Suporte.....	17
Anexo I – Passo-a-passo Portal Desenvolvedor.....	18
Anexo II – Postman e Collection .....	25
Anexo III – Pix Automático Recebedor .....	32
Anexo IV – Erros Frequentes.....	40
Anexo V – Geração Manual de Requisição (CSR) para assinatura de Certificado da API Pix Sicredi.....	46
Anexo VI – Extra .....	48

## 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, sejam elas Pagamentos Imediatos, Pagamento com vencimento Futuro e Pagamentos recorrentes através da solução de Pix Automático.

## 3. Funcionalidades da API Pix

As especificações e seus respectivos *endpoints* para cada funcionalidade listada abaixo estão disponíveis na Especificação API Pix Bacen disponível em: <https://bacen.github.io/pix-api/#/>.

- Gerenciamento de Cobrança
  - Criar Cobrança
  - Revisar cobrança

- Consultar Cobrança
- Consultar Lista de Cobranças
  
- Gerenciamento de Recorrências
  - Criar recorrência
  - Consultar recorrência
  - Revisar recorrência
  - Consultar lista de recorrências
  
- Gerenciamento de Solicitações de Recorrências
  - Criar Solicitação de confirmação de recorrência
  - Consulta solicitação de confirmação de recorrência
  - Revisar solicitação de confirmação de recorrência
  
- Gerenciamento de Cobranças associadas a uma recorrência
  - Criar cobrança recorrente
  - Consultar cobrança recorrente
  - Revisar cobrança recorrente
  - Solicitar retentativa de cobrança
  - Consultar lista de cobranças recorrentes
  
- Configuração de locations para payloads de recorrências
  - Criar location do payload
  - Consulta locations cadastradas
  - Recuperar location do payload
  - Desvincular uma recorrência de uma location

- Gerenciamento de Pix recebidos
  - Consultar Pix
  - Consultar Pix Recebidos
  - Solicitar devolução
  - Consultar devolução
  
- Gerenciamento de Notificações (Pix, Recorrências e Cobranças Recorrentes)
  - Configurar Webhook
  - Exibir informações acerca do Webhook Pix
  - Cancelar o Webhook Pix
  - Consultar Webhooks Pix (Disponível apenas para Webhook de Pix)

## 5. Jornada de adesão e implementação Sicredi

Por jornada de adesão, entende-se o processo por meio do qual um usuário receptor 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 receptor. 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 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 Desenvolver 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 > APIs > Catálogo de APIs > APIs de Recebimento > Certificados e Credenciais > 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

O técnico deve acessar o Portal do Desenvolvedor (<https://developer.sicredi.com.br>) com usuário e senha previamente criados, acessar **APIs > Catálogo de APIs > APIs de Recebimento > Certificados e Credenciais** 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*)

O 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 Tipo (CERTIFICADO\_VALIDADO), 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](mailto: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:

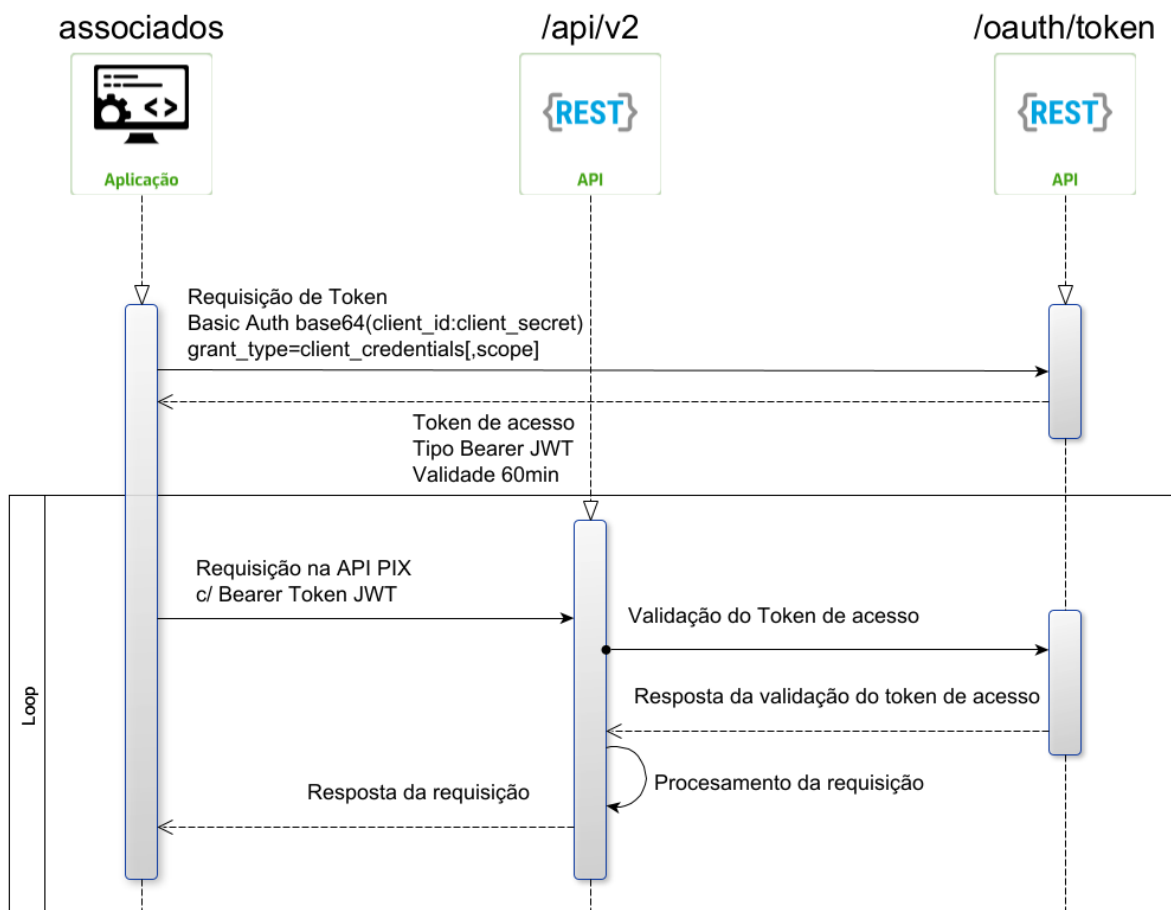
- Certificado digital *.CER* (disponibilizado através do Portal do Desenvolvedor);
- Chave *APLICACAO.KEY* gerada em conjunto com a requisição do certificado;
- Cadeia completa (disponibilizado através do Portal do Desenvolvedor).

### **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 Q0xJRu5UX01EX1BST0RVQ0FPOkNMSUVOVF9TRUNSRVRfUFJPRFVDQU8=' \
--data-urlencode 'grant_type=client_credentials' \
--data-urlencode 'scope=cob.write+cob.read+cob.write+cob.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



- **Especificação baseada em formato Swagger (Open API):**

<https://bacen.github.io/pix-api>

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, 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](https://www.bcb.gov.br/content/estabilidadefinanceira/spb_docs/ManualBRCode.pdf)

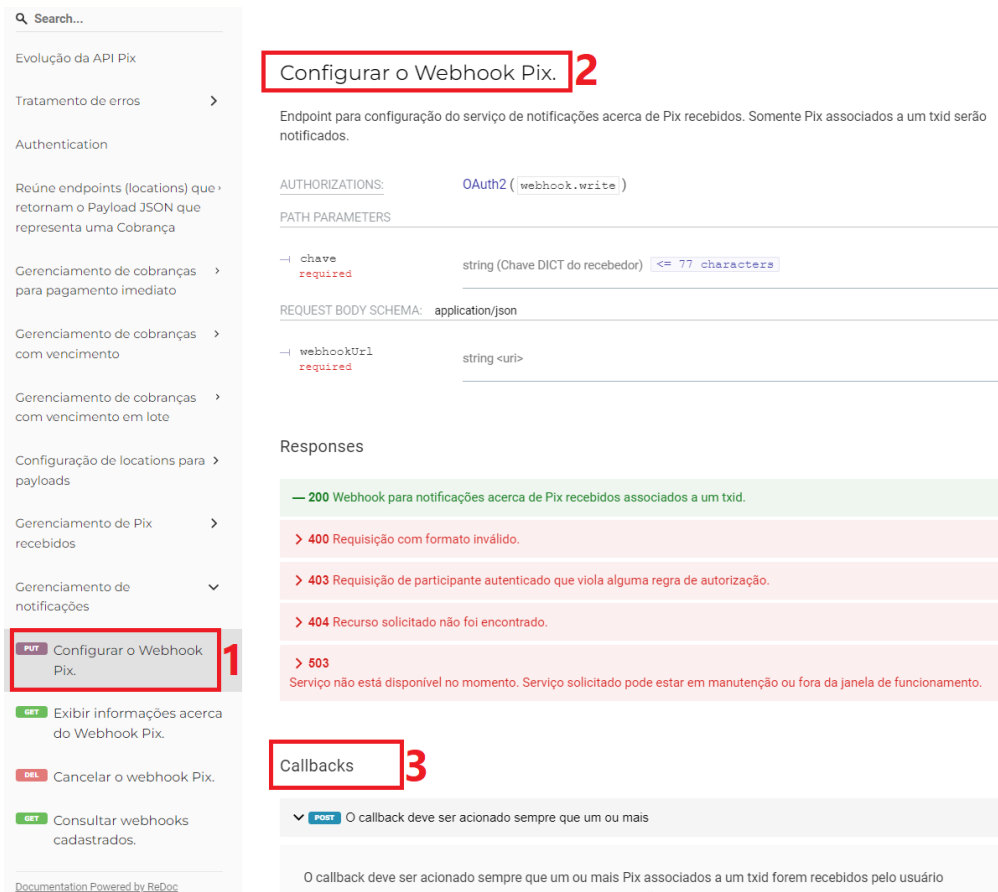
## 10. Webhook

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):



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>URL 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...](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.

- **Uso e reaproveitamento do Token de autenticação - (/oauth/token)**

**IMPORTANTE:** Por questões de segurança, o token obtido retorna um prazo de expiração, ele deve rigorosamente ser considerado no tratamento da automação para reaproveitamento durante o tempo em que estiver vigente. Isso evita o excesso de solicitações de autorização desnecessárias à API Pix, e possíveis bloqueios passíveis pelo PSP Sicredi em regra de segurança relacionada ao IP solicitante do token por suspeitas de ataque.

- **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](mailto:homologacoes_recebimentos@sicredi.com.br).

## 12. Suporte

O portal do Desenvolvedor Sicredi possui canal disponível para eventuais dúvidas do processo de homologação e pós integração da API Pix, dedicado às integrações que foram viabilizadas individualmente ou utilizando um provedor terceiro (não parceiro API Pix Sicredi). O acesso está disponível no Portal Dev Sicredi no seguinte caminho: **Página Inicial > Suporte > Abra um chamado > Abrir Chamado**, e selecionar API Pix como o produto que deseja suporte.

Integrações realizadas utilizando um provedor parceiro Sicredi (Lista de Provedores Parceiros disponível no site: <https://www.sicredi.com.br/site/pixpj/api-pix/>) o canal de suporte primário é o suporte indicado nos contatos do provedor parceiro, responsável por viabilizar a integração ao associado.

Assuntos urgentes, e alternativos, podem ser encaminhados ao endereço [integracoes\\_pix@sicredi.com.br](mailto:integracoes_pix@sicredi.com.br), no entanto reforçamos que o Portal do Desenvolvedor Sicredi é o canal prioritário para dúvidas e suporte às integrações, onde constam especialistas dedicados às resoluções.

### **Atenção:**

Integrações de **Cobrança**, onde há a necessidade de vínculo entre Boleto/código de barras e QR Code de Pix (Boleto Híbrido), o suporte a ser acionado deve ser o e-mail [produto\\_cobranca@sicredi.com.br](mailto:produto_cobranca@sicredi.com.br).

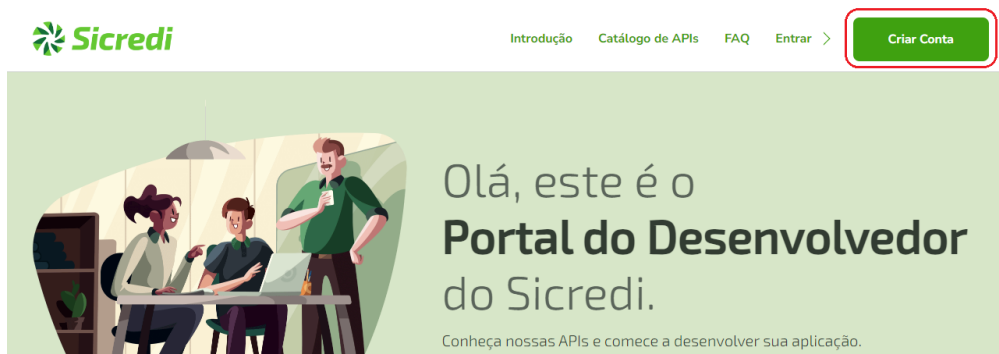
Nos casos de demanda sobre **Arrecadação Híbrida** (QRCode Dinâmico de Pix em boletos, carnês e demais documentos), o suporte a ser acionado deve ser o e-mail [homologacoes\\_recebimentos@sicredi.com.br](mailto:homologacoes_recebimentos@sicredi.com.br).

## 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).



Suporte > Abrir Chamado

## Abrir Chamado

Escolha o tipo de solicitação abaixo

Acesso à API PIX ▼

CNPJ do Associado

ID da Adesão

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*.

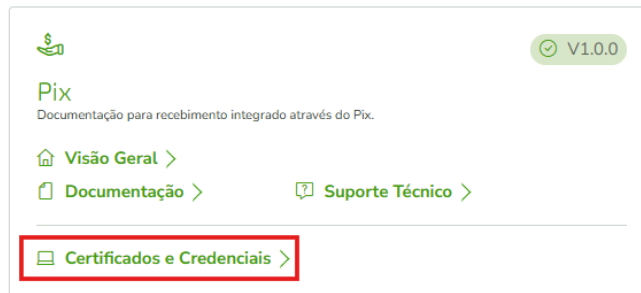
Introdução **APIs** ▼ Minha Conta ▼ Suporte ▼ Sair

Catálogo de APIs

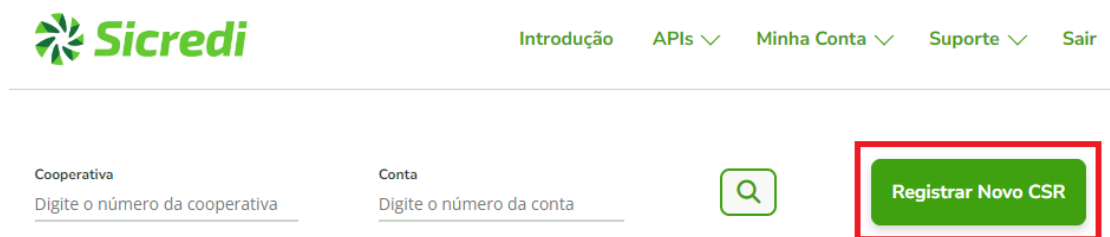
<https://developer.sicredi.com.br/api-portal/pt-br/content/catalogo-de-apis>

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

## APIs de Recebimento



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”.



[https://developer.sicredi.com.br/api-portal/csr\\_certs/generate](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 **i**. **Obs.:** É muito importante que neste preenchimento seja indicado o CPF/CNPJ da empresa integradora/responsável técnico da integração do associado, no campo destacado abaixo.

Por favor, preencha as configurações abaixo.

CPF/CNPJ DO ASSOCIADO

CPF/CNPJ DO PARCEIRO – EMPRESA/TÉCNICO RESPONSÁVEL PELA INTEGRAÇÃO

CNPJ real do parceiro/empresa integradora (somente números)

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-teste* criado com sucesso.

Para baixar o CSR, [clique aqui](#).

Para baixar a chave privada, [clique aqui](#).

Para baixar a chave privada sem senha, [clique aqui](#).

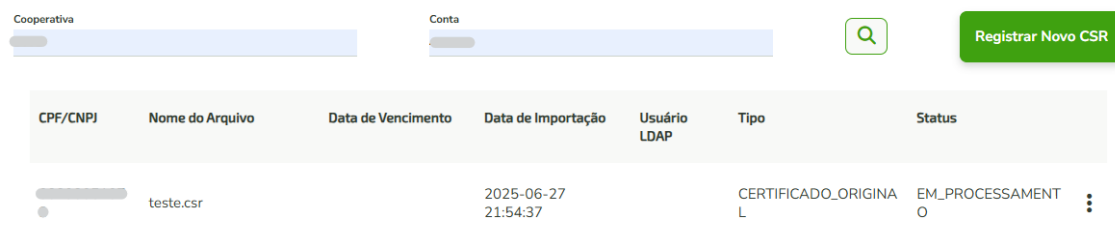
[Voltar para a lista](#)

\*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.



The screenshot shows a web interface for managing certificates. At the top, there are input fields for 'Cooperativa' and 'Conta', a search icon, and a green button labeled 'Registrar Novo CSR'. Below this is a table with the following columns: CPF/CNPJ, Nome do Arquivo, Data de Vencimento, Data de Importação, Usuário LDAP, Tipo, and Status. A single row is visible with the following data: a masked CPF/CNPJ, 'teste.csr', a blank 'Data de Vencimento' field, '2025-06-27 21:54:37' for 'Data de Importação', a blank 'Usuário LDAP' field, 'CERTIFICADO\_ORIGINAL' for 'Tipo', and 'EM\_PROCESSAMENTO' for 'Status'. A vertical ellipsis menu icon is present at the end of the row.

CPF/CNPJ	Nome do Arquivo	Data de Vencimento	Data de Importação	Usuário LDAP	Tipo	Status
[Masked]	teste.csr		2025-06-27 21:54:37		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:

Cooperativa  Conta

CPF/CNPJ	Nome do Arquivo	Data de Vencimento	Data de Importação	Usuário LDAP	Tipo	Status	
<input type="text"/>	CadeiaCompletaSicredi.cer		2023-10-19 14:37:30	*****	CERTIFICADO_CADEIA	OK	⋮
<input type="text"/>	certificado.cer	2025-10-19 02:35:11	2023-10-19 14:37:19	*****	CERTIFICADO_VALIDADO	OK	⋮
<input type="text"/>	APLICACAO.csr		2023-10-19 14:33:08	*****	CERTIFICADO_ORIGINAL	OK	⋮
<input type="text"/>	webhook-sicredi.cer		2023-07-17 14:10:47		CERTIFICADO_ORIGINAL	OK	⋮
<input type="text"/>	webhook-sicredi.cer		2023-07-17 14:10:47		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 desde este momento já é indicada a Validade do certificado, cujo deva ser renovado anterior a esta data, 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

CPF/CNPJ	Nome do Arquivo	Data de Vencimento	Data de Importação	Usuário LDAP	Tipo	Status	
<input type="text"/>	CadeiaCompletaSicredi.cer		2025-06-27 12:57:01	rpa*****	CERTIFICADO_CADEIA	OK	⋮
<input type="text"/>	<input type="text"/> .cer	2027-06-28 00:34:51	2025-06-27 12:56:51	rpa*****	CERTIFICADO_VALIDADO	OK	⋮
<input type="text"/>	<input type="text"/> .csr		2025-06-27 11:48:28	rpa*****	CERTIFICADO_ORIGINAL	OK	⋮

- Gerar nova Credencial
- Visualizar Certificado
- Download CER/PEM

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

Confirme se de fato deseja gerar a credencial de Produção para o CPF/CNPJ informado na mensagem.



## Anexo II – Postman e Collection

### Certificados Sicredi - Autenticação TLS mútua

O objetivo deste anexo é auxiliar o integrador técnico que tem posse de certificados Sicredi no processo de autenticação TLS mútua e deseja conhecer e/ou testar as funcionalidades para posteriormente migrar as informações para a automação do associado.

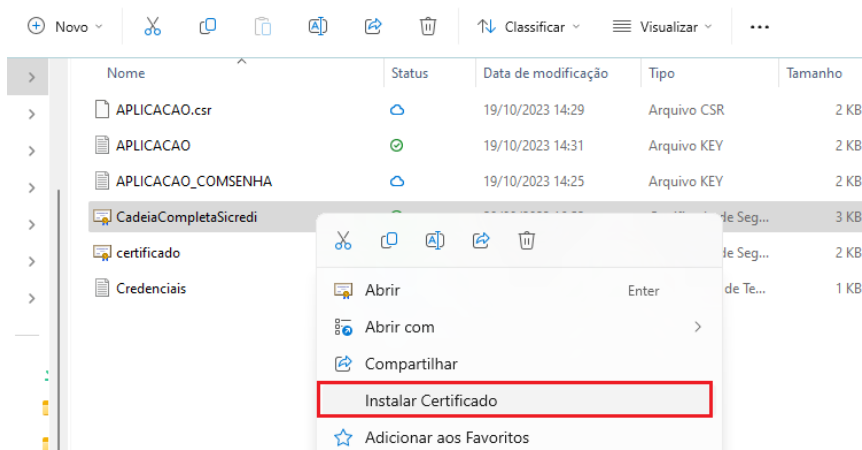
O Postman (até a confecção deste documento) aceita apenas certificados com estrutura (PEM), e aqui ilustramos como verificar a estrutura do arquivo que possui e como utilizar as credenciais SSL (certificado e chave) para a autenticação mútua no Postman utilizando a Collection construída pelo Sicredi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

**A Collection API Pix está disponível no [Portal do Desenvolvedor Sicredi](#) em:  
APIs > Catálogo de APIs > APIs de Recebimentos > Documentação**

### 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:

```
certificat.pem [2]
1 -----BEGIN CERTIFICATE-----
2 MIIHzTCCBrWgAwIBAgITdQAABYzXuWgXB+pWKgAAAAFjDANBgkqhkiG9w0BAQsF
3 ADCB4DESMBAGCgmSJomT8ixkARkWAmyMRMwEQYKZImiZPylGQBGRYDdmVOMRcw
4 FQYKZImiZPylGQBGRYHc2lJcmVkaTE4MDYGA1UEAxMvQXV0b3JpZGFkZSBkZDZl
5 aWZpY2Fkb3JhIFN1Ym9yZGlueWRhIFNpY3JlZGkgRzIxZCzAJBgNVBAYTAKJSMUcw
6 RQYDVQQKEz5Db25mZWRLcmFjYW8gSW50ZXJlc3RhZHVhbCBkYXMGQ29vcGVyYXRp
7 dmFzIEExpZ2FkYXMGYXV0b3JpZGFkZSBkZDZlJcmVkaTE4MDYGA1UEBRMDNTE4
8 NTQ0F0FoXDTIzMDgyNjE2NTQ0F0FowgFUCzAJBgNVBAYTAKJSMRowGAYDVQQIEiFS
9 aW8gR3JhbmRlIGRvIFN1bDEvR68Tl0laQWRhZCkYXMGQ29vcGVyYXRpdmFzIEExp
10 Ez5Db25mZWRLcmFjYW8gSW50ZXJlc3RhZHVhbCBkYXMGQ29vcGVyYXRpdmFzIEExp
```

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. (Conversão disponível no Anexo VI – Extra)

**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:

```
APLICACAO key [3]  APLICACAO_COMSENHA key [3]
1 -----BEGIN PRIVATE KEY-----
2 MIIEvAIBADANBgkqhkiG9w0BAQEFAASCByYwggSiAgEAAoIBAQC2GnJkCILUFY+D
3 eT/k1f1G2dTYJ9CzL1Gyyein3Vsj/1+GfGJW5upiBxJweRoLh1qWsaAGB3CW1B
4 dNJm9i1QwO+z4fC7e1/R68Tl0laQWRhZCkYXMGQ29vcGVyYXRpdmFzIEExpZ2Fk
5 ZR/f+d7s59BQdYdMT0UsDsa6DImU9grY3w6/u3zH9F39Ghr8BDw7XXYdZ2DGsC91

APLICACAO key [3]  APLICACAO_COMSENHA key [3]
1 -----BEGIN ENCRYPTED PRIVATE KEY-----
2 MIIFHDBOBgkqhkiG9w0BBQowQTApBgkqhkiG9w0BBQwwHAQI3jKotlobGTECAggA
3 MAwGCCqGSIb3DQIJBQAwFAyIKoZInvcNAwcEAE4ZE0NM11cBIIEyKjg+wDIT8Ho
4 kZt8qfLDwga/pD1TucaP2e32cgP+YFZnJpxQObocEXQ2a2aJ4tpPw6wcW6ln6i/2
5 SOYSONZTenFCWZ0exlnxTsnJE8FV+F2MZQwCkPbKFEHCTDhL00q/6Bf/DxU7saMw
```

## 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?

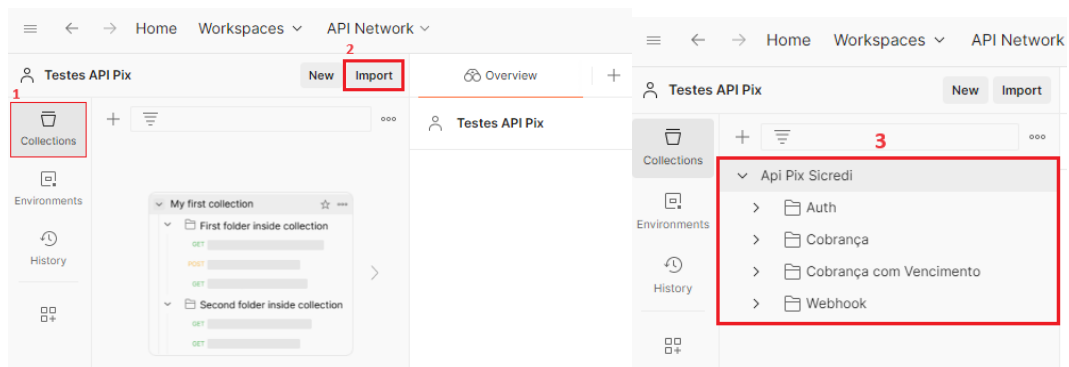
O Postman Collection é uma coleção de links de API, com seus respectivos métodos (POST, GET, PUT etc.) e demais configurações de envio como headers, body, entre outros.

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

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

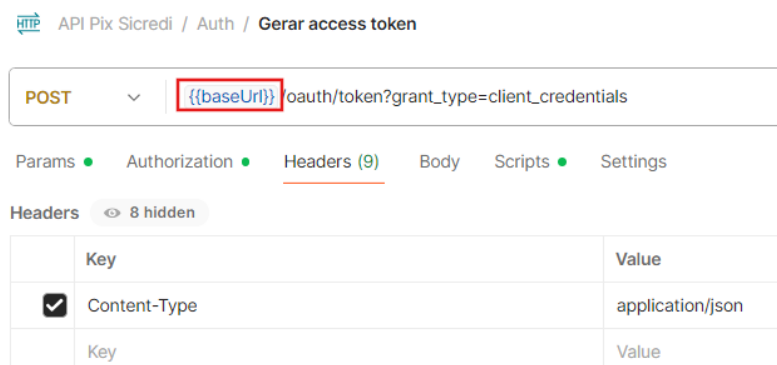
Dito isso, o Postman poderá ser baixado em (<https://www.postman.com/downloads>) sendo necessário também um cadastro de conta para iniciar as configurações e testes. E o arquivo de *Collection* API Pix Sicredi com extensão “.json” está disponível na documentação do Portal do Desenvolvedor em (Página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



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/v3/cob

Body

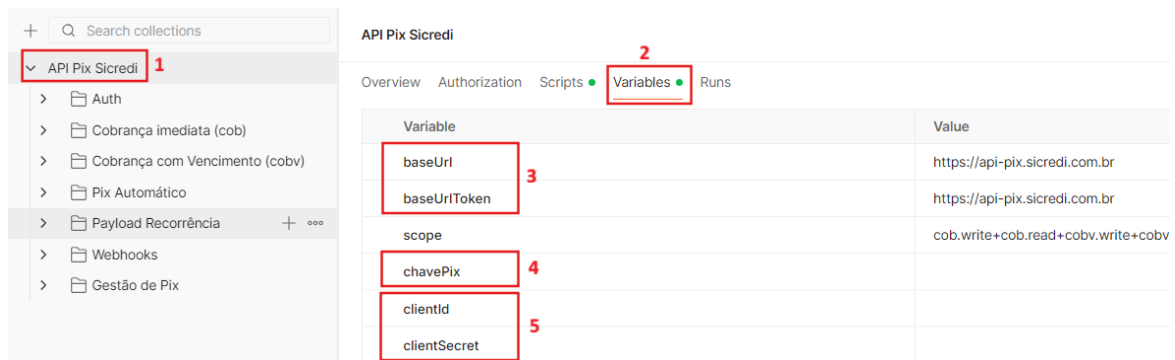
none form-data x-www-form-urlencoded raw binary GraphQL JSON

1 {
2   "calendario": {
3     "expiracao": 3600
4   },
5   "valor": {
6     "original": "3.00",
7     "modalidadeAlteracao": 0
8   },
9   "chave": "{{chavePix}}",
10  "solicitacaoPagador": "Serviço realizado.",
11  "infoAdicionais": [
12    {
13      "nome": "Campo 1",
14      "valor": "Informação Adicional1 do PSP-Recebedor"
15    },
16    {
17      "nome": "Campo 2",
18      "valor": "Informação Adicional2 do PSP-Recebedor"
19    }
20  ]
21 }

```

## 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 ou homologação), chave Pix (4) e credenciais (5) (Client ID e Client Secret), para prosseguir com requisições. Abaixo tela exemplificando um cadastro teste:

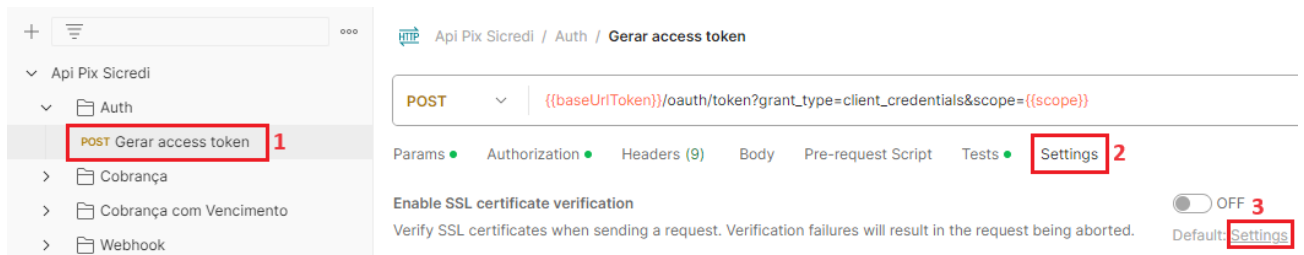


The screenshot shows the Postman interface. On the left, a collection named 'API Pix Sicredi' is selected. The main area shows the 'Variables' tab for this collection. A table lists the following variables:

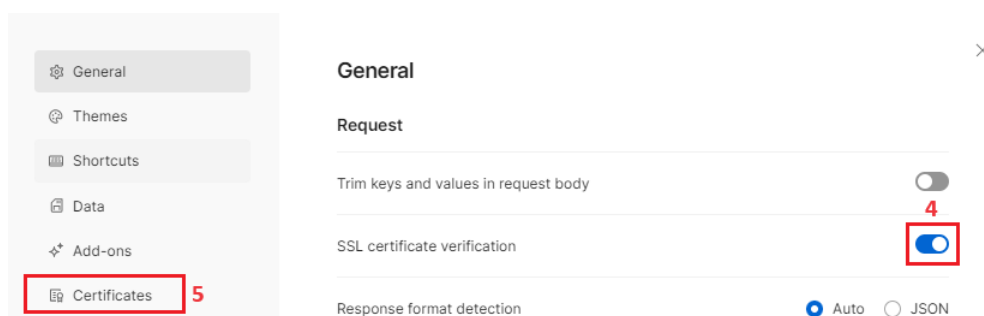
Variable	Value
baseUrl	https://api-pix.sicredi.com.br
baseUrlToken	https://api-pix.sicredi.com.br
scope	cob.write+cob.read+cobv.write+cobv
chavePix	
clientId	
clientSecret	

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

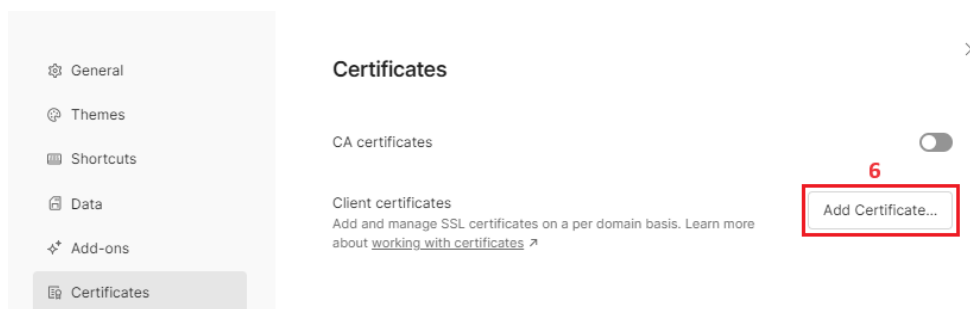
Agora, na primeira subpasta da Collection (Auth) em “Gerar access token” (1), clique em Settings (2) e em *Enable SSL certificate verification* clique em Settings (3).



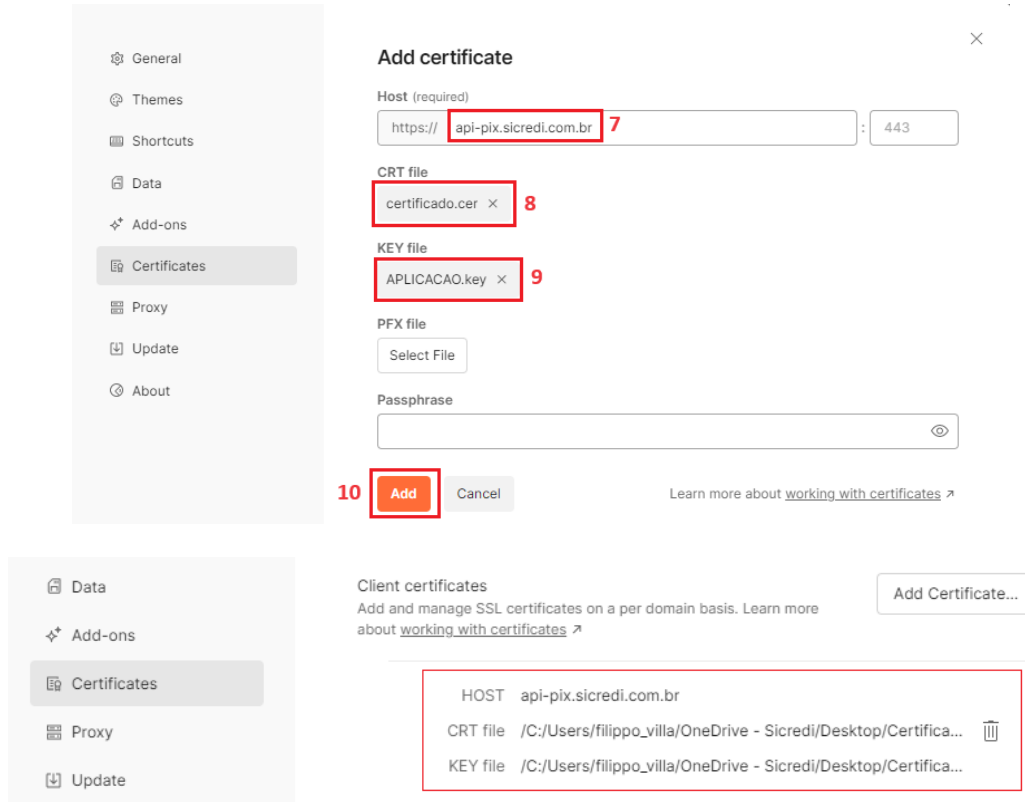
Na tela aberta, habilite o *SSL certificate verification* (4) e clique em Certificates (5) para acessar o ambiente a ser inserido os arquivos de certificado e chave privada.



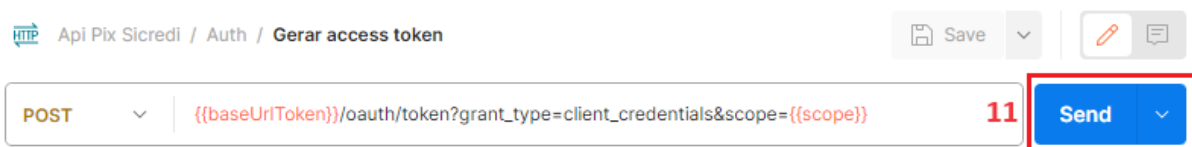
Adicione os arquivos (Certificado e Chave Privada.key) e defina a URL desejada para as requisições a serem realizadas.



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).



Pronto! Considerando essas configurações, a Collection está devidamente cadastrada levando em conta os dados 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):



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



## Anexo III – Pix Automático Recebedor

A solução do Pix Automático vem para ampliar o acesso à sistemática de cobranças recorrentes por empresas de todos os portes e reduzir os seus custos.

Considerando a ampliação do escopo da API Pix com a chegada do Pix Automático Recebedor, apresentamos o contexto das jornadas de iniciação do Pix Automático disponíveis na API Pix Sicredi e indicamos o [Guia de implementação do Pix Automático](#) como o documento oficial Bacen para sua aplicação.

O uso e gestão das funcionalidades do Pix Automático pelo usuário Recebedor (PJ) é exclusivo via API Pix, e a decisão de autorização e continuidade da adesão ao Pagamento Automático via Pix é compartilhado com o usuário/cliente Pagador possibilitando decisões unilaterais para continuidade dos negócios.

As funcionalidades para o usuário Recebedor via API Pix previstas pelo Bacen são:



A seguir, estão declaradas as 4 **jornadas de iniciação de solicitação do Pix Automático Recebedor** regulamentadas pelo Bacen. Verifique dentre elas qual faça mais sentido para o modelo de negócio a ser integrado, possibilitando o uso simultâneo de mais de uma jornada na automação para diferentes negociações. Abaixo de cada jornada, um direcionador para condução técnica.

Para além das indicações apresentadas em cada uma das jornadas, recomendamos verificar as Regras Gerais disponíveis no Guia de implementação do Pix Automático - Bacen, pág. 16 à 28, [aqui](#).

## **Jornada 1 - Autorização sem QR Code, com notificação via app para confirmação.**

Sugestão de uso: Jornada possível para clientes que estão aderindo ao Pix Automático diretamente no balcão de estabelecimentos físicos que não dispõe de um QR Code para solicitação de recorrência do Pix automático.

A solicitação do cliente é externa aos sistemas, ou seja, diretamente ao PJ através de canais disponíveis, no entanto a iniciação pelo PJ ocorre em sua automação e dispara notificação aos dados bancários e CPF informados pelo cliente, o qual recebe notificação no aplicativo da IF que utiliza para confirmação da adesão de recorrência ao pagamento automático criado pelo PJ.

Possível condução técnica:

#	Método	Endpoint	Descrição
1	POST	/v1/rec	Criar Recorrência
2	POST	/v1/SolicRec	Criação da Solicitação de recorrência e envio ao Pagador

## **Jornada 2 - Autorização com QR Code contendo apenas os dados da recorrência**

Sugestão de uso: Jornada possível para associados que desejam ofertar a recorrência via Pix Automático e farão futuramente o agendamento da primeira cobrança.

O PJ, através da API Pix, gera uma solicitação via QRCode/Pix Cópia&Cola de uso do Pix Automático e fornece ao cliente para leitura do QR Code contendo as informações da recorrência / permissão solicitada e concede a autorização.

Possível condução técnica:

#	Método	Endpoint	Descrição
1	POST	/v1/locrec	Criação da location payload de recorrência
2	POST	/v1/rec	Criação de recorrência vinculando location gerada.
3	GET	/v1/rec/{idRec}	Consulta de recorrência para obter o pixCópiaECola a ser apresentado/disponibilizado ao cliente. A atualização de status “Aprovada” da solicitação será notificada via webhook assim que recebida a autorização do Pagador.

### **Jornada 3 - Autorização com QR Code contendo dados para primeiro pagamento imediato e recorrência:**

Sugestão de uso: Jornada possível para negócios que exigem um pagamento imediato já na contratação do serviço, onde as demais cobranças serão automáticas ao cliente nos períodos acordados.

Jornada em que o usuário pagador lê um QR Code contendo as informações da recorrência / permissão solicitada e as informações relativas ao pagamento imediato da primeira cobrança e concede a autorização ao mesmo tempo em que inicia o pagamento imediato. Importante ressaltar que nesta jornada o pagamento imediato e a autorização para a recorrência via Pix Automático possuem relação e devem ambos ser bem-sucedidos, caso um deles não seja possível por motivo qualquer, a jornada é encerrada por completa.

Possível condução técnica:

#	Método	Endpoint	Descrição
1	POST	/v3/cob	Criação de cobrança imediata
2	POST	/v1/locrec	Criação da location do payload de recorrência
3	POST	/v1/rec	Criação da recorrência informando o txid da cobrança imediata e a location criada anteriormente
4	GET	/v1/rec/{idRec}	Consulta da recorrência para obter o pixCopiaECola

### **Jornada 4 - Autorização com QR Code contendo dados para pagamento/agendamento e para oferta da recorrência:**

Sugestão de uso: Jornada possível para clientes que já costumam/possuem uma recorrência de pagamentos de Pix para o estabelecimento, mas que por conveniência desejam alterar a modalidade de pagamento para o Pix Automático.

Jornada em que o usuário pagador aceita uma proposta após realizar ou agendar o pagamento de uma cobrança com vencimento ou estática, por meio de um QR Code contendo as informações do pagamento e da recorrência / permissão solicitada e concede a autorização. Importante ressaltar que nesta jornada, não há obrigatoriedade por parte do Pagador em aderir ao Pix Automático. Isso quer dizer que, por exemplo, o associado pode

receber a fatura com o QR Code de Cobrança com Vencimento, liquidar o seu QR Code, mas não desejar conhecer/aderir à recorrência de Pix Automático.

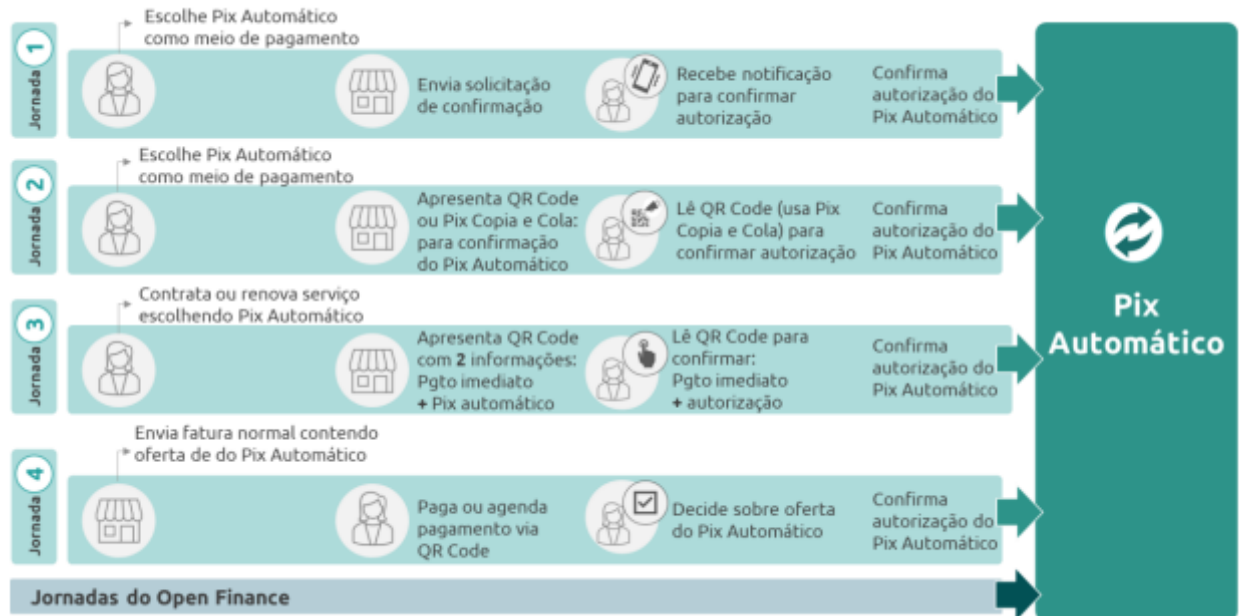
Possível condução técnica:

#	Método	Endpoint	Descrição
1	POST	/v1/locrec	Criação da location do payload de recorrência
2	POST	/v2/cobv	Criação da cobrança com vencimento
3	PUT	/v1/rec	Criação da recorrência informando o txid da cobrança com vencimento e a location criada anteriormente
4	GET	/v1/rec/{idRec}	Consulta da recorrência para obter o pixCopiaECola

**Recomendação Sicredi:** Indicamos, independentemente da jornada selecionada, na criação das cobranças recorrentes que o campo “agencia” pertencente ao array “Recebedor” seja informado na requisição, ainda que o Bacen indique ser um campo opcional. Isso facilita a identificação em casos de associados que possuem mais contas em agências diferentes no sistema Sicredi.

**Atenção:** As sugestões de uso de jornada presentes neste material, bem como a possível condução técnica para execução de cada uma delas são meros exemplos e podem ser adequados e/ou melhorados de acordo com a necessidade existente de cada modelo de negócio e/ou integrador técnico responsável pela implementação nas mais diversas automações.

## Resumo Bacen das jornadas:



Os materiais oficiais que regulam as jornadas, regras e endpoints com suas determinadas parametrizações estão disponíveis em:

- **Especificação Técnica API Pix – Bacen:** <https://github.com/bacen/pix-api>
- **Guia de Implementação do Pix Automático – Bacen:** [https://www.bcb.gov.br/content/estabilidadefinanceira/pix/automatico/guia\\_pix\\_automatico.pdf](https://www.bcb.gov.br/content/estabilidadefinanceira/pix/automatico/guia_pix_automatico.pdf)
- **Manual de Padrões para Iniciação do Pix – Bacen:** [https://www.bcb.gov.br/content/estabilidadefinanceira/pix/Regulamento\\_Pix/II\\_ManualdePadroesparaIniciacaoodoPix.pdf](https://www.bcb.gov.br/content/estabilidadefinanceira/pix/Regulamento_Pix/II_ManualdePadroesparaIniciacaoodoPix.pdf)

Quadro Bacen comparativo entre jornadas e suas atribuições:



**Quadro: Comparativo entre as jornadas de autorização do Pix Automático**

	Jornada 2	Jornada 3	Jornada 4 <sup>17</sup>
<b>Escopo</b>	Autorização do Pix Automático	Pagamento de uma cobrança imediata (pagamento obrigatório) + Autorização do Pix Automático (obrigatória)	Pagamento (ou agendamento do pagamento) de uma cobrança com vencimento (obrigatórios) + Autorização do Pix Automático (opcional)
<b>Início da jornada no ecossistema Pix</b>	Recebedor requisita criação da recorrência ao seu PSP e obtém um código para gerar um QR Code contendo: - location para dados da recorrência	Recebedor requisita criação de uma cobrança imediata e da recorrência ao seu PSP e obtém um código para gerar um QR Code contendo: - location para dados de uma cobrança imediata - location para dados da recorrência	Recebedor requisita criação de uma cobrança com vencimento e da recorrência ao seu PSP e obtém um código para gerar um QR Code contendo: - location para dados de uma cobrança com vencimento - location para dados da recorrência
<b>Experiência do usuário pagador</b>	Autoriza o Pix Automático no ambiente do PSP pagador, mediante leitura de um QR Code ou inserção de um código por meio do Pix Copia e Cola	Paga uma cobrança Pix imediata e autoriza, no mesmo ato, o Pix Automático para as cobranças subsequentes, mediante leitura de um QR Code ou inserção de um código por meio do Pix Copia e Cola	Paga ou agenda o pagamento de uma cobrança Pix com vencimento e recebe, na sequência, uma proposta para autorizar o Pix Automático para as cobranças subsequentes
<b>Tipo de QR Code</b>	Dinâmico contendo uma location referente aos dados da recorrência.	Dinâmico contendo uma location referente à cobrança imediata e outra referente aos dados da recorrência.	Dinâmico contendo uma location referente à cobrança com vencimento e outra referente aos dados da recorrência.

<sup>17</sup> Conforme detalhado na seção 3.5, o QR Code da jornada 4 pode conter os dados (estáticos) da cobrança

Reforçamos a atenção às Regras Gerais de cada etapa: Autorização, Agendamentos de Cobrança Recorrente e Liquidação. Nelas estão descritas as condições de negócio a serem observadas e rigorosamente cumpridas para o pleno funcionamento e sucesso da solução.

Abaixo, indicamos pontos importantes da etapa para o uso adequado da solução:

## **Autorização de Aceite do Pagador na jornada 1 (Oferta Pix Automático via Dados Bancários sem uso de QRCode)**

As recorrências enviadas pelo usuário recebedor por meio do seu PSP para que sejam confirmadas pelo usuário pagador poderão ficar pendentes de resposta por parte do usuário pagador pelo prazo máximo de 30 dias. Prazos inferiores poderão ser estabelecidos pelo usuário recebedor (em função do modelo de negócio, ou qualquer outra consideração a ser atendida). Passando esse prazo, a solicitação de confirmação da recorrência expirará, cabendo ao PSP pagador excluí-la.

## **Agendamentos de cobranças recorrentes**

As instruções de pagamento precisam ser enviadas, entre dois dias e dez dias corridos antes da data prevista para a liquidação;

Para Cancelamento de Agendamentos já realizados, por parte do PJ recebedor: deve informar ao seu PSP até às 22h da data anterior à prevista para liquidação, para que o PSP do usuário pagador seja comunicado do cancelamento de agendamento da liquidação.

## **Liquidação**

**A Liquidação dos agendamentos ocorre na janela de 0h à 08h da data agendada. Excepcionalmente, podem ocorrer fora dessa janela conforme as seguintes condições:**

- Insuficiência de recursos na conta transacional;
- Insuficiência do limite disponível para Pix Automático; ou
- Falha operacional.

Nessas situações, devem ser observados os seguintes procedimentos:

Caso o pagamento agendado não seja efetivado por insuficiência de recursos ou de limite disponível, ao término da janela, às 8h, o usuário pagador será notificado de que o pagamento não ocorreu por um desses motivos e será realizada nova tentativa de pagamento na mesma data, a partir das 18h (ou de horário definido pelo PSP desde que dentro da janela de 18h a 21h).

Após as 21h não serão mais ser realizadas tentativas de liquidação da transação pelos PSPs. Após a última tentativa realizada pelo PSP pagador, caso persista a impossibilidade de envio da ordem de pagamento, será enviada notificação ao usuário pagador informando-o de que não foi possível a efetivação daquele pagamento por meio do Pix Automático e que: ele deve efetuar o pagamento da cobrança por outros meios, caso a recorrência não permita novas tentativas de liquidação após o vencimento; ou poderão ser feitas novas tentativas ao longo dos próximos dias, caso a recorrência permita novas tentativas de liquidação após o vencimento.

Neste cenário em que a recorrência permita novas tentativas após a impossibilidade de envio da ordem de pagamento pelo PSP pagador às 21h da data agendada, cada nova tentativa corresponde a nova instrução de pagamento (mensagem pain.013). Seu envio pelo PSP recebedor é comandado pelo usuário recebedor por meio do endpoint POST `/v1/cobr/{txid}/retentativa/{data}` da API Pix.

Consulte todos os requisitos para que novas tentativas sejam sucedidas e também as Regras Gerais para o tema Liquidação disponíveis no Guia de implementação do Pix Automático - Bacen, pág. 42 à 44, [aqui](#).

## 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, no momento da geração das credenciais.

Modalidades de recebimento via API Pix e respectivos escopos:

- ✓ **Cobrança Imediata:** cob.write + cob.read;
- ✓ **Cobrança com Vencimento:** cobv.write + cobv.read + lotecobv.write + lotecobv.read.
- ✓ **Cobrança recorrente:** cobr.write + cobr.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 ]
}
```

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”:

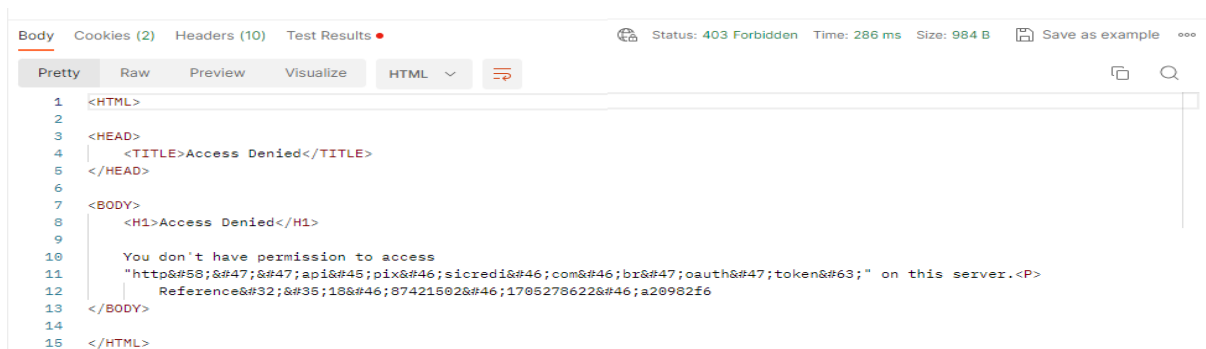
- **Descrição:** Não foi possível converter o token de acesso para o formato esperado.
- **Orientação:** Enviar o token no mesmo formato que foi recebido, pois pode ter ocorrido uma codificação ou conversão de dados antes do envio.

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

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

Exemplo de resposta status 403 (Acesso Negado):



```
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;&#47;api&#45;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 V – 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 OPENSSSL, 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 OPENSSSL, 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 VI – 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.

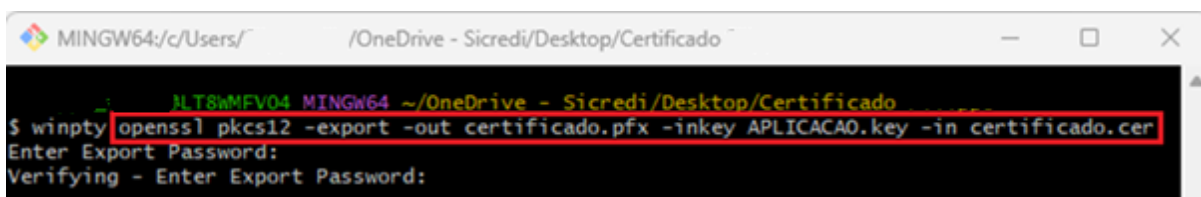
### Conversão dos arquivos Certificado (.CER) e Chave Privada (.KEY) para Certificado (.PFX)

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.*



```
MINGW64:/c/Users/.../OneDrive - Sicredi/Desktop/Certificado
$ winpty openssl pkcs12 -export -out certificado.pfx -inkey APLICACAO.key -in certificado.cer
Enter Export Password:
Verifying - Enter Export Password:
```

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$ 00000000ñú'no{ÖÄr_oÿFò(zø
0      *+H+±
00
0 00Ž1
0      00000000BR10000000000Rio Grande do Sul10000000 0
Porto Alegre10000000
0 SICREDI1:080000001Autoridade Certificadora Subordinada Sicredi 2040000
240218044232Z0
260217164302Z0r1
0      00000000BR10000000000Rio Grande do Sul10000000 0
Porto Alegre10000000
```

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-----
MIIEwTCCA6mgAwIBAgIUExVrX8cnK+3UYjMgu0FbNwtDLKUwDQYJKoZIhvcNAQEL
BQAwY4xCzAJBgNVBAYTAKJSMRowGAYDVQQIEwFSaW8gR3J3hbmR1IGRvIFN1bDZEV
MBMGA1UEBxMMUG9ydG8gQWx1Z3J1MRAwDgYDVQQKEwDTSUNSRURJMTowOAYDVQQD
EzFBdXRvcmlkYW91IEN1cnR1jYWRvcmlkYW91b3JkaW5hZG8gU21jcmVkaSAy
MDQwMB4XDTE0MDIwTE5MjIwMVoXDTI0MDIwOTA3MjIzMDUwczELMAkGA1UEBhMC
Q1IeGjAYBgNVBAgTEVJpbyBHcmFuZGUgZG8gU3VsMRUwEwYDVQQHEwxB3J0byBB
bGVncmlUxEDA0BgNVBAoTB1NjQ1JFREkxHzAdBgNVBAMTFmFwaS1waXgtNDcxOTA4
NjQwMDAxODcwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC0ca4Nmwy5
E3PQT0bpnYsr6qYhR0yWUVSYEDaSiSm7pkp45EvvwWZns+6XNMxuOzxbwa6KDZV3
n1A2A78fSuaPdXnTH/0f+aPp0Wk0kPi/48KiYF+0hTxv/4m41FTT/n+GF118WuPF
```

## 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:



Could not send request

Error: error:0b000074:X.509 certificate routines:OPENSSL\_internal:KEY\_VALUES\_MISMATCH

[View in Console](#)

[What's wrong?](#)

[Learn more about troubleshooting API requests](#)

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

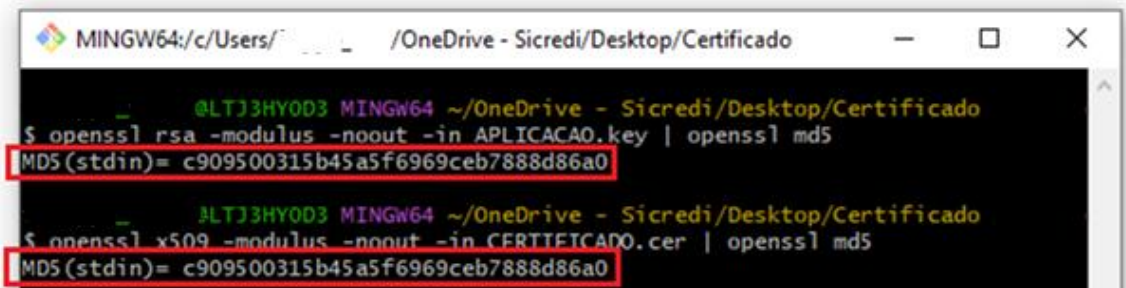
MD5 (stdin) da Chave Privada:

```
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:

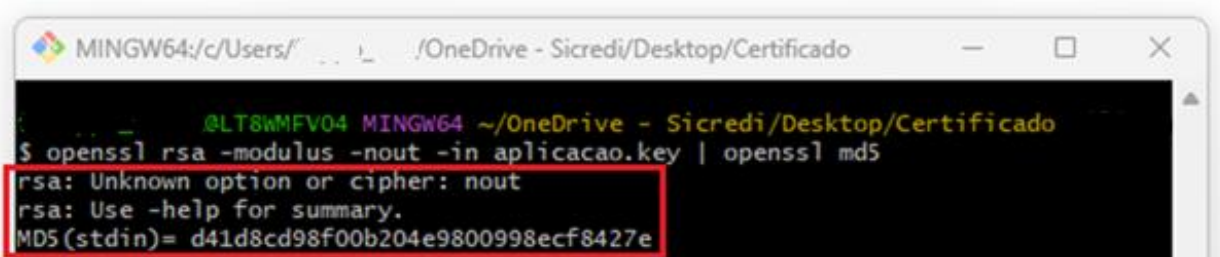


```
MINGW64:/c/Users/.../OneDrive - Sicredi/Desktop/Certificado
@LTJ3HY0D3 MINGW64 ~/OneDrive - Sicredi/Desktop/Certificado
$ openssl rsa -modulus -noout -in APLICACAO.key | openssl md5
MD5(stdin)= c909500315b45a5f6969ceb7888d86a0
@LTJ3HY0D3 MINGW64 ~/OneDrive - Sicredi/Desktop/Certificado
$ openssl 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.



```
MINGW64:/c/Users/.../OneDrive - Sicredi/Desktop/Certificado
@LT8WMFV04 MINGW64 ~/OneDrive - Sicredi/Desktop/Certificado
$ openssl rsa -modulus -nout -in aplicacao.key | openssl md5
rsa: Unknown option or cipher: nout
rsa: Use -help for summary.
MD5(stdin)= d41d8cd98f00b204e9800998ecf8427e
```