Manual para utilização da API Pix 2.2.1

Sicoob Pix

Histórico de Revisão

As alterações de versão serão comunicadas nessa seção:

Data	Versão	Descrição
03/2021	1.0	Elaboração do documento

Sumário

Guia para Utilização da API Pix

1 OBJETIVO

O objetivo deste guia é apresentar os conceitos de negócio, funcionalidades ofertadas e orientações técnicas para a utilização da API Pix do Sicoob de modo a orientar os interessados sobre como realizar a integração sistêmica.

Importante ressaltar que a API Pix – Interface de Programação de Aplicativos é normatizada pelo Bacen, sendo que as suas funcionalidades, as formas de iniciação do Pix, bem como requisitos de segurança contidos neste guia seguem de forma fidedigna as orientações e regras estabelecidas pelo Banco Central do Brasil e atende aos requisitos obrigatórios de segurança; Maiores detalhes podem ser obtidos por meio da documentação oficial:

- Manual de Padrões de Iniciação do Pix;
- Manual de Segurança do SFN; e
- Especificação técnica da API Pix

O documento contém o passo a passo para automatizar o uso da API Pix com foco no processo de autenticação e autorização de aplicações em todas as etapas do processo.

2 PÚBLICO ALVO

Este documento contém informações relevantes aos times de negócio, cooperativas, cooperados e empresas parceiras as quais fornecem soluções aos nossos associados.

3 CONCEITOS BÁSICOS

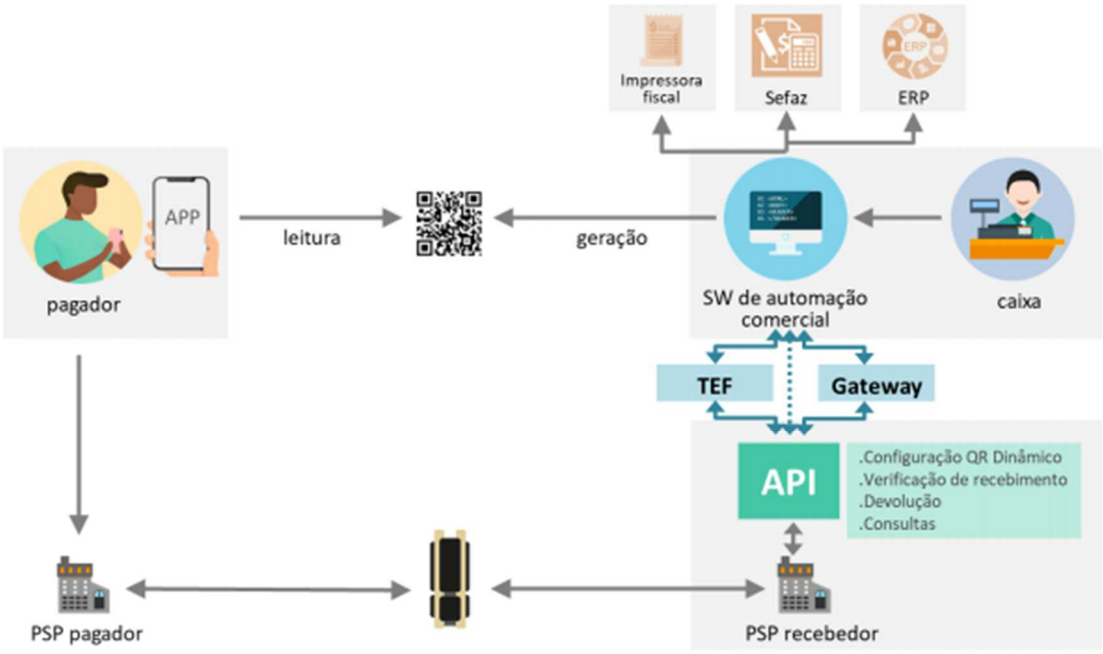
3.1 Pix Cobrança

O Pix Cobrança é uma maneira que o usuário recebedor do Pix tem para gerenciar e receber com mais facilidade as cobranças relacionadas a:

- Pagamentos imediatos, feitos no momento da cobrança por um QR Codes, em pontos de venda físicos e comércio eletrônico, por exemplo;

- Pagamentos com vencimento, realizados em data futura, que podem incluir outras informações como juros, multas, outros acréscimos, descontos e outros abatimentos, semelhante ao boleto (em breve).

3.2 API Pix



Fonte: https://www.bcb.gov.br/content/estabilidadefinanceira/pix/Regulamento_Pix/II-ManualdePadroesparaIniciacaodoPix.pdf

A API Pix é o componente do arranjo de Pagamentos Instantâneos instituído pelo Banco Central que visa possibilitar que o usuário recebedor, no contexto *Person Tio Business* (P2B) ou *Business to Business* (B2B), possa automatizar a interação com seu prestador de serviços de pagamento (PSP). Nesse contexto, a presente versão da API Pix busca automatizar a interação do usuário recebedor com seu prestador de serviços de pagamento (PSP), a fim de gerar cobranças e confirmar o recebimento do pagamento dessas cobranças por meio do Pix. Na figura

acima, pode-se visualizar possíveis caminhos de integração dos sistemas do usuário recebedor com a API Pix do PSP.

O usuário recebedor poderá, via API Pix:

- Gerar cobranças Pix (cópia e cola e QR Code) que poderão ser pagas pelos seus clientes em qualquer aplicativo das instituições financeiras participantes do arranjo;
- Alterar dados de uma cobrança Pix previamente cadastrada;
- Remover dados da cobrança, em caso de necessidade de cancelamento;
- Verificar a liquidação da cobrança por meio de Pix recebidos;
- Realizar a conciliação dos pagamentos realizados por meio do Pix de maneira automatizada;
- Suportar o processo de devolução de valores, que pode ser acionado em função, por exemplo, da devolução dos valores envolvidos em uma compra.

3.3 Chave Pix

A chave Pix é um apelido utilizado para identificar sua conta. Ela representa o endereço da sua conta transacional no Pix perante o Banco Central. Os quatro tipos de chaves Pix que você pode utilizar são:

- CPF/CNPJ;
- E-mail;
- Número de telefone celular; ou
- Chave aleatória.

A chave vincula uma dessas informações básicas às informações completas que identificam a conta transacional do cliente (identificação da instituição financeira ou de pagamento, número da agência, número da conta e tipo de conta). A chave aleatória é uma forma de você receber um Pix sem precisar informar quaisquer dados pessoais ao devedor. É formada por um conjunto de números e letras gerado aleatoriamente pelo BACEN.

Acesse qualquer um dos canais digitais do Sicoob e realize o cadastramento da sua chave Pix.

3.4 QR Code

Através desta nova solução de pagamento instantâneo criada pelo Banco Central, sua empresa poderá gerar QR Codes e compartilhar com seus clientes a imagem ou a URL através do “Pix Copia e Cola” para facilitar o pagamento. Existem dois tipos de QR Code:

- **QR Code Estático**: apresenta um rol de funcionalidades compacto, são apenas quatro opções de configuração. Primeiramente, o usuário do QR Code estático precisa configurá-lo com uma chave Pix válida perante o Banco Central em algum dos nossos

canais de atendimento, as outras três configurações são opcionais: identificador da transação, campo de texto livre e valor do pagamento.

- **QR Code Dinâmico**: este dispõe de um rol de funcionalidades abrangente, tais como conciliação via identificador da transação, configuração de valor e de campos livres estruturados. O QR Code dinâmico também deve ser configurado para apresentar uma chave Pix. O QR Code dinâmico, em sua estrutura interna, é configurado com uma URL que é acessada no momento de sua leitura. Essa funcionalidade abre diversas possibilidades de uso, dado que as informações trazidas pela URL podem variar em função de diversos parâmetros. A URL também cumpre o papel de reduzir a quantidade de dados codificados diretamente na imagem. O QR Code dinâmico contém somente as informações básicas do usuário recebedor. O restante das informações é obtido em um webservice do PSP do recebedor, com base nessa URL.

Ambos servem para receber um ou mais Pix e podem ser gerados pela instituição financeira ou de pagamento na qual se possui conta. Podem ser disponibilizados em papel ou em meio eletrônico. Ambos foram normatizados pelo Bacen através do BR Code. O QR Code estático permitirá receber pagamentos sem precisar cadastrar um valor fixo, o que permitirá ao devedor informar o valor no momento em que for realizado o pagamento, lembrando que este tipo não possui data de vencimento ou expiração e não faz parte da API Pix para emissão, apenas consulta. O QR Code dinâmico apresentará as informações específicas daquela transação, como data de vencimento ou expiração, valor e multa, sendo ideal para transações únicas.

4 FUNCIONALIDADES DA API PIX 2.2.1

As funcionalidades da API Pix da versão 2.2.1 estão definidas em grupos conforme abaixo:

Gerenciamento de Cobranças com pagamento imediato (Cob): permite emitir, alterar e consultar as cobranças/QR Code.

Endpoint	Descrição
PUT/cob/{txid}	Criar uma cobrança imediata
PATCH/cob/{txid}	Alterar dados da cobrança imediata
GET/cob/{txid}	Consultar uma cobrança imediata
POST/cob	Criar uma cobrança imediata sem passar txId
GET/cob	Consultar a lista de cobranças imediatas

Gerenciamento de Pix Recebidos (Pix): permite gerenciar e conciliar os recebimentos de Pix.

Endpoint	Descrição
GET/pix/{e2eid}	Consultar informações sobre um Pix emitido.
GET/pix	Consultar a relação de Pix e a respectiva situação de cada um.
PUT/pix/{e2eid} /devolucao/{id}	Solicitar a devolução de um Pix emitido.

GET/pix/{e2eid} /devolucao/{id}	Consultar informação sobre uma devolução.

Gerenciamento de Localizações (Loc): permite realizar a configuração e remoção de *locations* para uso dos *payloads*. É um recurso que permite ao PSP Recebedor reusar uma URL, retornando diferentes cobranças (paylods JSON) ao longo do tempo, mas apenas uma por vez. Tipicamente, é utilizado quando o usuário recebedor precisa apresentar um QR Code impresso, mas que seja dinâmico.

Endpoint	Descrição
POST/loc	Criar location do payload.
GET/loc	Consultar locations cadastradas.
GET/loc/{id}	Recuperar location do payload.
DELETE/loc/{id}/txid	Desvincular um txid de uma location.

Gerenciamento de Cobranças para pagamento com vencimento (CobV): permite o gerenciamento de cobranças com vencimento.

Endpoint	Descrição
PUT /cobv/{txid}	Criação e atualização de cobrança
GET /cobv/{txid}	Consulta de uma cobrança
GET /cobv/	Consulta de lista de cobranças
PATCH /cobv/{txid}	Alteração de uma cobrança

Gerenciamento de lote de Cobranças para pagamento com vencimento (LoteCobV): permite o gerenciamento de cobranças com vencimento em lote.

Endpoint	Descrição
PUT /lotecobv/{id}	Criação de lote de cobrança
GET /lotecobv/{id}	Consulta de um lote de cobrança
GET /lotecobv/	Consulta lista de lotes de cobranças
PATCH/lotecobv/{id}	Alterar cobranças específicas dentro de um lote de cobranças com vencimento.

Gerenciamento de Notificações (Webhook): permite configurar uma URL a ser chamada para que o Sicoob sinalize de forma ativa os recebimentos de cada Pix.

Endpoint	Descrição
PUT/webhook/{chave}	Configurar o Webhook Pix.
GET/webhook/{chave}	Exibir informações acerca do Webook Pix.
DELETE/webhook /{chave}	Cancelar o webhook Pix.
GET/webhook	Consultar webhooks cadastrados.

5 ESPECIFICAÇÕES TÉCNICAS

5.1 Protocolos e tecnologias

A API Pix utiliza os seguintes protocolos e tecnologias:

- Definição da API: A API Pix está detalhada no formato OpenAPI 3.0.
- Formato: O formato de dados utilizados é o JSON.
- Protocolo: a automação do recebedor interage com a API utilizando *webservices* baseados em REST sobre HTTPS.

5.2 Requisitos de segurança obrigatórios

O Banco Central definiu os requisitos obrigatórios de segurança a serem seguidos pelos PSPs na disponibilização da API Pix, abaixo os requisitos que impactam diretamente na integração entre cliente e Sicoob (PSP) são:

- A conexão à API deve ser criptografada utilizando o protocolo TLS versão 1.2 ou superior, permitindo apenas *cipher suites* que atendam ao requisito de *forward secrecy*.

- O PSP deve implementar o framework OAuth 2.0 (RFC 6749) com TLS mútuo (mTLS – RFC 8705) para autenticação na API, conforme especificações abaixo:

    - Os certificados digitais dos clientes da API devem ser emitidos por ACs externas e devem obedecer ao padrão internacional x.509. O Sicoob não aceita certificados auto-assinados pelo cliente para o ambiente de produção.

    - O *Authorization Server* do Sicoob implementa a técnica de vinculação do certificado do cliente aos *access tokens* emitidos ("*Client Certificate-Bound Access Tokens*"), conforme seção 3 da RFC 8705.

    - O *Resource Server* do Sicoob confirmará que o *thumbprint* do certificado associado ao *access token* apresentado pelo cliente é o mesmo do utilizado na autenticação TLS (*proof-of-possession*).

    - O fluxo OAuth a ser utilizado é o "*Client Credentials Flow*".

    - Os escopos OAuth serão definidos na especificação Open API 3.0 da API Pix e permitirão associar diferentes perfis de autorização ao software cliente.

- Para a funcionalidade de *webhooks*, as notificações oriundas do Sicoob ao usuário recebedor trafegarão utilizando um canal mTLS.

5.3 Processos adicionais de segurança do Sicoob

O Banco Central entende que os PSPs poderão adotar processos, tecnologias e soluções de segurança para a API que mais acharem apropriados, desde que sejam atendidos os requisitos obrigatórios de segurança, abaixo as recomendações do BACEN que poderão adotadas pelos Sicoob que impactam o cliente:

- Assegurar a segurança do desenvolvimento do software cliente da API, mesmo que desenvolvido por terceiros. Sugere-se que o PSP institua e mantenha processo de homologação dos softwares clientes, estabelecendo critérios mínimos de segurança para que eles sejam autorizados a interagir com a API. Nesse caso, a API deve negar tentativas de comunicação de clientes não homologados.

- Definir uma política de troca periódica do certificado, senha e outras credenciais utilizadas no acesso à API;

- Validar a segurança do ambiente computacional dos usuários nos aspectos de infraestrutura, implementação e configuração do software cliente da API;

- Exigir que as empresas e instituições que utilizem a API tenham uma Política de Segurança da Informação formalmente instituída.

6 JORNADA DE ADESÃO

Por jornada de adesão, entende-se como o processo pelo 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 das credenciais de acesso (Client_IDs e Client_Secrets) pelo PSP e de certificados pelo usuário recebedor.

É facultado ao Sicoob homologar os sistemas integrantes com a API Pix, caso opte, as credenciais de produção serão disponibilizadas após está etapa.

Os cooperados Pessoa Jurídica que desejarem credenciais para integrar seus sistemas com a API disponibilizada pelo Sicoob devem procurar as suas cooperativas que por sua vez devem abrir chamados através da ferramenta Top Desk conforme a orientação abaixo:

A credencial de deverá ser solicitada conforme o ambiente desejado à cooperativa singular por meio da abertura de um chamado no Top Desk em:

1) Quando se tratar do ambiente de homologação: *Página Inicial > Serviços CCS > Open Banking > API Pix > Ambiente de Homologação > Solicitação*
2) Quando se tratar do ambiente de Produção: *Página Inicial > Serviços CCS > Open Banking > API Pix > Ambiente de Produção > Solicitação*

No momento da abertura do chamado será necessário informar:

1) Dados do cooperado: central, cooperativa, conta, nome completo, razão social, CNPJ, e-mail, telefone móvel para envio de SMS, url de callback;

2) IP fixo do seu servidor;
3) Informações sobre seu Aplicativo/Website: finalidade e *endpoints* que serão utilizados;
4) Anexar o arquivo contendo a chave pública do certificado (vide anexo I);

Ao final deste processo a credencial será enviada para o e-mail do cooperado informado pela cooperativa no momento da abertura do chamado. Estes dados serão utilizados pelo cooperado para autenticar e utilizar as API.

6.1 Requisição para obter token de acesso

1.1.1. Homologação

URL Post: https://api-homol.sicoob.com.br/cooperado/pix/token

Exemplo de consumo:

Form Data
grant_type=client_credentials
client_id=xxxxxxxxxxxxxxxxxx
client_secret=xxxxxxxxxxxxxxxxxx
scope=< -- Lista de escopos desejados --

Exemplo

```
curl -v --key private-key.pem --cert certificate.crt --location --request POST
'https://api-homol.sicoob.com.br/cooperado/pix/token' --header 'Content-Type:
application/x-www-form-urlencoded' --data-urlencode 'grant_type=client_credentials' -
-data-urlencode 'client_id=xxxxxxxxxxxxxxxxxxxx' --data-urlencode
'client_secret=xxxxxxxxxxxxxxxxxx' --data-urlencode 'scope=cob.read'
```

1.1.2. Produção

URL: https://apis.sisbr.com.br/cooperado/pix/token

6.2 Chamada API Pix

1.1.3. Homologação

URL Resource: https://api-homol.sicoob.com.br/cooperado/pix/api/v2

Exemplo de consumo:

Header
Authorization: Bearer <Access Token>
client_id: xxxxxxxxxxxxxxxxxx

Exemplo

```
curl -v --key private-key.pem --cert certificate.crt --location --request GET 'https://api-homol.sicoob.com.br/cooperado/pix/api/v2/cob?inicio=2020-06-01T00%3A00%3A00.00-03%3A00&fim=2020-10-27T23%3A59%3A59.00-03%3A00' --header 'client_id: xxxxxxxxxxxxxxxxxxx' --header 'Authorization: Bearer < -- Access Token gerado no passo anterior -- >'
```

1.1.4. Produção

URL: https://apis.sisbr.com.br/cooperado/pix/api/v2/

7 REFERÊNCIAS

1. https://www.bcb.gov.br/content/estabilidadefinanceira/pix/Regulamento_Pix/II-ManualdePadroesparaIniciacaodoPix.pdf

2. https://www.bcb.gov.br/content/estabilidadefinanceira/cedsfn/Manual%20de%20Seguranca%20do%20PIX%20v3.2.pdf

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

Como visto anteriormente o processo de uso da API Pix exige certificado digital emitido por uma entidade certificadora ICP Brasil. No momento da emissão do certificado o emissor entrega um par de chaves que não podem ser compartilhados em nenhuma hipótese com ninguém.

Será necessária a extração da chave pública deste certificado para que possa ser enviado ao Sicoob. **Em hipótese alguma a sua chave privada deve ser compartilhada ou enviada ao Sicoob**.

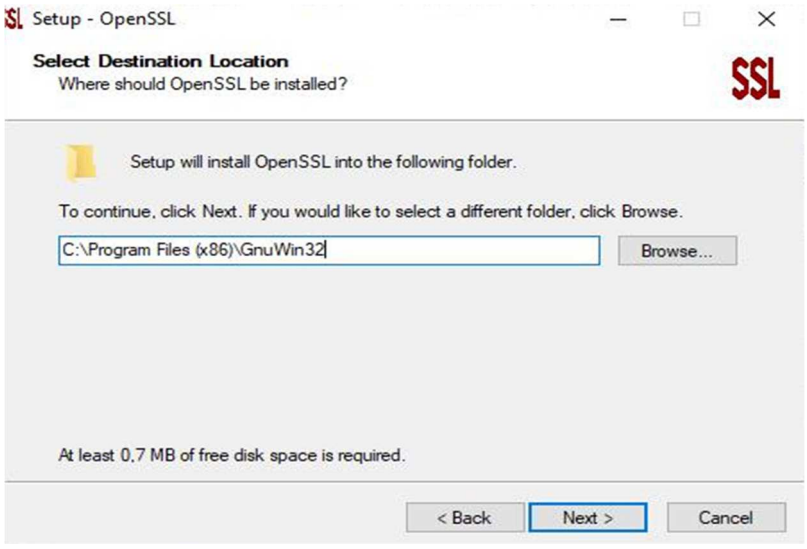
Este tutorial visa orientar e disponibiliza sugestões de endereços para realizar o download dos arquivos, não sendo obrigatório seguir este modelo ou se utilizar unicamente deste cenário para exportação do certificado digital (chave pública).

1. Realizar o download dos seguintes arquivos “openssl” através do endereço http://gnuwin32.sourceforge.net/packages/openssl.htm:

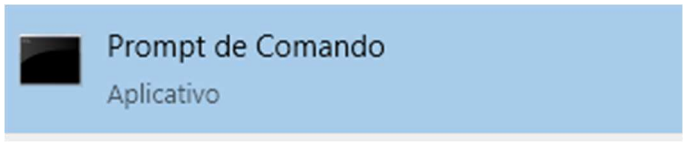
Download

Description	Download	Size	Last change	Md5sum
• Complete package, except sources	Setup	4658384	4 December 2008	9d9e1c90bb4976a554f604e9e69ac0a0
• Sources	Setup	5348830	4 December 2008	d53a2219527bace9be1702b16cc4b64a

2. Executar a instalação dos dois pacotes conforme item 1.



3. Abrir o Prompt de comando do Windows. Para isso basta digitar “cmd” na barra de pesquisa:

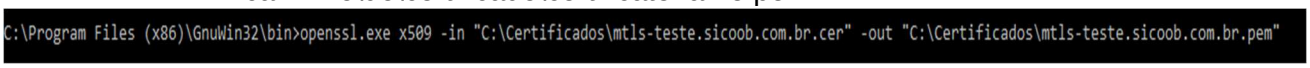


4. Dentro do CMD digitar as seguintes linhas de comando:

   i. C:\>cd "Program Files (x86)\GnuWin32\bin" --> aqui deverá ser informado o diretório de instalação dos arquivos mencionados no item 1.

   ii. openssl.exe x509 -in "caminho\do\certificado\certificatename.cer" -outform PEM -out "caminho\do\certificado\certificatename.pem".

   iii. Em alguns casos, o comando adicional é necessário, executar: openssl.exe x509 -in "caminho\do\certificado\certificatename.cer" -out " caminho\do\certificado\certificatename.pem "



5. O certificado foi exportado com êxito e pode ser recuperado no caminho escolhido no passo 4. O arquivo “.pem” deverá ser enviado conforme descrito no processo de “Jornada de Adesão”.