



Versão 1.1.3 – 02/07/2021

GUIA DE OPERAÇÃO

DO DIRETÓRIO

CENTRAL

Requisitos Mínimos e Recomendações



CONTEÚDO DO GUIA

01.

Introdução

02.

Registrando um usuário no Diretório

ETAPA 1: Registrando um usuário no Diretório

ETAPA 2: Verificando os dados informados

ETAPA 3: Confirmando o processo de registro

ETAPA 4: Confirmação da assinatura eletrônica

ETAPA 5: Análise e confirmação do Termo de Aceite

03.

Acessando uma Organisation

ETAPA 1: Exibindo detalhes de uma organização

Cadastramento de conglomerado

04.

Cadastrando contatos de notificação

ETAPA 1: Cadastrando um novo contato



CONTEÚDO DO GUIA

05.

Cadastrando reivindicações de domínio de autoridade

ETAPA 1: Cadastrando uma nova reivindicação de domínio

06.

Cadastrando reivindicações de autoridade

ETAPA 1: Cadastrando uma nova reivindicação de domínio

ETAPA 2: Cadastrando um usuário de domínio de autorização

07.

Cadastrando um Authorisation Server

ETAPA 1: Criando um novo servidor de autorização

08.

Cadastrando recursos de uma API

ETAPA 1: Cadastrando um novo recurso de uma API



CONTEÚDO DO GUIA

09.

Criando um Software Statements

ETAPA 1: Criando uma nova declaração de software

10.

Criando uma nova reivindicação de autoridade de software

ETAPA 1: Criando reivindicação de autoridade de software

11.

Criando certificados de transporte e assinatura em Sandbox

ETAPA 1: Criando um novo certificado de transporte

ETAPA 2: Criando um novo certificado de assinatura

12.

Carregando certificados emitidos por autoridade de certificação em Produção

ETAPA 1: Carregando certificado de transporte

ETAPA 2: Carregando certificado de assinatura



CONTEÚDO DO GUIA

13.

Cadastrando administradores da organização

ETAPA 1: Cadastrando um administrador da organização

14.

Obtendo um Software Statements Assertion

ETAPA 1: Exibindo detalhes de uma organização

15.

Configurando eventos de notificação no Diretório

ETAPA 1: Inscrever-se em um tópico

ETAPA 2: Solicitando uma subscrição

ETAPA 3: Confirmando uma subscrição

ETAPA 4: Analisando um evento de notificação

16.

Obtendo um token de acesso para as APIs do Diretório

ETAPA 1: Localizando o identificador do cliente

ETAPA 2: Localizando a URI de token no Diretório

ETAPA 3: Adicionando certificados SSL por domínio

ETAPA 4: Obtendo um token de acesso



CONTEÚDO DO GUIA

17.

Listando as organizações cadastradas no Diretório via API

ETAPA 1: Obtendo detalhes das organizações

18.

Listando os servidores de autorização de uma organização via API

ETAPA 1: Listando os servidores de autorização

19.

Obtendo um Software Statement via API

ETAPA 1: Obtendo um SSA do Diretório via API

20.

Obtendo um Software Statement Assertion via API

ETAPA 1: Obtendo um SSA do Diretório via API



CONTEÚDO DO GUIA

21.

Como obter suporte ao Diretório

22.

Anexos

Modelo de Segurança

Alterações da versão



01.

Introdução

O Open Banking ou Sistema Financeiro Aberto é uma iniciativa do Banco Central do Brasil que tem como principais objetivos trazer inovação ao sistema financeiro, promover a concorrência, e melhorar a oferta de produtos e serviços financeiros ao consumidor final. Este guia tem o objetivo de auxiliar os profissionais envolvidos no negócio e no desenvolvimento desse serviço, facilitando e esclarecendo dúvidas relacionadas ao Diretório e boas práticas envolvidas.

[Clique aqui para uma visão completa do Open Banking no Brasil.](#)



ANTES DE COMEÇAR!

Esse guia tem como objetivo demonstrar de forma prática a operação do Diretório Central do Open Banking Brasil. Além disso, ele é complementar a outras documentações disponibilizadas pela governança e não fazem parte do escopo do mesmo quaisquer detalhes relacionados a experiência do usuário e desenvolvedor, definições de segurança e especificação de APIs.

Todas as funcionalidades estão disponíveis em sandbox e podem ser testadas em:

<https://web.sandbox.directory.openbankingbrasil.org.br>

Procedimentos em produção pendentes serão disponibilizados assim que possível.

As ações aqui apresentadas podem ser realizadas tanto por administradores quanto por contatos técnicos primários e secundários.





ANTES DE COMEÇAR!

Para ilustrar este guia e tentar deixar as situações de uso mais palpáveis, foram criadas instituições e telas fictícias.

- **As instituições e marcas não são reais.**
- **As telas desenvolvidas, os softwares e sites são meramente ilustrativos**, para que seja possível ver um exemplo de como os requisitos e as recomendações podem ser aplicados em situações de uso real.
- **Nomenclaturas e imagens ilustrativas estão descritas na língua inglesa**, devido sua ampla abrangência e por conter terminologia técnica que em algumas situações não dispõe de tradução literal. O ajuste do idioma no Diretório fica a critério do usuário, podendo ser ajustado a qualquer momento.





TIPOS DE USUÁRIOS

Neste exemplo, mostramos as diversas possibilidades suportadas de atribuições de função para um usuário cadastrado no Diretório.



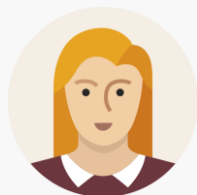
Público

O Diretório possibilita o cadastramento de usuários sem vínculos com nenhuma instituição. Esse tipo de usuário não tem nenhum acesso ou poder no Diretório. O cadastramento de um usuário relacionado a um participante, até que não seja feito o vínculo no Diretório, possui essas mesmas características.



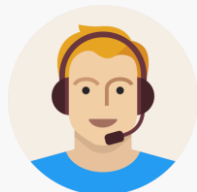
Administrativo

Usuários com poderes de administração no Diretório, podendo realizar todas ações.



Operação

Usuários com poderes específicos no Diretório.



Plataforma

Usuários para gestão e operação das plataformas do ecossistema, como o Service Desk, Portal, Plataforma de Resolução de Disputas e Plataforma Centralizada (Ressarcimento).

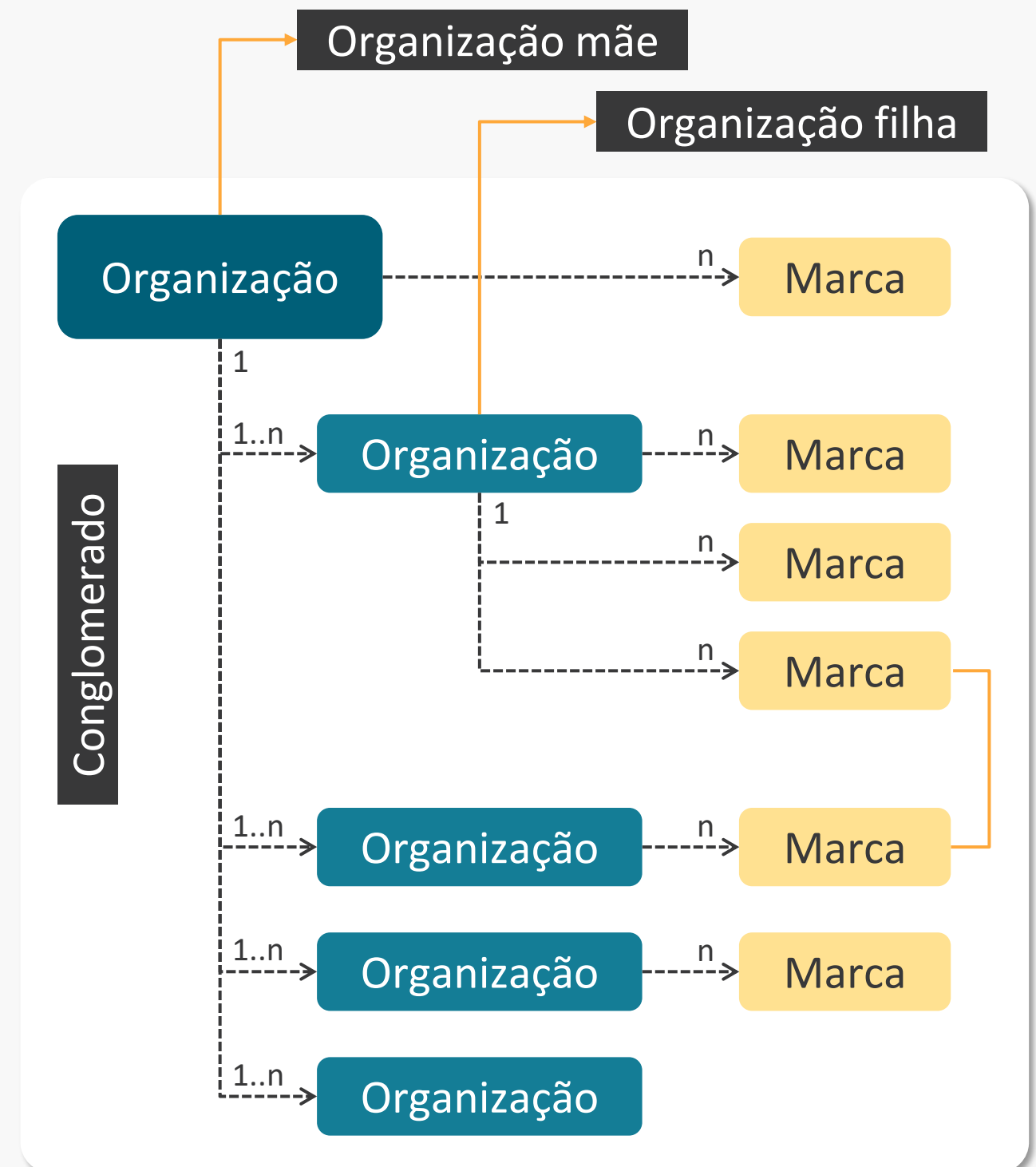


RELAÇÃO ORGANIZAÇÃO X MARCAS

Neste exemplo, mostramos as diversas possibilidades suportadas para se realizar cadastros de organizações no Diretório. Assim, **uma organização pode ser cadastrada de forma independente ou pertencente a um conglomerado**. Já as marcas são uma forma mais amigável, democrática e fácil para identificação das instituições participantes. **Uma Marca de um conglomerado pode estar correlacionada a mais de uma Instituição Participante**, assim como uma Instituição Participante pode estar correlacionada a mais de uma marca.

Importante: a Marca cadastrada no diretório será a mesma apresentada para escolha do usuário na Jornada de Compartilhamento de Dados e Iniciação de Pagamentos. As Instituições Participantes (ou organizações) também serão apresentadas em tela, apenas em caráter informativo. Para maiores detalhes, consulte o Guia de Experiência do Usuário.

Para obter mais detalhes sobre como cadastrar uma marca veja a seção [Cadastrando um Authorisation Server](#).





PONTOS DE ATENÇÃO NO CADASTRAMENTO DE MARCA/AUTHORISATION SERVER

- Uma marca é representada por um Authorisation Server e o mesmo sempre deve ser cadastrado associado a uma organização;
- O vínculo entre uma organização master (mãe) e uma organização que pertence ao conglomerado é realizado via o preenchimento do campo Parent Organization Reference ID no cadastro da organização filha, informando o CNPJ da organização mãe (caso seja necessário ajuste, favor entrar em contato com cadastro@openbankingbr.org);
- Quando a estrutura for de um conglomerado (uma organização master e uma ou mais organizações relacionadas) é recomendado o cadastro da marca na instituição mãe, caso as filhas venham a utilizar somente a mesma marca e arquitetura de autenticação. Importante ressaltar que caso não seja cadastrado uma marca exclusiva para a organização filha, a mesma irá herdar a(s) marca(s) da organização mãe;
- Caso uma marca pertença a uma organização filha o cadastro deve ser exclusivamente realizado na filha;
- Caso a mesma marca pertença a mais de uma organização, deve ser realizado um cadastro de Authorisation Servers para cada uma das organizações. É recomendado que as configurações dos Authorisation Servers sejam iguais, principalmente o campo Customer Friendly Server Name (marca);
- Quando for necessário cadastrar uma marca exclusiva para uma organização filha ela deixa de herdar a(s) marca(s) da organização mãe. Caso uma filha tenha que estar relacionada a uma marca exclusiva e também a da mãe, é necessário cadastrar a marca da mãe na filha.



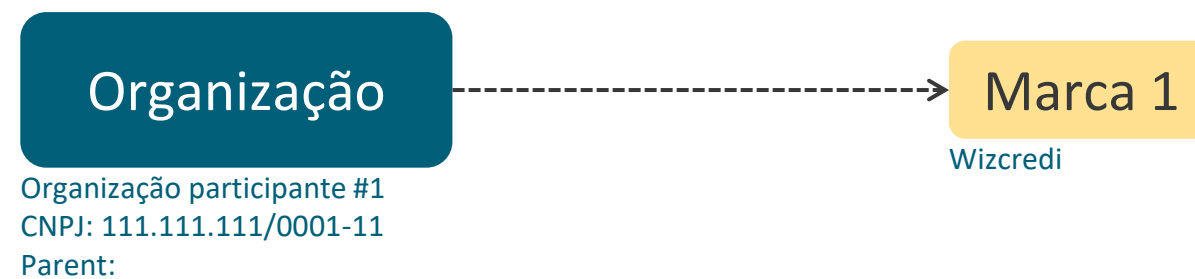
CADASTRAMENTO FASE 1 x FASE 2

- Se o cadastramento do Authorisation Server na Fase 1 já foi realizado com uma marca válida para a Fase 2:
É necessário cadastrar os recursos de Fase 2 no mesmo Authorisation Server, mantendo o Customer Friendly Server Name (marca) da Fase 1;
- Se o cadastramento do Authorisation Server na Fase 1 não foi realizado com uma marca válida para a Fase 2:
É necessário atualizar o Customer Friendly Server Name (marca) para a Fase 2 e cadastrar os recursos de Fase 2 no mesmo;
- **Os recursos da Fase 1 devem estar declarados em pelo menos um Authorisation Server do participante válido para a Fase 2;**
- Após esse processo, caso a instituição venha a ter Authorisation Servers / marcas oferecendo recursos exclusivos de fase 2, recomenda-se a criação de novos registros sem os recursos de Fase 1.



Exemplo de possíveis cenários

Organização e Marcas

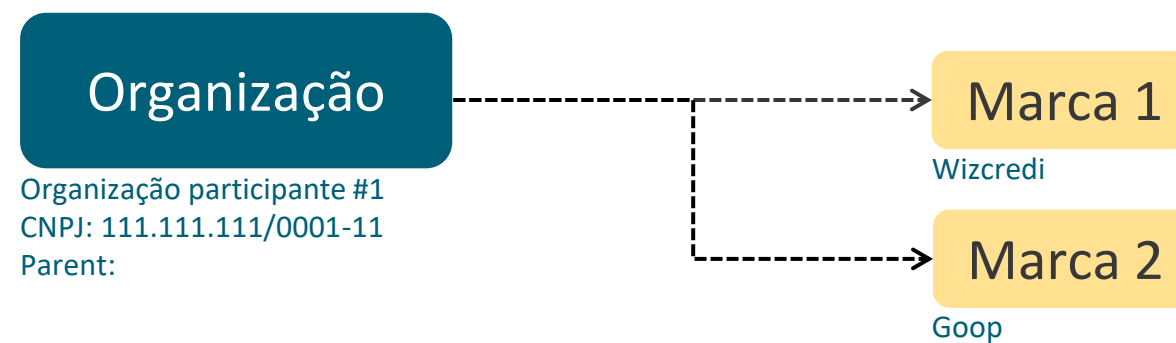


Neste exemplo, temos uma “organização” que não possui “organizações filhas” e possui apenas um AS/marca, a “marca 1”.



Exemplo de possíveis cenários

Organização e Marcas

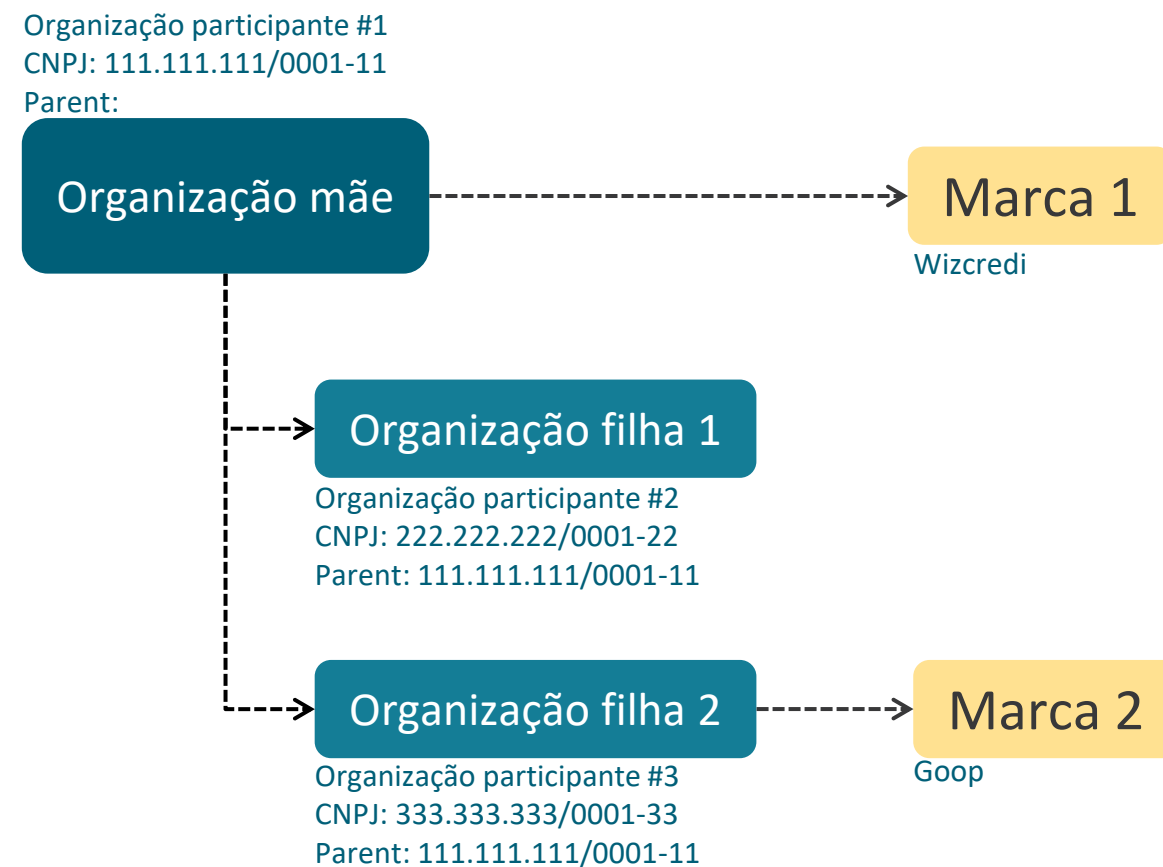


Neste exemplo, temos uma “organização” que não possui “organizações filhas”, mas que possui N AS/marca.
Neste exemplo, N = 2 marcas (“marca 1” e “marca 2”).



Exemplo de possíveis cenários

Conglomerado



O relacionamento entre as “organizações filhas” com a “organização mãe” é realizado via PARENT ORGANISATION REFERENCE ID, preenchendo o Parent das “organizações filhas” com o CNPJ da “organização mãe”.

Quando uma “organização mãe” tem uma ou mais de uma “organização filha”, temos um conglomerado

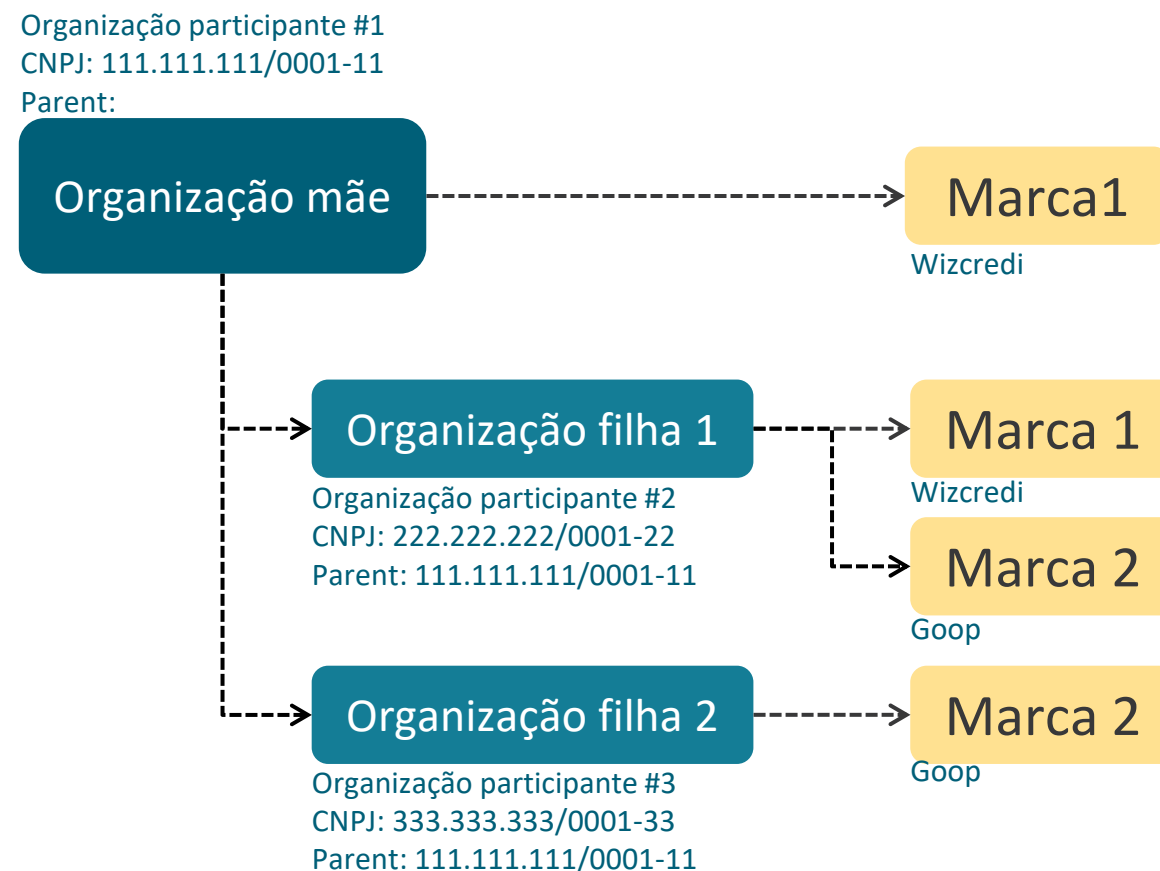
Neste exemplo, temos uma “organização mãe” que possui uma marca (“marca 1”) que é compartilhada com a “organização filha 1”.

Já a “organização filha 2” possui sua própria marca “marca 2”



Exemplo de possíveis cenários

Organização e Marcas



Neste exemplo, temos uma “organização mãe” que possui uma marca “marca 1”. A mesma “marca 1” está presente na “organização filha 1”, mas não na “organização filha 2”.

A “organização filha 1” deve apresentar a “marca 1” e a “marca 2”, como ela possui uma marca não receberia a da “organização mãe” por isso ambas as marcas devem ser declaradas.

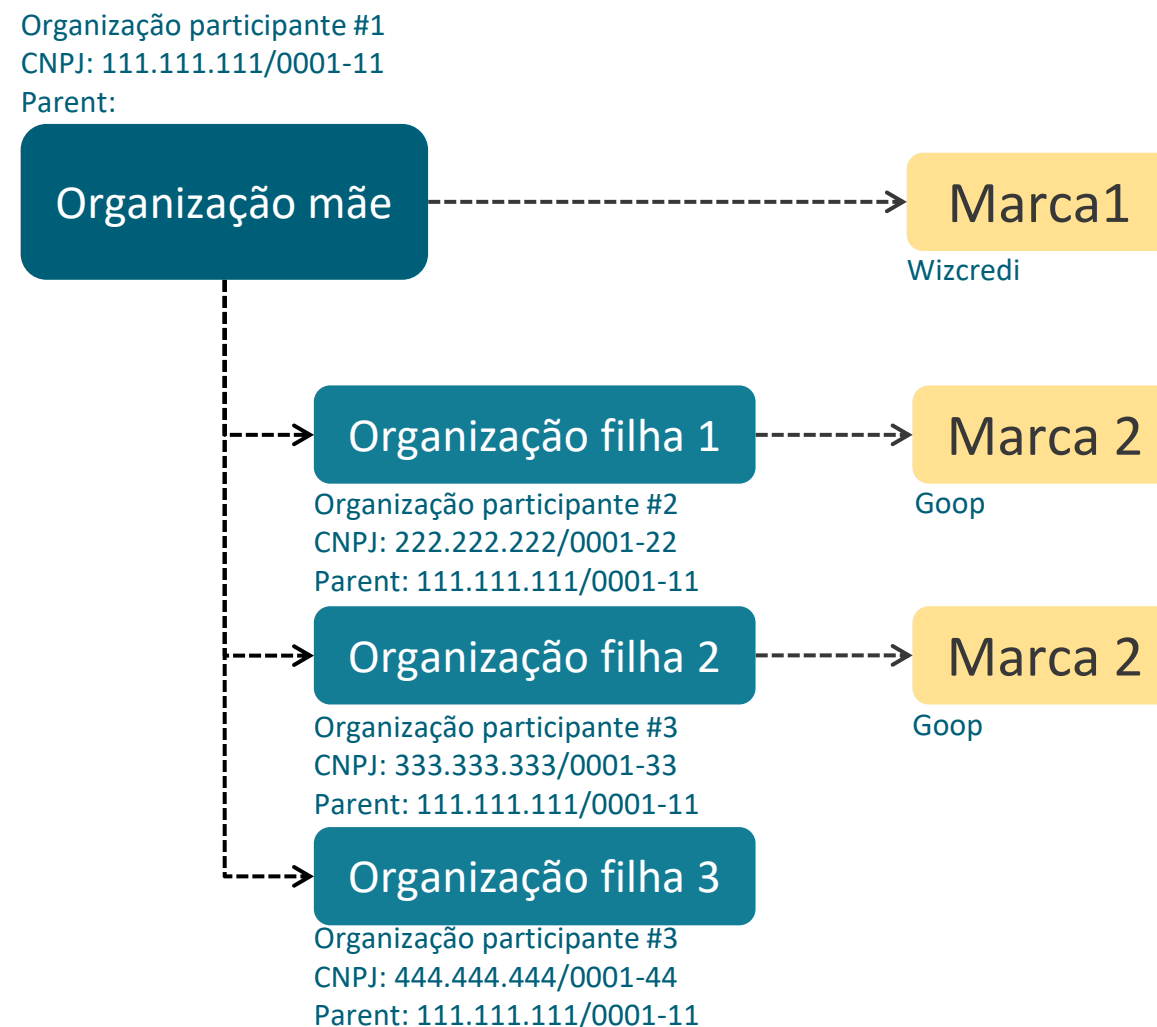
Atenção! Uma “organização filha” que tenha qualquer marca cadastrada, não assume a marca da mãe! A “organização filha” só assume a marca da mãe se não tiver nenhuma marca cadastrada nela!

Lembrando, o relacionamento entre as organizações é realizado via preenchimento do campo PARENT ORGANISATION REFERENCE ID na instituição filha referenciando a mãe.



Exemplo de possíveis cenários

Organização e Marcas



Neste exemplo, temos uma “organização mãe” que possui uma “marca 1” que é compartilhada com a “organização filha 3”. Logo, a “organização filha 3” assume a “marca 1”.

Já a “organização filha 1” e “organização filha 2” possuem sua próprio marca, que é a “marca 2” e devem ser relacionada a cada uma delas.

Se a “marca 2” fosse adicionada na “organização mãe” a “organização filha 3” iria receber também.

Lembrado, o relacionamento entre as organizações é realizado via preenchimento do campo PARENT ORGANISATION REFERENCE ID na instituição filha referenciando a mãe.



Exemplo de possíveis cenários

Organização e Marcas

Organização participante #1
CNPJ: 111.111.111/0001-11
Parent:

Organização mãe

Marca1

Wizcredi

Organização filha 1

Organização participante #2
CNPJ: 222.222.222/0001-22
Parent: 111.111.111/0001-11

Marca 2

Goop

Organização filha 2

Organização participante #3
CNPJ: 333.333.333/0001-33
Parent: 111.111.111/0001-11

Marca 2

Goop

Organização filha 3

Organização participante #4
CNPJ: 444.444.444/0001-44
Parent: 111.111.111/0001-11

Marca 3

Bratech Crédito

Organização filha 4

Organização participante #5
CNPJ: 555.555.555/0001-55
Parent: 111.111.111/0001-11

Marca 4

Wizcard

Vejamos um cenário mais complexo:

Neste exemplo, temos uma “organização mãe” que possui uma marca “marca 1” que é compartilhada com a “organização filha 4”. Já a “organização filha 1” e “organização filha 2” possuem sua própria marca igual “marca 2” mas que está relacionada a apenas a elas.

A “organização filha 3” possui duas marcas exclusivas dela “marca 3” e “marca 4”.

Lembrando, o relacionamento entre as organizações é realizado via preenchimento do campo PARENT ORGANISATION REFERENCE ID na instituição filha referenciando a mãe.



02.

Registrando um usuário no Diretório

Para acessar o Diretório de participantes você precisa estar registrado com um usuário válido. Esta seção descreve as etapas necessárias para realizar o registro de um novo usuário.



ETAPA 1: Registrando um usuário no Diretório

Requisitos

1. No navegador, digite a URL de acordo com o ambiente a ser acessado:

Sandbox

<https://web.sandbox.directory.openbankingbrasil.org.br/>

Produção

<https://web.directory.openbankingbrasil.org.br/>

2. Clique no link *Register*
3. Na tela *Register for an account*, preencha os campos do formulário. O slide a seguir apresenta cada um dos campos em mais detalhes.
4. Clique no botão *Register*.

NOTA: E-mails sociais não são permitidos, e você deve utilizar um endereço de e-mail válido da instituição. O cadastro pode ser realizado por qualquer colaborador da organização, identificado aqui como um Iniciador de Cadastro, podendo ser tanto um contato administrativo quanto técnico da instituição.

The screenshot shows a login form titled "Sign in to Connect." with a teal header. It contains two input fields: "USERNAME OR EMAIL" and "PASSWORD". Below the password field is a link "FORGOT PASSWORD?". A teal "Sign in" button is centered below the fields, with a "Cancel" link underneath it. At the bottom, there is a link "Don't have an account? Register". At the very bottom of the form, there is a small disclaimer: "By proceeding you agree to our use of cookies. Please read our Privacy Policy for more information. Full terms and conditions are available here Monitor the service here".

The screenshot shows a registration form titled "Register for an account." with a teal header. It contains several input fields: "FIRST NAME" and "FAMILY NAME" (split), "EMAIL ADDRESS", a phone number field with a dropdown set to "+55" and a label "PHONE NUMBER", "PASSWORD", "CONFIRM PASSWORD", and "NATIONAL ID (CPF)". Below these fields is a toggle switch labeled "Do you possess an e-signature certificate?". A teal "Register" button is centered at the bottom, with a link "Already have an account? Sign in." underneath it.



Detalhamento dos campos

Nome do campo	Descrição	Exemplo
First Name	Deve ser preenchido com o primeiro nome do usuário	João
Family Name	Deve ser preenchido com o sobrenome do usuário	Silva
E-mail Address	Deve ser informado um endereço de e-mail corporativo	joao.silva@wizcredi.com.br
Phone Number	Informar o número de telefone de contato do usuário.	+55 51 900000000
Password	Definir uma senha que deve conter entre 8 e 24 caracteres com letras maiúsculas, minúsculas, números e ao menos um carácter especial	<senha_secreta>
Confirm Password	Repetir a mesma senha informada no campo anterior.	<senha_secreta>
National ID (CPF)	Informar o número de registro do Cadastro de Pessoa Física (CPF)	999999999-00
Do you possess na e-signature certificate?	O seletor deve estar assinalado caso o usuário possua um e-CPF.	



ETAPA 2: Verificando os dados informados

Requisitos

1. Nesta etapa, o Diretório irá enviar uma senha de uso único (OTP), que será encaminhada ao endereço de e-mail e número de telefone informado na etapa anterior.
2. No e-mail recebido, selecione, copie e cole o código OTP no campo *EMAIL VERIFICATION CODE*.
3. Na mensagem SMS recebida no telefone celular, copie o código OTP e informe no campo *PHONE NUMBER VERIFICATION CODE*.
4. Clique no botão *Verify*.

NOTA: Caso você não tenha recebido o e-mail com o código de confirmação, verifique sua caixa de *SPAM* e as políticas de bloqueio de mensagens. O envio das mensagens poderá sofrer algum atraso, contudo, se o problema persistir, clique no botão *Resend OTP* para reenvio das mensagens.

Verify your account.

We've sent you some one-time passwords to verify your account details.

Enter the OTP sent to pedro.silva@wizcredi.com.br

EMAIL VERIFICATION CODE

Enter the OTP sent to +5500000000000

PHONE NUMBER VERIFICATION CODE

Verify

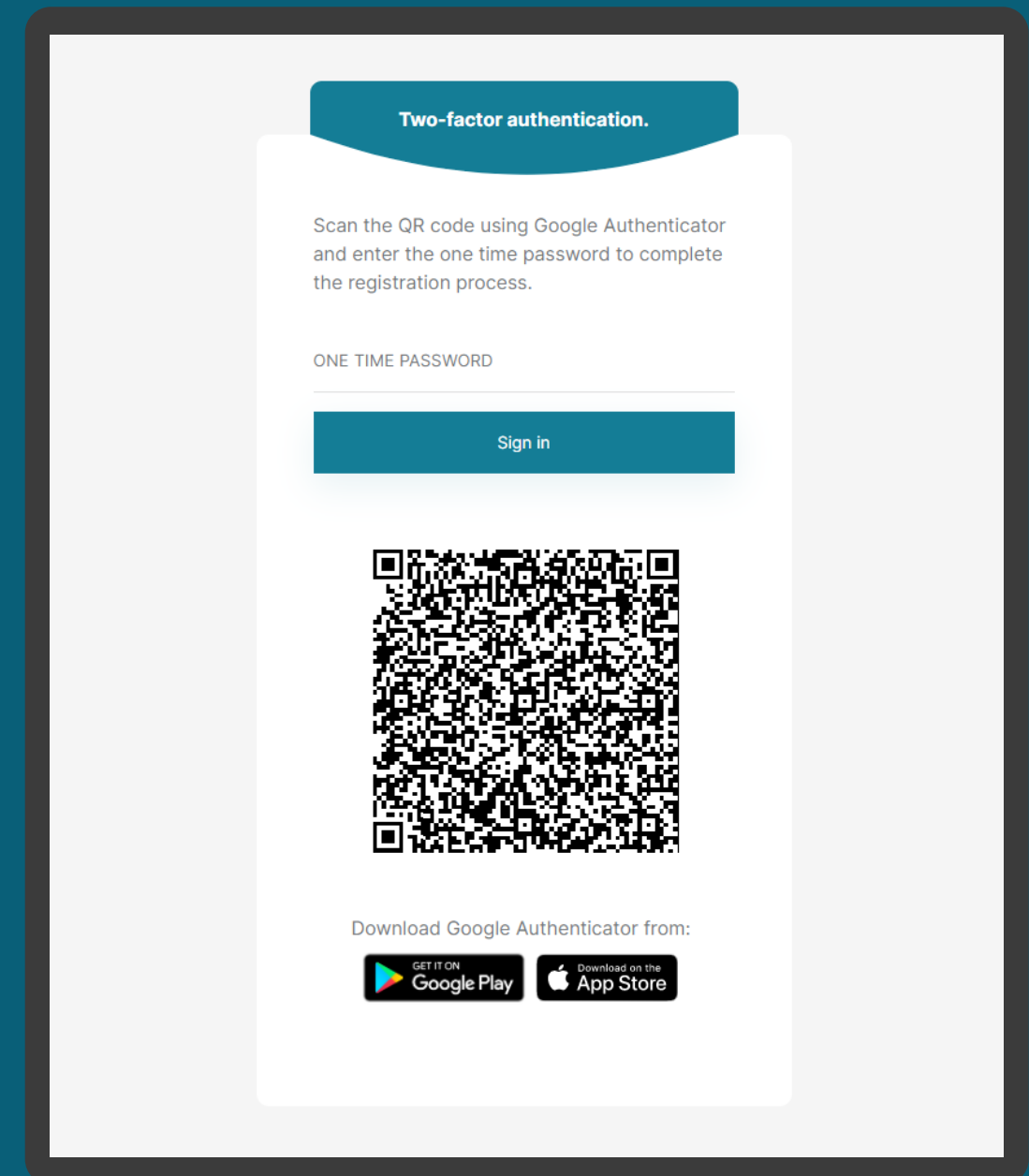
Resend OTP



ETAPA 3: Confirmando o processo de registro

Requisitos

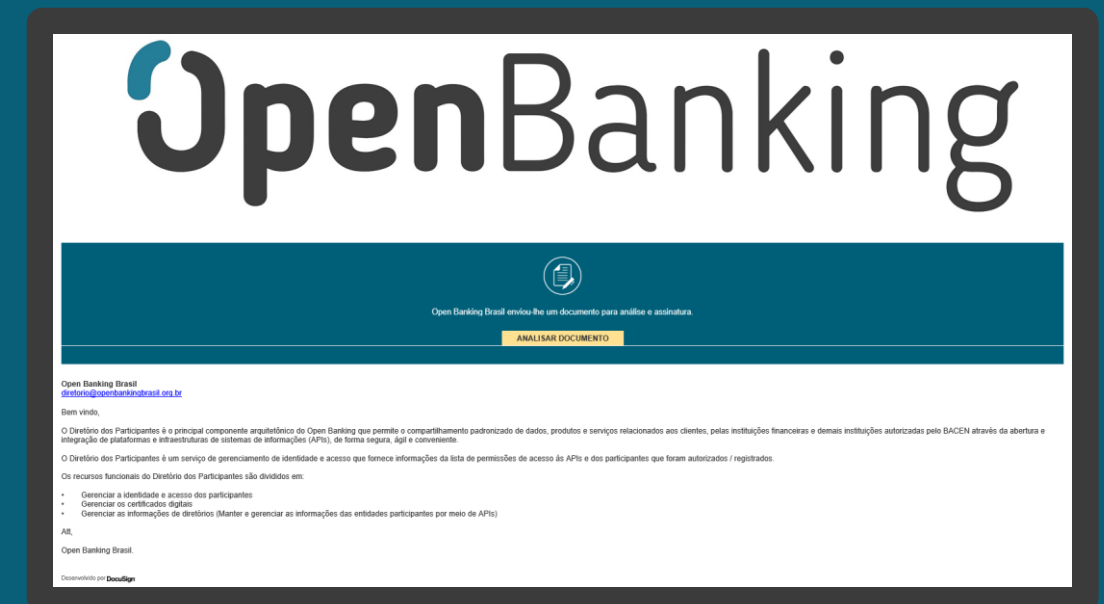
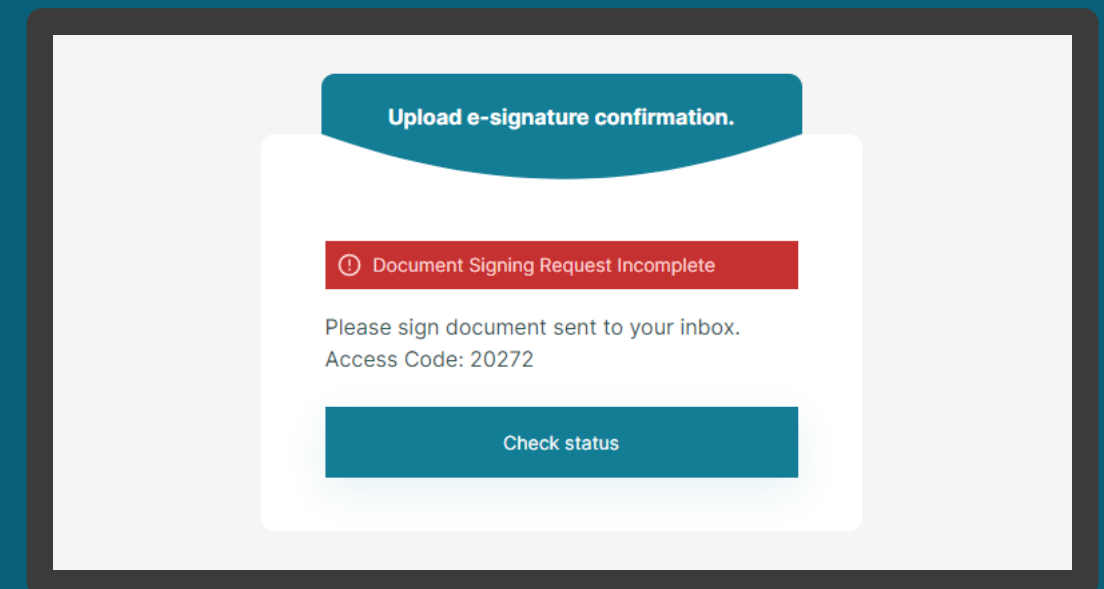
1. Nesta etapa, faça o *download* de um aplicativo de autenticação de sua preferência. É possível utilizar o *Google Authenticator*, *Microsoft Authenticator*, *LastPass Authenticator*, *1Password* entre outros.
2. Digitalize o QR Code que aparece na página e no aplicativo de autenticação, copie e cole a senha de uso único (OTP).
3. Clique no botão *Sign-In*



ETAPA 4: Confirmação da assinatura eletrônica

Requisitos

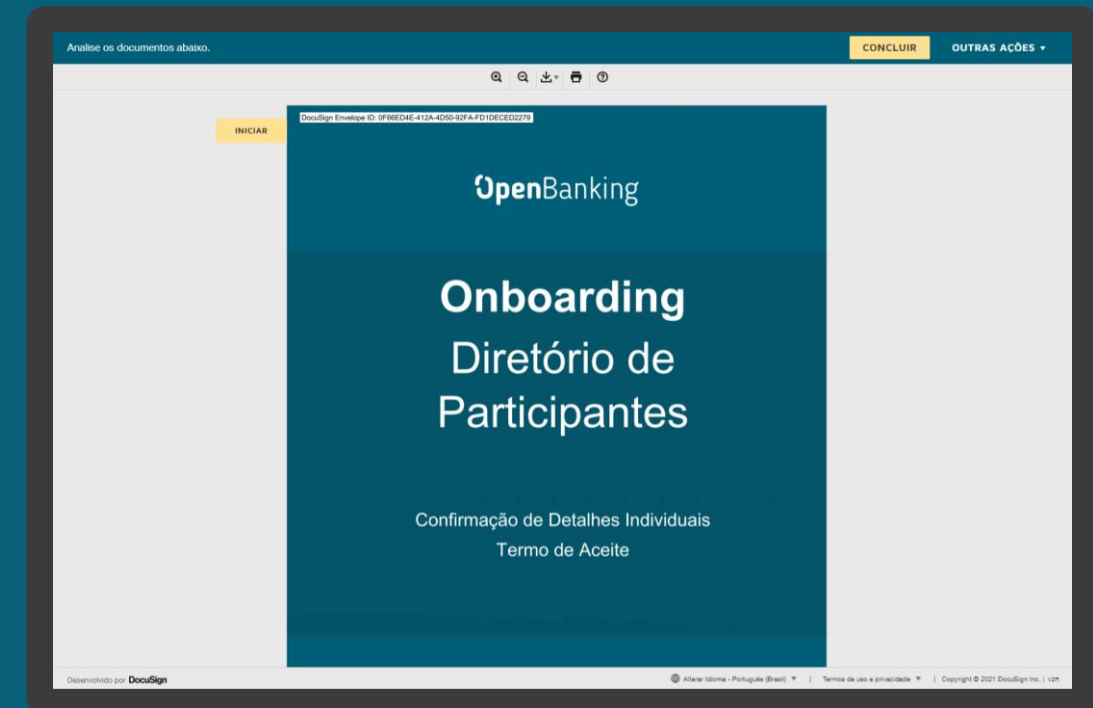
1. Nesta etapa, será enviado um e-mail contendo um *link* para análise e assinatura do Termo de Aceite.
2. Selecione e copie o código de acesso apresentado na janela *Upload e-signature confirmation*.
3. Na mensagem recebida na caixa de entrada em nome da *DocuSign*, clique no *link ANALISAR DOCUMENTO*. Ao clicar, você será redirecionado para o website da DocuSign.
4. No navegador, cole o valor copiado no passo 2 e cole no campo *Código de acesso*.
5. Clique no botão *Validar*.



ETAPA 5: Análise e confirmação do Termo de Aceite

Requisitos

1. Nesta etapa, no website da DocuSign, clique no botão *Continuar*.
2. Role o documento para baixo, e na página seguinte clique no ícone *Rubricar*, e ao final das páginas no ícone *Assinar*.
3. Clique no botão Concluir.
4. Na janela *Salvar uma cópia do seu documento*, você pode ser inscrever para obter uma conta DocuSign gratuita e assinar todos os seus documentos eletronicamente. Nesta janela, também é possível clicar no ícone *Fazer Download* e baixar uma cópia do documento assinado.
5. Clique no botão *Submeter*. Ao clicar no botão Submeter, você aceita os Termos e Condições e reconhece que seus dados serão utilizados conforme descrito na Política de Privacidade da DocuSign.



Salvar uma cópia do seu documento

Inscreva-se agora para obter uma conta DocuSign GRATUITA e assinar todos os seus documentos eletronicamente.

E-mail
joao.silva@wizcredi.com.br

Senha

Confirmar Senha

País
-- selecione --

Ao clicar no botão "SUBMETER" abaixo, você aceita os [Termos & Condições](#) e reconhece que seus dados serão utilizados conforme descrito na [Política de Privacidade](#) da DocuSign.

Assinar o documento eletronicamente.

Obter assinaturas de outras pessoas

Sign on the go with DocuSign Mobile!

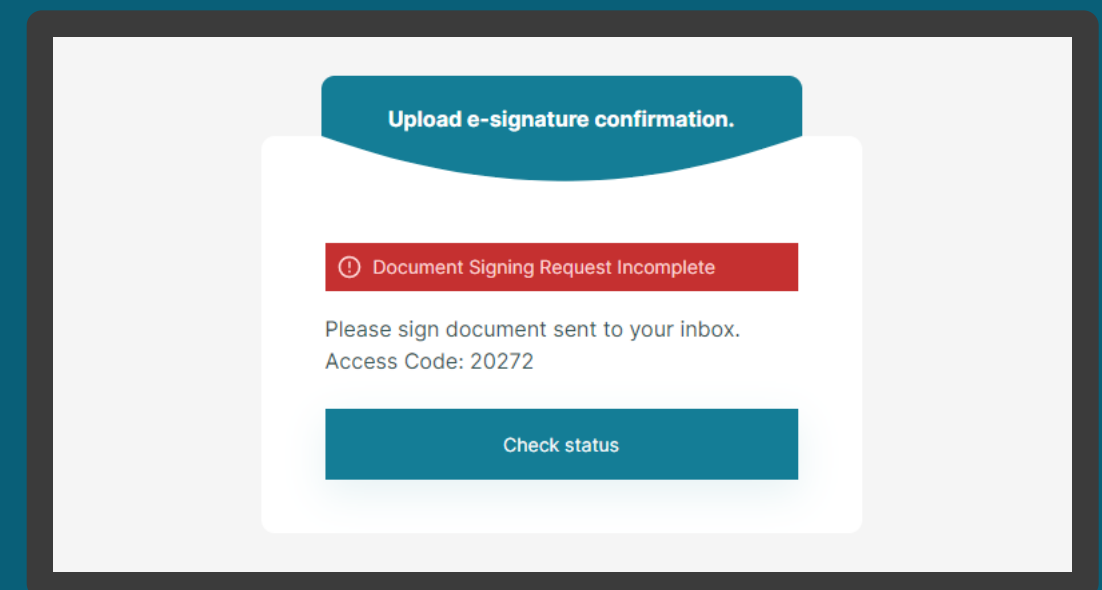
SUBMETER NÃO, OBRIGADO



ETAPA 5: Análise e confirmação do Termo de Aceite

Requisitos

6. Na caixa de entrada, você receberá um e-mail enviado pela DocuSign contendo um cópia do documento *Termo de Aceite* assinado eletronicamente.
7. Retorne ao Diretório, e na janela *Upload e-signature confirmation* clique no botão *Check status*. Se todas as etapas anteriores forem validadas com sucesso, você será automaticamente redirecionado à página inicial do Diretório.





03.

Acessando uma Organisation

Esta seção descreve as etapas necessárias para exibir detalhes de uma organização.

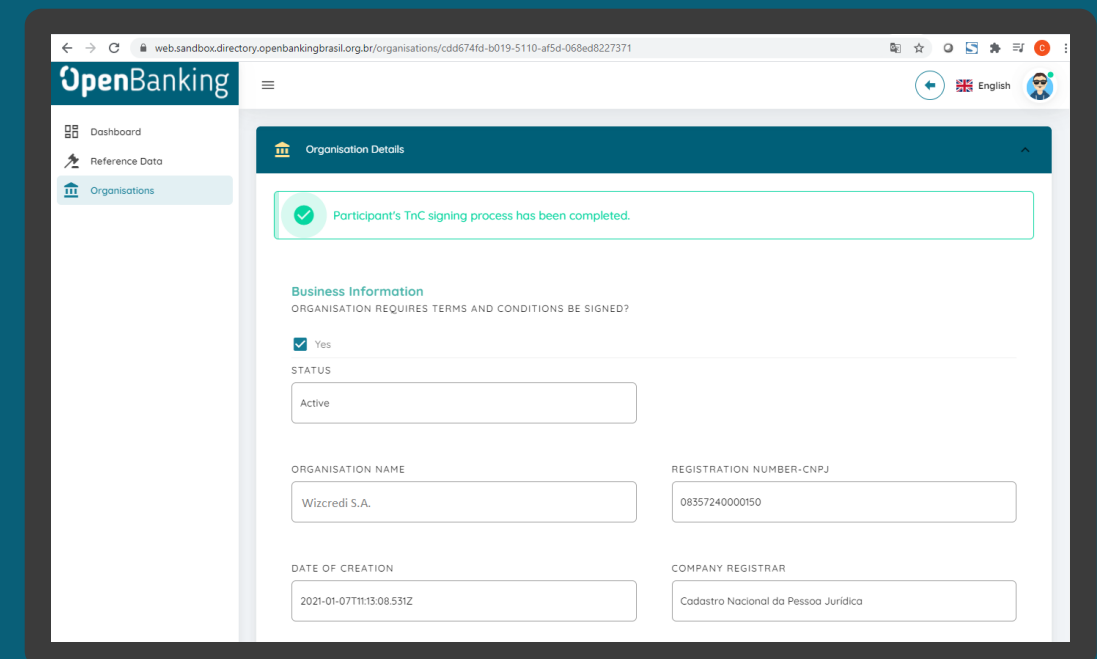
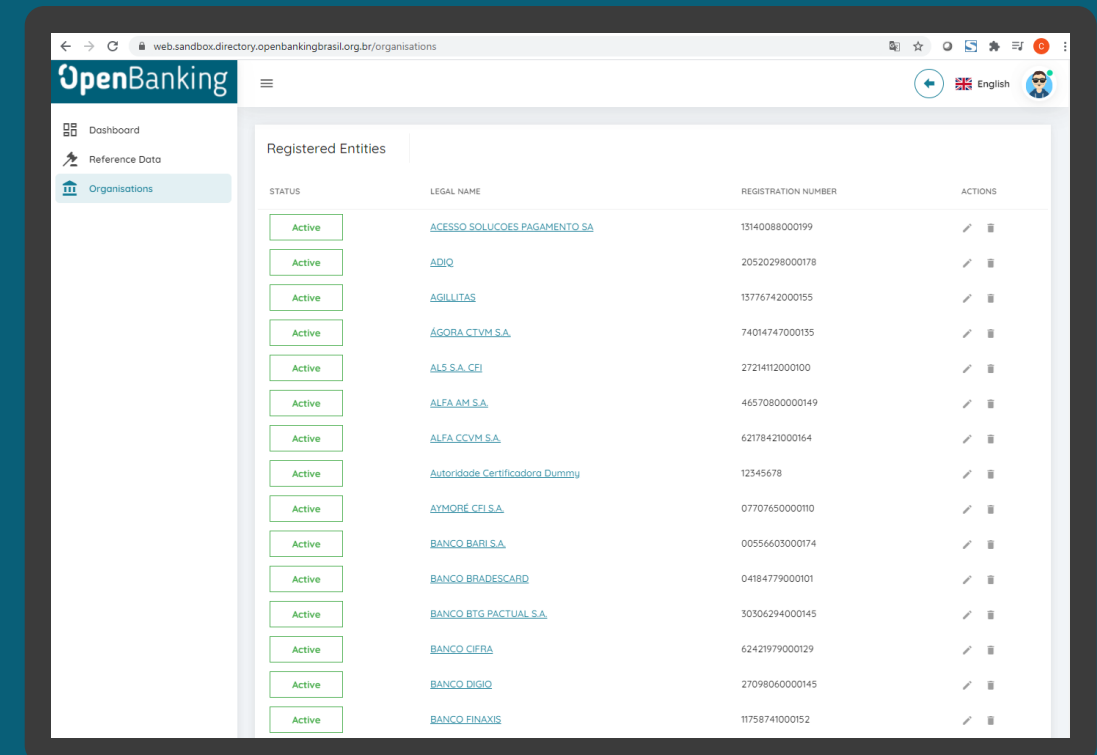


ETAPA 1: Exibindo detalhes de uma organização

Requisitos

1. No Diretório, localize e selecione a sua organização.
2. Revise as informações previamente cadastradas.

NOTA: Os cadastrados foram realizados de forma antecipada a partir de informações fornecidas junto ao Banco Central do Brasil. É fundamental que as organizações verifiquem as informações cadastradas. Em Caso exista alguma divergência entre em contato pelo e-mail cadastro@openbankingbr.org



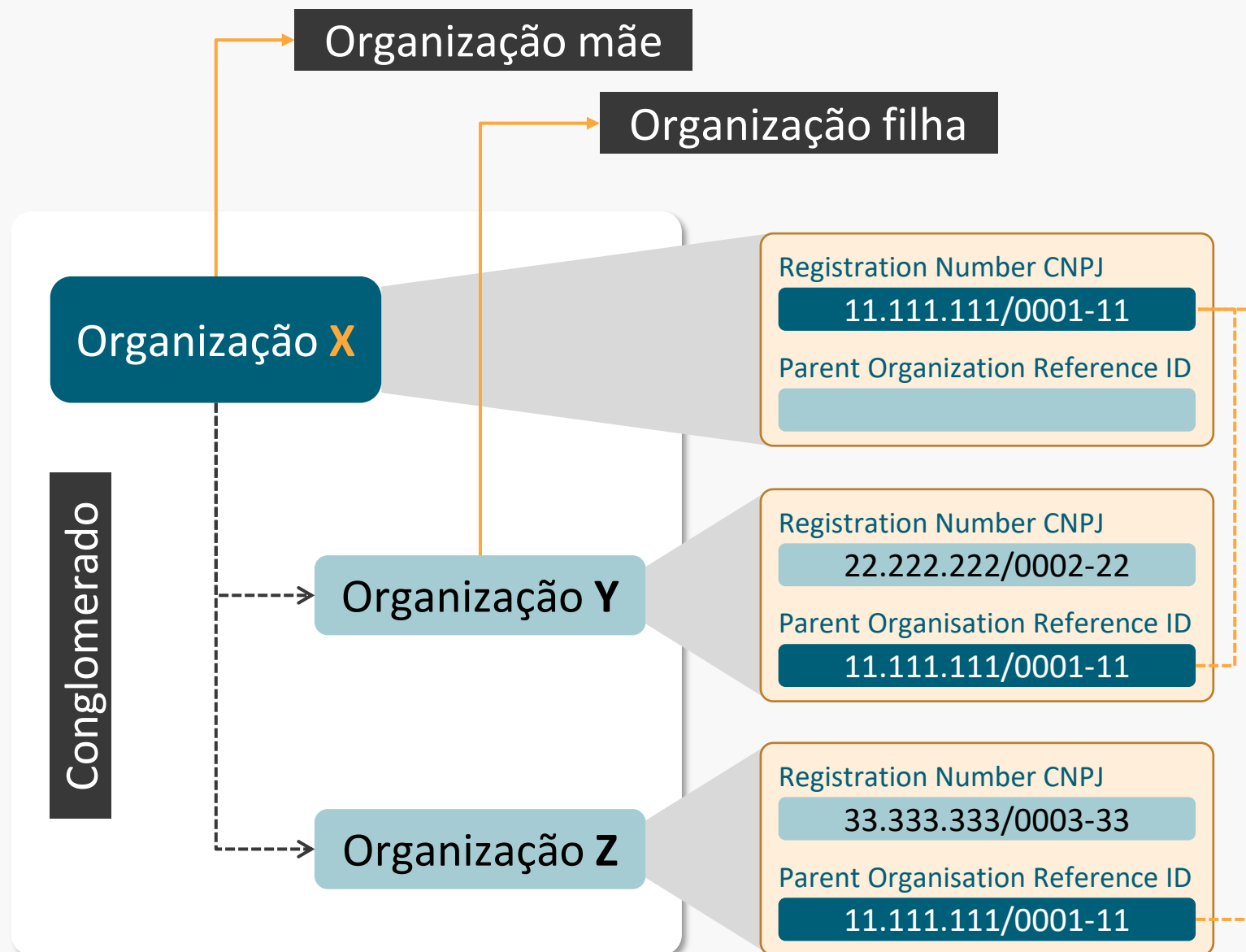


Detalhamento dos campos

Nome do campo	Descrição	Exemplo
Status	Define o estado atual do cadastro, se ativo ou não.	Active
Organisation Name	Deve ser informado o nome da organização.	BCO Wizcredi S.A.
Registration Number-CNPJ	Deve ser informado o número de Cadastro Nacional da Pessoa Jurídica (CNPJ) da organização.	22.222.222/0002-22
Date of Creation	Data de criação do registro de cadastro da organização.	2021-01-07T11:13:08.531Z
Company Registrar		Cadastro Nacional da Pessoa Jurídica
Organisation ID	Identificador da organização. Esta informação será gerada automaticamente.	cdc674fd-b019-5110-af5d-0268ed8227371
Parent Organisation Reference ID	Deve ser informado o número de Cadastro Nacional da Pessoa Jurídica (CNPJ) da organização mãe para casos em que seja necessário a constituição de um conglomerado. O slide Cadastramento de conglomerados ilustra este cenário em mais detalhes.	11.111.111/0001-11
Legal Name	Deve ser informado o nome legal de cadastro da instituição.	Banco Wizcredi S.A.
Address Line 1	Deve ser informado o logradouro da organização.	Av. Dr. Chucri Zaidan 296
Address Line 2	Deve ser informado o logradouro da organização.	Cidades Monções
City	Deve ser informado a cidade da organização.	São Paulo, SP
Country	Deve ser informado o país da organização.	BR



CADASTRAMENTO DE CONGLOMERADO



No diretório de participantes há o conceito de conglomerado.

Assim, **uma organização mãe poderá ser referenciada em um cadastro de uma organização filha**, atribuindo-se o CNPJ da organização mãe no campo PARENT ORGANISATION REFERENCE ID da organização filha.



Importante! Se a sua organização faz parte de um conglomerado é fundamental referenciar as organizações filhas com a organização mãe.



04.

Cadastrando contatos de notificação

Após o *onboarding* da instituição e do representante da mesma é necessário realizar o cadastro da equipe de contatos de notificação no Diretório Central. Esses contatos são para possíveis comunicações entre os participantes e a estrutura central.



ETAPA 1: Cadastrando um novo contato

Requisitos

1. No Diretório, localize e selecione a sua organização.
2. Selecione o menu *Contacts* e clique no botão *New Contact*.
3. Na janela *New Contact* preencha os campos do formulário. O slide a seguir apresenta cada um dos campos em mais detalhes.
4. Clique no botão *Save*.

NOTA: Os usuários de notificação não possuem ações dentro do Diretório e nas demais plataformas do perímetro central.

STATUS	CONTACT TYPE	EMAIL ADDRESS	PHONE NUMBER	ACTIONS
--------	--------------	---------------	--------------	---------

☒ Status

Contact Information

CONTACT TYPE*
Type of contact

DEPARTMENT
The contact's department

FIRST NAME
The contact's given Name

LAST NAME
The contact's family name

EMAIL*
The contact's email address

PHONE NUMBER*
Phone Number

ADDITIONAL INFORMATION
Incident notification e-mail group



Detalhamento dos campos

Nome do campo	Descrição	Exemplo
Contact Type*	Tipo do contato (Business/Negócio, Technical/Técnico, Billing/Cobrança, Incident/Incidente e Security/Segurança)	Business
Department	Deve ser informado o departamento do contato	Gerencia de Open Banking
First Name	Deve ser informado o primeiro nome do contato	João
Last Name	Deve ser informado o sobrenome do contato	Silva
Email*	O endereço de e-mail do contato	joao.silva@wizcredi.com.br
Phone Number*	Deve ser informado o número de telefone do contato	+55 51 900000000
Additional Information	Deve ser informado o e-mail para o grupo de notificação do contato.	openbanking@wizcredi.com.br
PGP Public Key	Chave pública PGP	
Address Line 1	Deve ser informado o endereço (Rua, Avenida ou Alameda)	Av. Dr. Chucri Zaidan 296
Address Line 2	Deve ser informado o bairro	Cidades Monções
City	Deve ser informado a cidade de domicílio	São Paulo
Post Code	Deve ser informado o código postal	99.999-99
Country	Deve ser informado o país de domicílio	Brasil

*Campo obrigatório



05.

Cadastrando reivindicações de domínio de autoridade

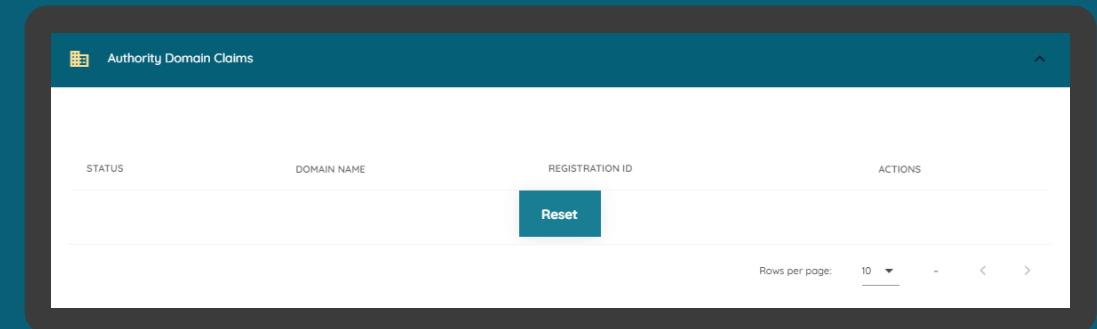
Esta seção explica as etapas para cadastrar reivindicações de domínio de autoridade.



ETAPA 1: Cadastrando uma nova reivindicação de domínio

Requisitos

1. No Diretório, localize e selecione a sua organização.
2. Selecione o menu *Authority Domain Claims* e clique no botão *New Domain Claim*.
3. Na janela *New Authority Domain Claim* preencha os campos do formulário. O slide a seguir apresenta cada um dos campos em mais detalhes.
4. Clique no botão *Save*.





Detalhamento dos campos

Nome do campo	Descrição	Exemplo
Authority Name*	Informe o nome da autoridade.	Banco Central do Brasil
Authorisation Domain Name*	Informe o nome de domínio de autorização.	Open Banking Brasil
Authority ID	Exibe o identificador de autoridade única. Esta informação será gerada automaticamente.	5360d5bf-5024-47cd-bd18-daab08df38ba
Registration ID	Informe o ID de registro de reivindicação de domínio exclusivo. Não é necessário preencher esta informação.	<CNPJ-OBB>

*Campo obrigatório



06.

Cadastrando reivindicações de autoridade

Esta seção explica as etapas para cadastrar reivindicações de autoridade e como adicionar usuários com suas respectivas funções que serão desempenhadas pela organização dentro do Open Banking.



Detalhamento das modalidades

Nome da modalidade no diretório	Descrição
DADOS	Instituição transmissora e/ou receptora de dados é a instituição que sendo: <ul style="list-style-type: none">• Transmissora de dados: instituição participante que compartilha os dados com a instituição receptora;• Receptora de dados: instituição participante que apresenta solicitação de compartilhamento à instituição transmissora para recepção dos dados.
CONTA	Instituição detentora de conta é a instituição participante que mantém conta de depósitos à vista ou de poupança ou conta de pagamento pré-paga de cliente.
PAGTO	Instituição prestadora de serviço de iniciação de transação de pagamento é uma instituição participante que presta serviço de iniciação de transação de pagamento sem deter em momento algum os fundos transferidos na prestação do serviço.
CCORR	Instituição que tenha firmado, na condição de contratante, contrato de correspondente no País, cujo objeto contemple a atividade de atendimento prevista no art. 8º., inciso V, da Resolução nº 3.954, de 24 de fevereiro de 2011, por meio eletrônico.

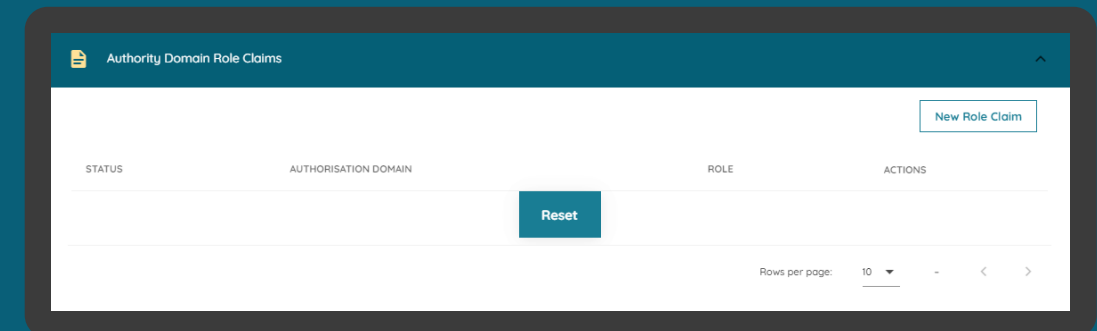
NOTA: As modalidades assumidas pelos participantes no âmbito do Open Banking são auto declaratórias e podem ser exercidas simultaneamente. Contudo, tais modalidades deverão estar em conformidade com o modelo de negócio do participante e estarão sujeitas à verificação pela fiscalização do Banco Central do Brasil, especialmente com relação ao cumprimento do princípio da reciprocidade no compartilhamento de dados no Open Banking Brasil.



ETAPA 1: Cadastrando uma nova reivindicação de função

Requisitos

1. Necessário realizar a seção [Cadastrando reivindicações de domínio de autoridade](#).
2. No Diretório, localize e selecione a sua organização.
3. Selecione o menu *Authority Domain Role Claims* e clique no botão *New Role Claim*.
4. Na janela *New Authority Domain Role Claim* preencha os campos do formulário. O slide a seguir apresenta cada um dos campos em mais detalhes.
5. Clique no botão *Save*.



☒ Active

Authority Information

AUTHORITY NAME*

Authority Name

AUTHORISATION DOMAIN NAME*

Authorisation Domain

ROLE*

Authorisation Domain Role

UNIQUE TECHNICAL IDENTIFIER
Unique Technical Identifier

REGISTRATION ID*
Unique Registration Number

Cancel Save



Detalhamento dos campos

Nome do campo	Descrição	Exemplo
Authority Name*	Selecione o nome da autoridade.	Banco Central do Brasil
Authorisation Domain Name*	Selecione o nome de domínio de autorização.	Open Banking Brasil
Role*	Selecione a modalidade (função) sendo um dos valores: CONTA, DADOS, CCORR ou PAGTO, para obter mais detalhes verifique em Detalhamento das modalidades .	DADOS
Unique Technical Identifier	Selecione o identificador técnico único.	
Registration ID*	Deve ser informado o número de registro único [ISPB-OBB-FUNÇÃO]. Substitua o [ISPB] pelos primeiros 8 dígitos do seu CNPJ e o [FUNÇÃO] pela sigla da função que você está inserindo.	12345678-OBB-DADOS

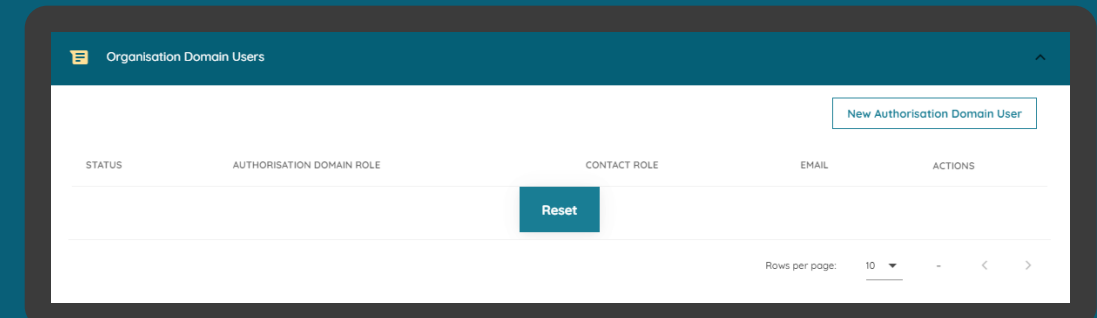
*Campo obrigatório



ETAPA 2: Cadastrando um usuário de domínio de autorização

Requisitos

1. Necessário realizar a [Cadastrando uma nova reivindicação de domínio](#).
2. No Diretório, localize e selecione a sua organização.
3. Selecione o menu *Authority Domain Role Claims* e clique no link *Open Banking Brasil* na qual se deseja cadastrar os usuários.
4. Na janela *New Authority Domain Role Claim* role a página para baixo e selecione o menu *Organisation Domain Users* clique no botão *New Authorisation Domain User*.
5. Na janela *New Authorisation Domain User* preencha os campos do formulário. O slide a seguir apresenta cada um dos campos em mais detalhes.
6. Clique no botão *Save*.



New Authorisation Domain User

☒ Status

Authorisation Domain Information

DOMAIN NAME
The authorisation domain to which this domain claim is mapped

Open Banking Brasil

AUTHORISATION DOMAIN ROLE
Role mapped to the authorisation domain

DADOS

Organisation Domain Users Information

SYSTEM*
The System of the contact

System

CONTACT ROLE*
The Role assumed by the contact

Contact Role

EMAIL*
Email address of the contact

Cancel Save



Detalhamento dos campos

Nome do campo	Descrição	Exemplo
Domain Name	É apresentado o domínio de autorização para o qual esta a reivindicação de domínio está mapeada.	Open Banking Brasil
Authorisation Domain Role	É apresentada a função mapeada para o domínio de autorização.	DADOS
System*	Selecione o sistema de contato sendo um dos valores a seguir: <i>Directory</i> , <i>Service Desk</i> , <i>Dispute Resolution</i> , <i>Portal</i> ou <i>Centralized Platform</i> . Para obter mais detalhes verifique em Sistemas e Funções de um usuário/contato .	Directory
Contact Role*	Selecione o papel assumido pelo contato. Para obter mais detalhes verifique em Sistemas e Funções de um usuário/contato .	PBC
Email*	Deve ser informado o endereço de e-mail corporativo do contato.	joao.silva@wizcredi.com.br

*Campo obrigatório



SISTEMAS E FUNÇÕES DE UM USUÁRIO/CONTATO

System		Contact Role		
Operação	Directory	PTC	Primary Technical Contact	Contato Técnico Primário
		PBC	Primary Business Contact	Contato de Negócio Primário
		STC	Secondary Technical Contact	Contato Técnico Secundário
		SBC	Secondary Business Contact	Contato de Negócio Secundário
Plataforma	Service Desk	PSDC	Primary Service Desk Contact	Contato de Service Desk Primário
		SSDC	Secondary Service Desk Contact	Contato de Service Desk Secundário
	Dispute Resolution	PDC	Primary Dispute Contact	Contato de Disputa Primário
		SDC	Secondary Dispute Contact	Contato de Disputa Secundário
	Portal	PPC	Primary Portal Contact	Contato de Portal Primário
		SPC	Secondary Portal Contact	Contato de Portal Secundário
	Centralized Platform	PCPC	Primary Centralized Platform Contact	Contato de Plataforma Centralizada Primário
		SCPC	Secondary Centralized Platform Contact	Contato de Plataforma Centralizada Secundário

Notas

- Para obter mais detalhes dos poderes do usuário verifique a tabela [Modelo de Segurança](#).
- Podem existir quantos contatos primários e secundários a instituição achar necessário.
- Contatos primários podem acessar o Diretório e adicionar contatos secundários. Já os Contatos secundários não conseguem acessar o Diretório e consequentemente, não conseguem adicionar novos usuários secundários.
- A implementação dos poderes de acesso de contatos primários e secundários dependem e podem variar de plataforma.



07.

Cadastrando um Authorisation Server

Durante a jornada de consentimento do usuário, os receptores exibirão a marca e o servidor de autorização que está sendo solicitado o acesso aos dados do usuário. Esta seção descreve as etapas necessárias para cadastrar as marcas e os servidores de autorização da organização.



ETAPA 1: Criando um novo servidor de autorização

Requisitos

1. No Diretório, localize e selecione a sua organização.
2. Selecione o menu *Authorisation Servers* e clique no botão *New Authorisation Server*.
3. Na janela *New Authorisation Server* preencha os campos do formulário. O slide a seguir apresenta cada um dos campos em mais detalhes.

New Authorisation Server

☒ Active ☒ dynamic client registration

Authorisation Server Information

CUSTOMER FRIENDLY SERVER NAME*
The common name of the authorisation server

URIs

OPENID DISCOVERY DOCUMENT URI*
The URI to the location of the OpenID discovery document

PAYLOAD SIGNING CERTIFICATE URI*
The URI to the location of the payload signing certificate

CUSTOMER FRIENDLY LOGO URI*
The URI to the organisation's branding artefacts

DEVELOPER PORTAL URI*
The URI of the developer portal

TERMS OF SERVICE URI*
The location the terms of service document



Detalhamento dos campos

Nome do campo	Descrição	Exemplo
Active*		
Dynamic Client Registration*		
Customer Friendly Server Name*	Deve ser definido o valor da marca que será exibido no receptor. Apresentar seu nome por inteiro, sem abreviações, de forma a ser reconhecido pelo cliente e aderente a interfaces menores. Limite de caracteres: 256 (padrão do campo) Para mais informações sobre marca, consulte o Guia de Experiência de Usuário.	Wizcredi
OpenID Discovery Document URI*	O URI para a localização do documento de descoberta OpenID.	https://www.wizcredi.com.br/.well-known/openid-configuration
Payload Signing Certificate URI*	O URI para a localização do certificado de assinatura.	https://www.wizcredi.com.br/jwks

*Campo obrigatório



Detalhamento dos campos

Nome do campo	Descrição	Exemplo
Customer Friendly Logo URI*	Deve ser definida a URI para o logotipo da marca. Para obter mais detalhes sobre formato, dimensão e peso máximo do arquivo consulte o Guia de Experiencia Fase 2.	https://www.wizcredi.com.br/logo.svg
Developer Portal URI	O URI do portal do desenvolvedor.	https://developers.wizcredi.com.br
Terms Of Service URI	A URI de localização do documento de termos e serviços da organização.	https://www.wizcredi.com.br/tos.html
Notification Webhook Endpoint	Endpoint do Webhook de notificação. A seção Configurando eventos de notificação no Diretório descreve esta configuração em mais detalhes.	https://webhook.site/9d84a827-c200-4170-b0f8-f830170037bb
Description*	<ol style="list-style-type: none">1. Limite de caracteres: 256 (padrão do campo)2. Não deve ser permitido que a descrição traga links3. O que deve conter:<ul style="list-style-type: none">• Esse é um texto de marcação onde deverá ser descrita a marca, trazendo informações adicionais para que o cidadão não tenha dúvidas sobre a escolha feita.4. Orientações sobre o que pode conter:<ul style="list-style-type: none">• Texto institucional de apresentação• Desde quanto atua• Diferenciais de atuação• Canais de atendimento	Esse é um texto de marcação onde deverá ser descrita a marca, trazendo informações adicionais para que o cidadão não tenha dúvidas sobre a escolha feita.

*Campo obrigatório



Detalhamento do logotipo

O logotipo das instituições participantes deverá ser aplicado no Portal do Cidadão e também poderá ser aplicado no redirecionamento entre instituições durante a Jornada de Compartilhamento de Dados.

Por isso foram deliberadas práticas para uso e disponibilização:

- Utilizar preferencialmente logotipo prioritário, que os clientes reconheçam nos canais;
- Versão reduzida do logo, símbolo ou favicon de site;
- Enviar arquivo SVG contendo a área de proteção do logo da instituição para garantir a leitura e o espaçamento correto;
- Formato de envio:
 - SVG**
 - Dimensão mínima: 512px x 512px
 - Sem sombra
- Peso máximo do arquivo: 1 mega;





08.

Cadastrando recursos de uma API

Esta seção explica as etapas para cadastrar os *endpoints* de recursos de uma API.



CADASTRAMENTO DE RECURSOS FASE 1

Para cada uma das famílias de APIs devem ser adicionadas todos os endpoints disponíveis. Supondo que a instituição tenha disponibilizado dados em todos os endpoints da fase 1, a publicação deveria ser:

TYPE ↑ API DISCOVERY ENDPOINTS	
admin	https://api.instituicao.com.br.com.br/open-banking/admin/v1/metrics ✕
products-services	https://api.instituicao.com.br.com.br/open-banking/products-services/v1/personal-accounts ✕ https://api.instituicao.com.br.com.br/open-banking/products-services/v1/business-accounts ✕ https://api.instituicao.com.br.com.br/open-banking/products-services/v1/personal-loans ✕ https://api.instituicao.com.br.com.br/open-banking/products-services/v1/business-loans ✕ https://api.instituicao.com.br.com.br/open-banking/products-services/v1/personal-financings ✕ https://api.instituicao.com.br.com.br/open-banking/products-services/v1/business-financings ✕ https://api.instituicao.com.br.com.br/open-banking/products-services/v1/personal-invoice-financings ✕ https://api.instituicao.com.br.com.br/open-banking/products-services/v1/business-invoice-financings ✕ https://api.instituicao.com.br.com.br/open-banking/products-services/v1/personal-credit-cards ✕ https://api.instituicao.com.br.com.br/open-banking/products-services/v1/business-credit-cards ✕ https://api.instituicao.com.br.com.br/open-banking/products-services/v1/personal-unarranged-account-overdraft ✕ https://api.instituicao.com.br.com.br/open-banking/products-services/v1/business-unarranged-account-overdraft ✕
channels	https://api.instituicao.com.br.com.br/open-banking/channels/v1/branches ✕ https://api.instituicao.com.br.com.br/open-banking/channels/v1/electronic-channels ✕ https://api.instituicao.com.br.com.br/open-banking/channels/v1/phone-channels ✕ https://api.instituicao.com.br.com.br/open-banking/channels/v1/shared-automated-teller-machines ✕ https://api.instituicao.com.br.com.br/open-banking/channels/v1/banking-agents ✕
discovery	https://api.instituicao.com.br.com.br/open-banking/discovery/v1/status ✕ https://api.instituicao.com.br.com.br/open-banking/discovery/v1/outages ✕



CADASTRAMENTO DE RECURSOS FASE 2

Na Fase 2 o padrão de cadastramento continua como na Fase 1, segue alguns pontos de atenção:

- A API de consentimento é necessário apenas o cadastramento de uma entrada para o GET e o DELETE;
- A API de customers foi dividida em duas famílias para facilitar o consumos pelos receptores. Customers-business onde é cadastrado os Endpoints PJ e customers-personal onde será cadastrado os endpoints PF. Cabendo aqui o cadastramento conforme a disponibilização do produto pela instituição;
- O cadastramento de recursos deve respeitar a tabela de etapas da implementação assistida, conforme IN BCB nº 120 de 25/6/2021.

TYPE	API DISCOVERY ENDPOINTS
consents	https://api.banco.com.br/consents/v1/consents ✕ https://api.banco.com.br/consents/v1/consents/{consentId} ✕
resources	https://api.banco.com.br/resources/v1/resources ✕
customers-business	https://api.banco.com.br/customers/v1/business/qualifications ✕ https://api.banco.com.br/customers/v1/business/financial-relations ✕ https://api.banco.com.br/customers/v1/business/identifications ✕
customers-personal	https://api.banco.com.br/customers/v1/personal/identifications ✕ https://api.banco.com.br/customers/v1/personal/qualifications ✕ https://api.banco.com.br/customers/v1/personal/financial-relations ✕

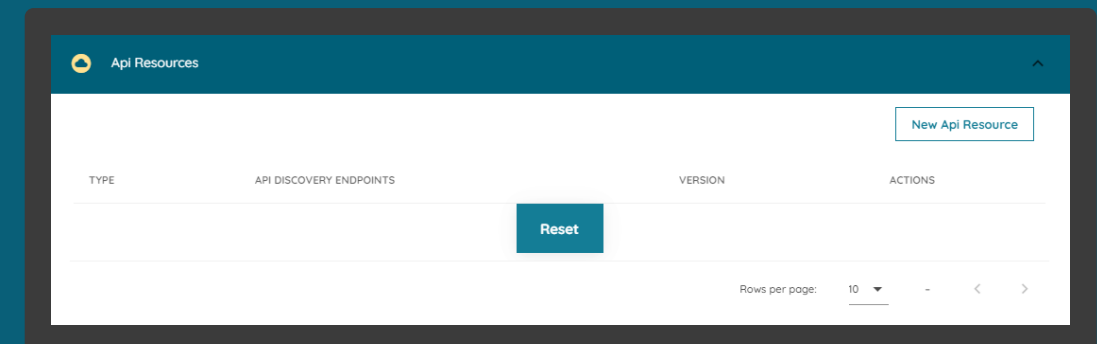
*Exemplo de preenchimento, levando em consideração que a instituição disponibilize tanto PF e PJ e o inicio da implementação assistida.



ETAPA 1: Cadastrando um novo recurso de uma API

Requisitos

1. No Diretório, localize e selecione a sua organização.
2. Selecione o menu *Authorisation Servers* e clique no link do servidor de autorização na qual se deseja cadastrar os recursos. O link cujo o nome representa a marca estará disponível na coluna *Customer Friendly Name*.
3. Na janela *Authorisation Server* role a página para baixo e selecione o menu *API Resources*.
4. Clique no botão *New API Resources* para abrir a janela *New API Resource*.
5. Na janela *New API Resource*, clique na caixa de seleção *API Family Type* e selecione uma das opções disponíveis (*admin*, *products-services*, *channels*, *discovery*, *other*).
6. No campo ao lado, em *Version* especifique o valor apropriado e clique no botão *Save*.



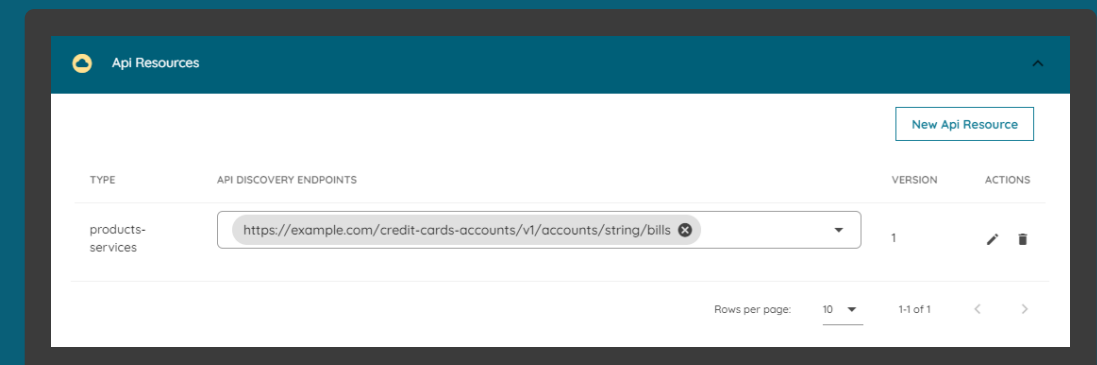


ETAPA 1: Cadastrando um novo recurso de uma API

Requisitos

7. De volta a tela *API Resources*, informe URI principal no campo *API Discovery Endpoints*, e em seguida pressione a tecla *Enter*.
8. Para cada uma das famílias de APIs repita os passos 4 a 7.

Nota: Todos os *endpoints* deverão ser preenchidos, incluindo os respectivos recursos. Para obter mais detalhes sobre o padrão do *endpoints* e versão consulte o [Portal do Desenvolvedor do Open Banking](#).





09.

Criando um Software Statements

Aqui apresentamos a configuração necessária para criar uma nova declaração de software no Diretório.



ETAPA 1: Criando uma nova declaração de software

Requisitos

1. No Diretório, localize e selecione a sua organização.
2. Selecione o menu *Software Statements* e clique no botão *New Software Statement*.
3. Na janela *New Software Statement* preencha os campos do formulário. O slide a seguir apresenta cada um dos campos em mais detalhes.

New Software Statement [X]

☒ Active

Software Statement Details

MODE*
The operational status of the software statement
[Dropdown menu]

VERSION*
The software statement's version number
[Text input field]

ENVIRONMENT*
The operational environment of the software statement
[Text input field]

URIs

CLIENT NAME*
The common name of the software statement's client
[Text input field]

CLIENT URI*
The URI to the software statement's client
[Text input field]

POLICY URI*
The URI to the software statement's policy document
[Text input field]

LOGO URI*
The URI to the software statement's branding artefacts
[Text input field]



Detalhamento dos campos

Nome do campo	Descrição	Exemplo
Mode*		Live
Version*	A versão do software deve ser definida para um valor numérico, um número inteiro (por exemplo, 1) ou um número de ponto flutuante (1,2, 2,2, 3,2 etc.).	1
Environment*		Live
Client Name*	Para registro de software da instituição receptora (software statement), no campo Client Name, recomenda-se usar o nome da Marca, de conhecimento do cliente. Se o nome da marca foi declarado Authorisation Server, por exemplo, pode-se usar o nome da marca que foi utilizado no cadastro (customer friendly server name). Este é o nome que a transmissora irá receber e declarar ao cliente durante a jornada.	Wizcredi
Client URI*	O site ou URI raiz do recurso	https://www.wizcredi.com.br/info.html
Policy URI	Deve ser definido como uma sequência de texto que representa uma URI única de política.	https://www.wizcredi.com.br/policy.html
Logo URI*	Deve ser definida a URI para o logotipo da marca. Para obter mais detalhes sobre formato, dimensão e peso máximo do arquivo consulte o Guia de Experiência Fase 2.	https://www.wizcredi.com.br/logo.svg
Redirect URI*	Os URIs de redirecionamento devem ser definidos como uma string de texto que representa uma URI único de redirecionamento.	https://www.wizcredi.com.br/cb1 https://www.wizcredi.com.br/cb2
Terms of Service URI	Deve ser definido como uma string de texto que representa uma URI única dos Termos de Serviço.	https://www.wizcredi.com.br/tos.html
Description	Deve ser definido como uma string de texto de sua escolha.	Aplicativo Wizcredi para o segmento de varejo
On Behalf Of	O campo “Em nome de” é classificado como opcional para implementação.	<Não se aplica para o contexto do Open Banking Brasil>

*Campo obrigatório



10.

Criando uma nova reivindicação de autoridade de software

Esta seção explica as etapas para criar uma reivindicação de autoridade de software. Esta etapa será necessária para definir as funções regulatórias que serão inseridas no *Software Statement Assertion*.

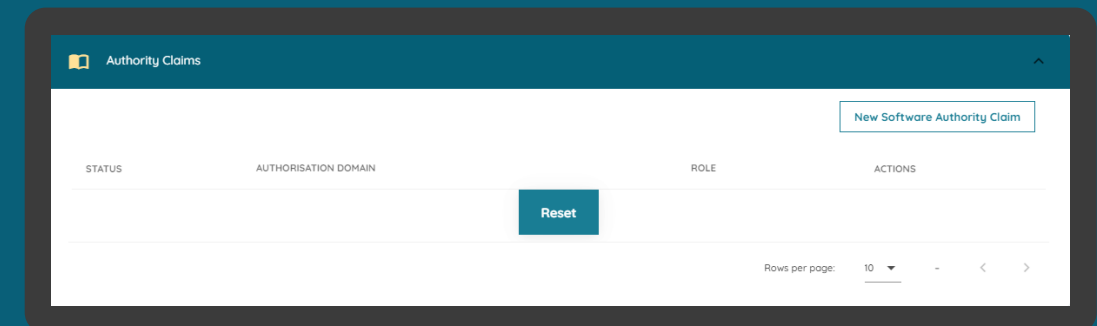


ETAPA 1: Criando reivindicação de autoridade de software

Requisitos

1. Necessário realizar a seção [Cadastrando reivindicações de domínio de autoridade](#).
2. Necessário realizar a seção [Cadastrando reivindicações de autoridade](#).
3. Necessário ter criado uma [Criando um Software Statements](#) para sua organização.
4. No Diretório, selecione a sua organização e vá até a página detalhes da organização.
5. Selecione o menu *Software Statements* e clique no link contendo a declaração de software previamente criada.

Nota: Para mais detalhes consulte a seção [Funções regulatórias para mapeamentos OpenID e OAuth 2.0](#) no documento de especificação para implementadores do [Open Banking Brasil Financial-grade API Dynamic Client Registration 1.0 Implementers Draft 1](#).





ETAPA 1: Criando reivindicação de autoridade de software

Requisitos

6. Na janela *Software Statements Details*, role a página para baixo, selecione o menu *Authority Claims* e clique no botão *New Software Authority Claims*.
7. Na janela *New Software Authority Claims* preencha os campos do formulário. O slide a seguir apresenta cada um dos campos em mais detalhes.

New Software Authority Claim

☒ Status

Authorisation Domain Information

AUTHORISATION DOMAIN NAME* CDR

ROLE*

Cancel Save

Authority Claims

New Software Authority Claim

STATUS	AUTHORISATION DOMAIN	ROLE	ACTIONS
Active	Open Banking Brasil	DADOS	

Rows per page: 10 1-1 of 1



Detalhamento dos campos

Nome do campo	Descrição	Exemplo
Authorisation Domain Name	É apresentado o domínio de autorização para o qual esta a reivindicação de domínio está mapeada.	Open Banking Brasil
Role	É apresentada a função mapeada para o domínio de autorização.	DADOS

*Campo obrigatório



11.

Criando certificados de transporte e assinatura em Sandbox

Esta seção explica as etapas para criar uma solicitação de assinatura de certificado para certificados de transporte e assinatura que não foram emitidos por uma autoridade de certificação e para uso exclusivo em ambiente de Sandbox do Diretório.



ETAPA 1: Criando um novo certificado de transporte

Requisitos

1. Necessário ter criado uma [Criando um Software Statements](#) para sua organização.
2. No Diretório, selecione a sua organização e vá até a página detalhes da organização.
3. Selecione o menu *Software Statements* e clique no link contendo a declaração de software previamente criada.
4. Na janela *Software Statements Details*, role a página para baixo, selecione o menu *Certificates* e clique no botão *New Certificate*.
5. Na janela *New Certificate*, na caixa de seleção *Select Certificate Type* selecione a opção *BRCAC* e clique no botão *Continue*.
6. No passo seguinte, exemplo a seguir acesse a URL [certificate-generation-instructions](#) e descarregue os arquivos de suporte.

New Certificate

1 Select Certificate Type

eg Signing, Transport etc
BRCAC

Continue Cancel

2 Generate CSR

3 Upload CSR/PEM

4 Done

New Certificate

✓ Select Certificate Type

2 Generate CSR

Consult published documentation to generate the required certificate file. Link [here](#).

Continue Cancel

3 Upload CSR/PEM

4 Done



ETAPA 1: Criando um novo certificado de transporte

Requisitos

7. Usando sua própria geração de chaves e políticas de gerenciamento, um par de chaves públicas privadas deve ser criado. A seguir está um exemplo usando [OpenSSL](#) e apenas para fins ilustrativos.
8. Edite o arquivo `brcac.cnf` de forma que as informações contidas neste arquivo sejam idênticas as informações contidas no Diretório na página de detalhes da organização.
9. Edite o arquivo `brcac.sh` para que referencie o caminho do arquivo `brcac.cnf`.
10. Execute o arquivo `brcac.sh` através do prompt de comando para a geração do par CSR e KEY.
11. No Diretório, selecione a opção *Upload CSR/PEM* e localize o `brcac.csr` gerado pela execução do passo anterior e clique no botão *Continue*.

```
pid_section = new_oids
[ new_oids ]
atributos-obrigatorios_cnpj = 2.16.76.1.3.3
atributos-obrigatorios_name_cnpj = 2.16.76.1.3.8

[ req ]
default_bits = 2048 # RSA key size
encrypt_key = no # Protect private key: yes or no. yes recommended
default_md = sha256 # MD to use. sha256 recommended
utf8 = yes # Input is UTF-8.
string_mask = utf8only # Emit UTF-8 strings
prompt = no # Prompt for DN, yes or no.
distinguished_name = client_dn # DN template. Mandatory to include organizationIdentifier
req_extensions = client_reqext # Desired extensions

[ client_dn ]
#Fixed value
countryName = BR
#Organisation Name from directory
organizationName = Open Banking Brasil
#Can be Anything (not validated right now, must be present)
commonName = Whatever
#Software Statement Id
UID = 278bbdde-eeb3-42e4-995c-b265bc0a3014
#One of "Private Organization", "Government Entity", "Business Entity", "Non-Commercial Entity"
businessCategory = Private Organization
#Country of registration of the company
jurisdictionCountryName = BR
#CNPJ/registration number
serialNumber = 1335323600189
```

```

C:\Certificates>openssl req -new -newkey rsa:2048 -nodes -out brcac.csr -keyout brcac.key -config ./brcac.cnf
Generating a RSA private key
.....+++++
.....+++++
writing new private key to 'brcac.key'
-----
```

New Certificate

- ✓ Select Certificate Type
- ✓ Generate CSR
- 3 Upload CSR/PEM
 - Upload CSR
 - brcac.csr (1.5 kB)
- 4 Done

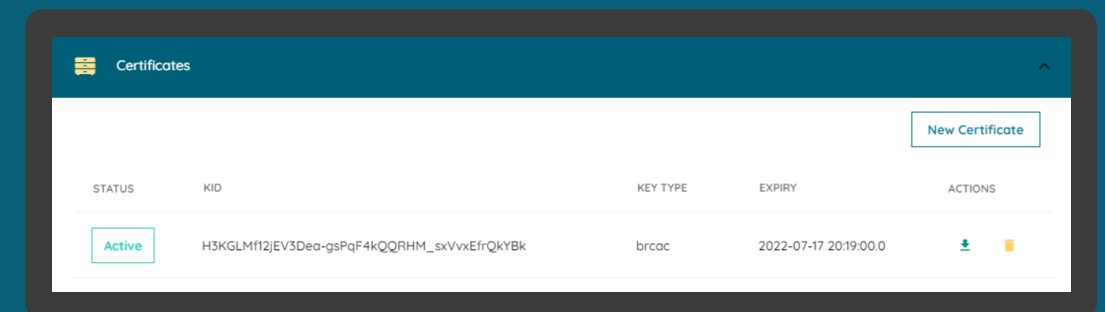
Continue Cancel



ETAPA 1: Criando um novo certificado de transporte

Requisitos

12. Aguarde o carregamento do arquivo para o Diretório e no passo seguinte clique no botão Done.
13. Na tela anterior de *certificates*, vá até *actions* e clique na seta de *download*. Salve o <arquivo>.pem em uma pasta local.



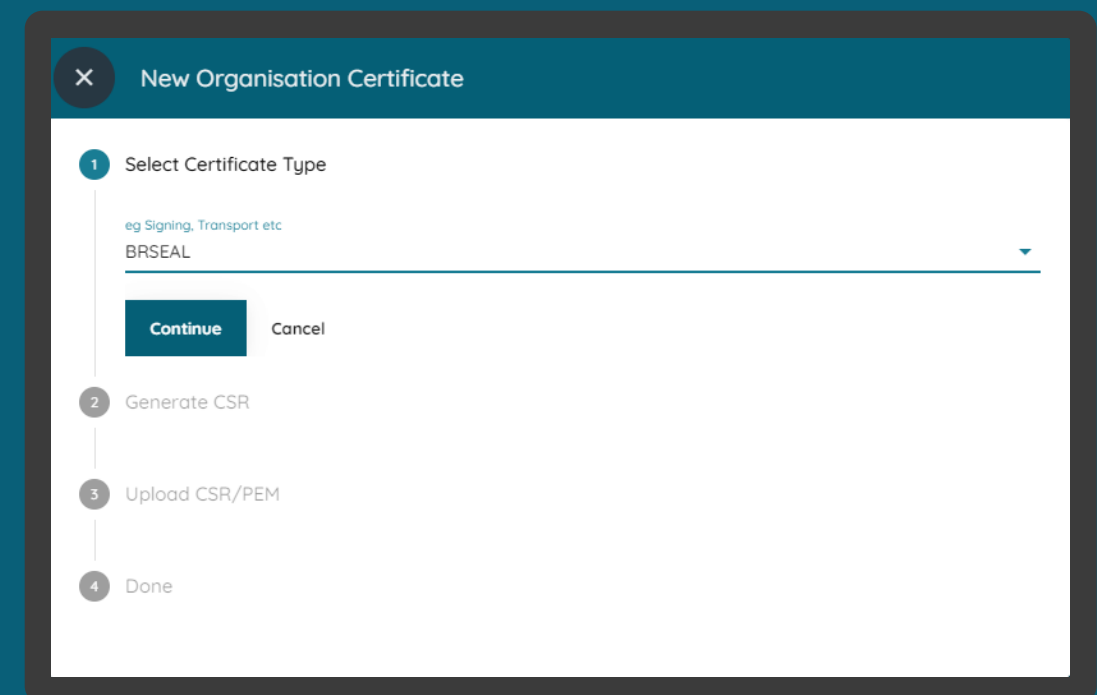
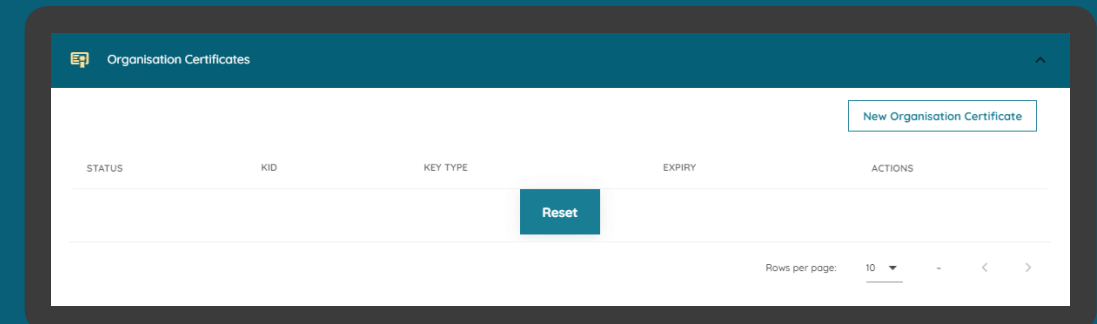


ETAPA 2: Criando um novo certificado de assinatura

Requisitos

1. No Diretório, selecione a sua organização e vá até a página detalhes da organização.
2. Selecione o menu *Organisation Certificates* e clique no botão *New Organisation Certificates*.
3. Na janela *New Organisation Certificate*, na caixa de seleção *Select Certificate Type* selecione a opção *BRSEAL* e clique no botão *Continue*.
4. No passo seguinte, exemplo a seguir acesse a URL [certificate-generation-instructions](#) e descarregue os arquivos de suporte.
5. Usando sua própria geração de chaves e políticas de gerenciamento, um par de chaves públicas privadas deve ser criado. A seguir está um exemplo usando [OpenSSL](#) e apenas para fins ilustrativos.
6. Edite o arquivo `brseal.cnf` de forma que as informações contidas neste arquivo sejam idênticas as informações contidas no Diretório na página de detalhes da organização.

* Maiores informações podem ser encontradas no através desse [link](#).

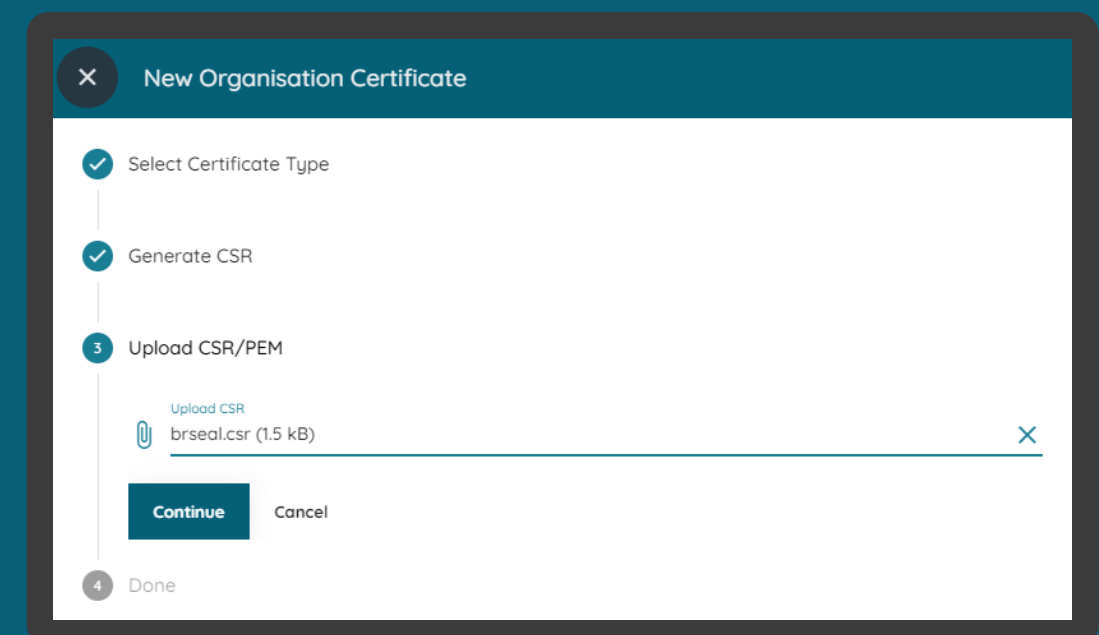
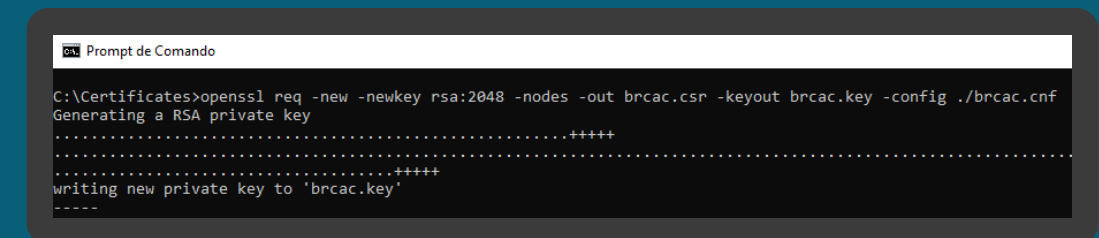
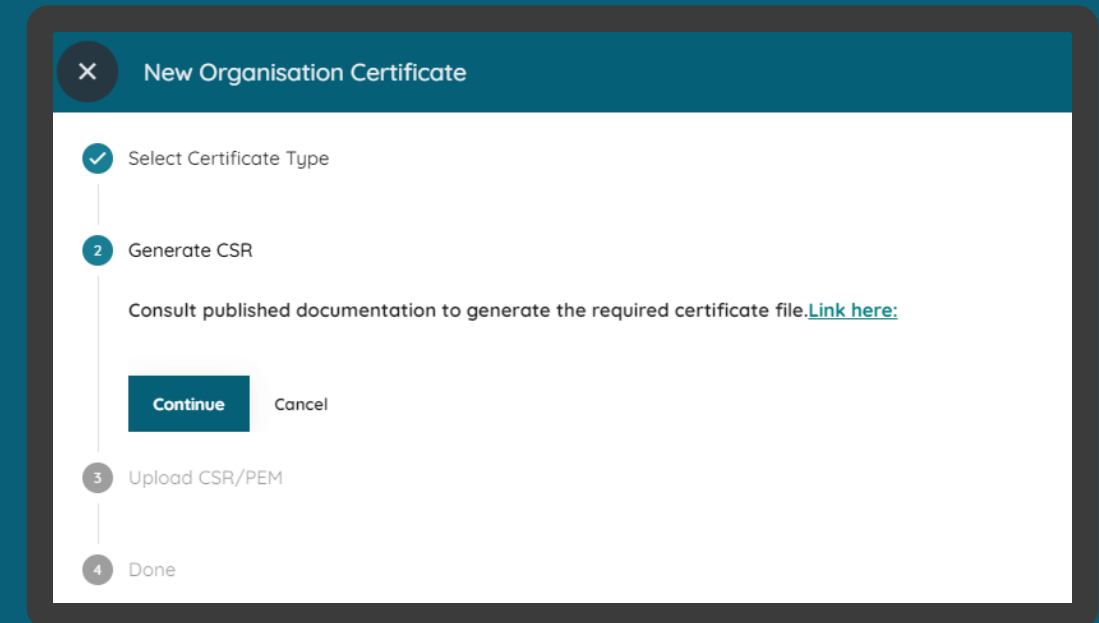




ETAPA 2: Criando um novo certificado de assinatura

Requisitos

7. Edite o arquivo `brseal.sh` para que referencie o caminho do arquivo `brseal.cnf`.
8. Execute o arquivo `brcac.sh` através do prompt de comando para a geração do par CSR e KEY.
9. No Diretório, selecione a opção *Upload CSR/PEM* e localize o `brseal.csr` gerado pela execução do passo anterior e clique no botão *Continue*.
10. Aguarde o carregamento do arquivo para o Diretório e no passo seguinte clique no botão *Done*.
11. Na tela anterior de *certificates*, vá até *actions* e clique na seta de *download*. Salve o `<arquivo>.pem` em uma pasta local.





12.

Carregando certificados emitidos por autoridade de certificação em Produção

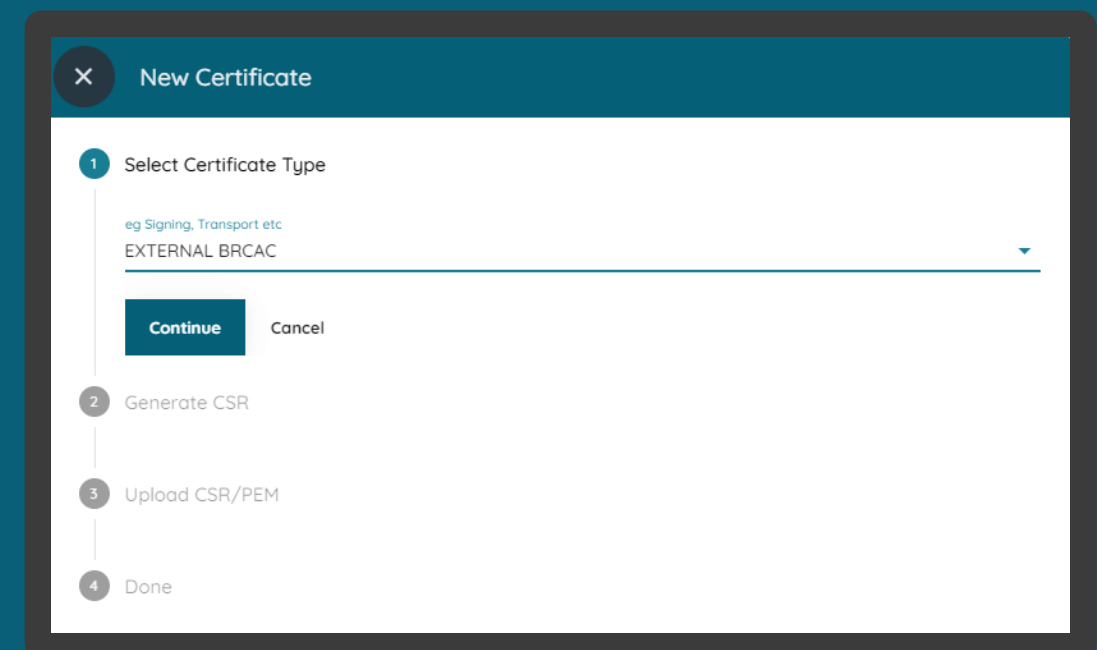
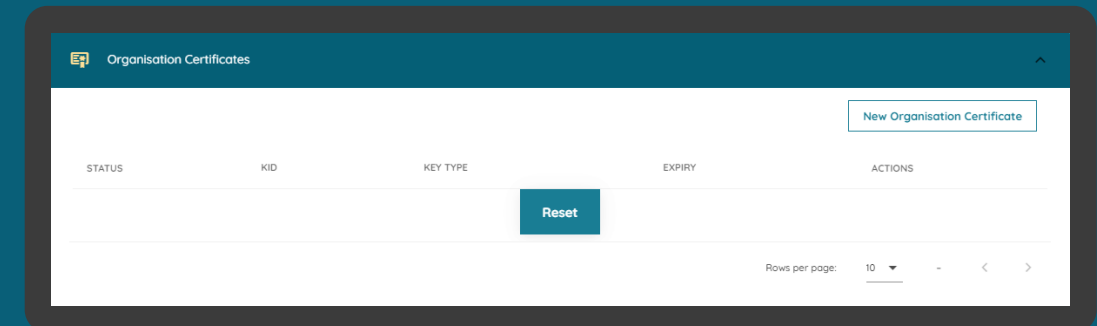
Esta seção explica as etapas para importar certificados que foram emitidos por uma autoridade de certificação e para uso exclusivo em ambiente de Produção do Diretório.



ETAPA 1: Carregando certificado de transporte

Requisitos

1. Necessário ter criado uma [Criando um Software Statements](#) para sua organização.
2. No Diretório, selecione a sua organização e vá até a página detalhes da organização.
3. Selecione o menu *Software Statements* e clique no link contendo a declaração de software previamente criada.
4. Na janela *Software Statements Details*, role a página para baixo, selecione o menu *Certificates* e clique no botão *New Certificate*.
5. Na janela *New Certificate*, na caixa de seleção *Select Certificate Type* selecione a opção *EXTERNAL BRCAC* e clique no botão *Continue*.
6. No passo seguinte, em *Generate CSR*, clique no botão *Continue*.

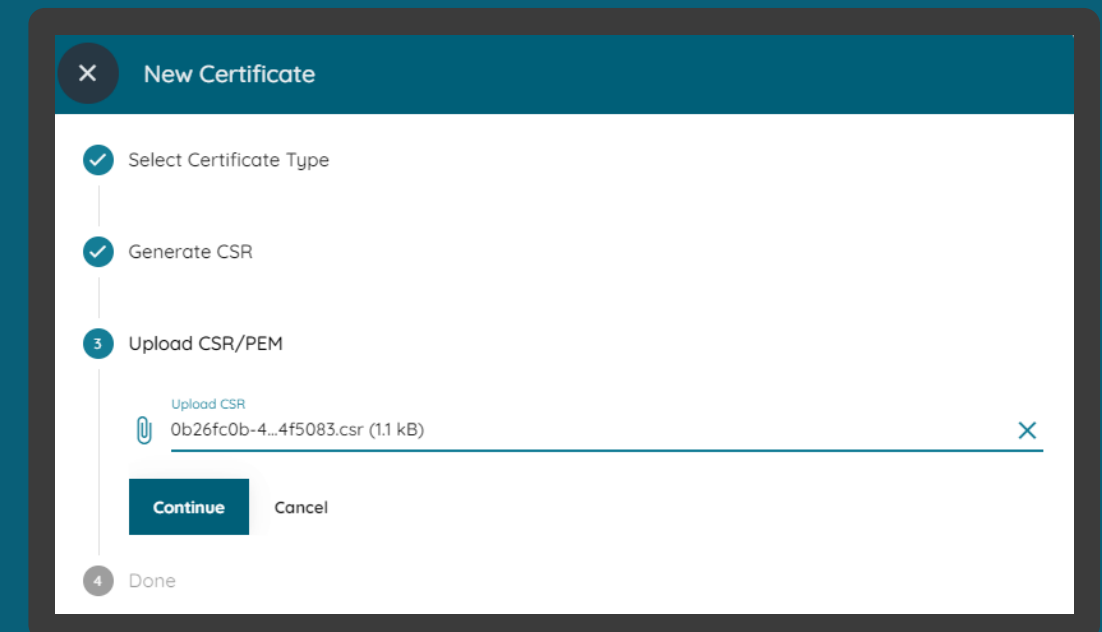




ETAPA 1: Carregando certificado de transporte

Requisitos

7. Na opção *Upload CSR/PEM*, localize o <arquivo>.csr e clique no botão *Continue*.
8. Aguarde o carregamento do arquivo para o Diretório e no passo seguinte clique no botão *Done*.
9. Na tela anterior de *certificates*, vá até *actions* e clique na seta de *download*. Salve o <arquivo>.pem em uma pasta local.

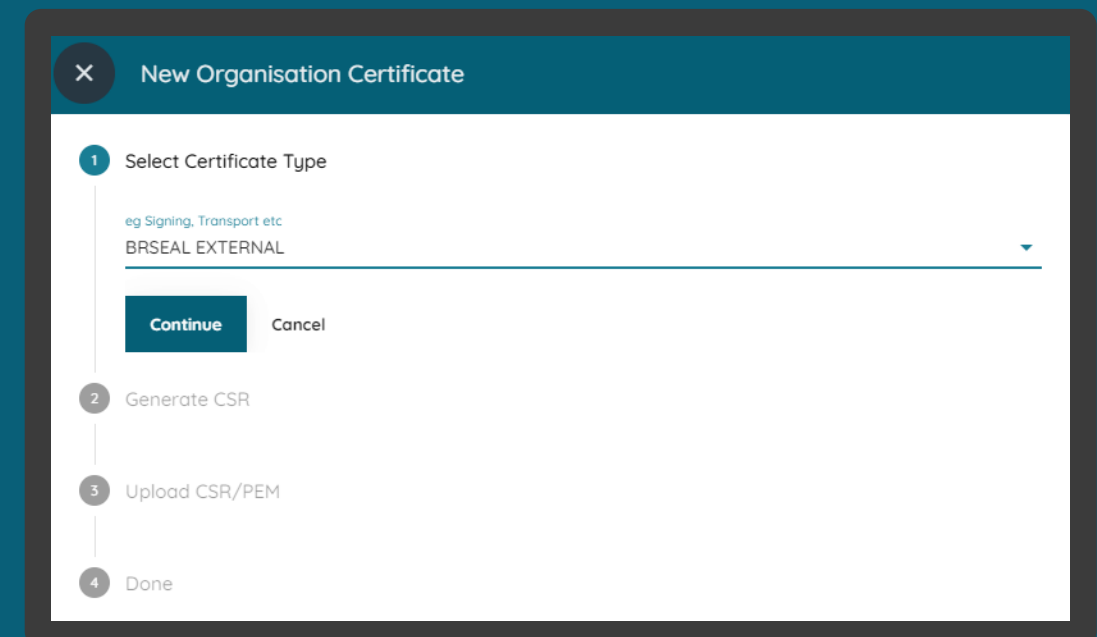
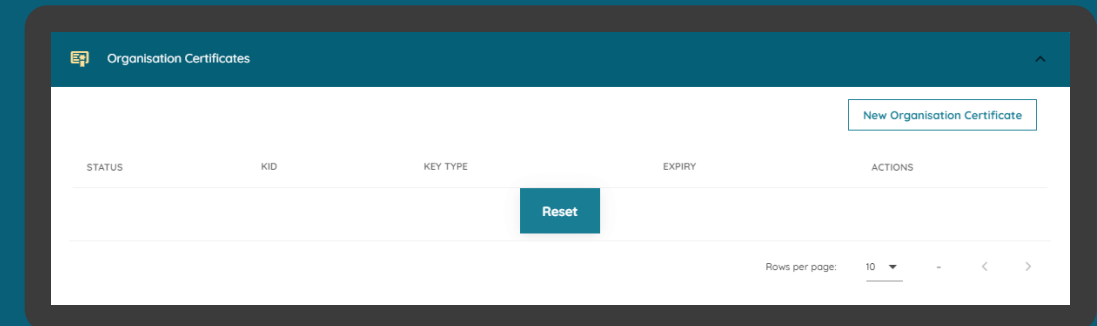




ETAPA 2: Carregando certificado de assinatura

Requisitos

1. No Diretório, selecione a sua organização e vá até a página detalhes da organização.
2. Selecione o menu *Organisations Certificate* e clique no botão *New Organisations Certificate*.
3. Na janela *New Organisations Certificate*, na caixa de seleção *Select Certificate Type* selecione a opção *BRSEAL EXTERNAL* e clique no botão *Continue*.
4. No passo seguinte, em *Generate CSR*, clique no botão *Continue*.
7. Na opção *Upload CSR/PEM*, localize o <arquivo>.csr e clique no botão *Continue*.
8. Aguarde o carregamento do arquivo para o Diretório e no passo seguinte clique no botão *Done*.
9. Na tela anterior em *Organisation Certificates*, vá até *actions* e clique na seta de *download*. Salve o <arquivo>.pem em uma pasta local.





13.

Cadastrando administradores da organização

Esta seção explica as etapas necessárias para realizar o cadastro de um novo administrador da organização.

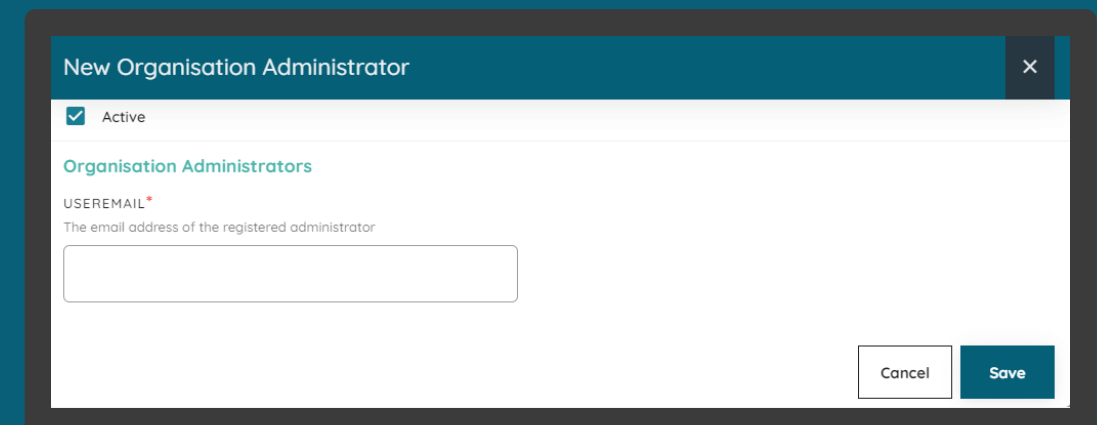
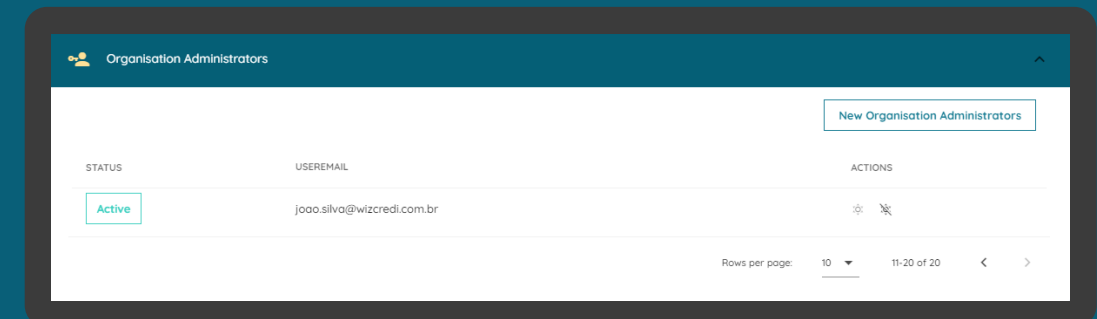


ETAPA 1: Cadastrando um administrador da organização

Requisitos

1. No Diretório, localize e selecione a sua organização.
2. Selecione o menu *Organisation Administrator* e clique no botão *New Organisation Administrators*.
3. Na janela *New Organisation Administrator* preencha o campo do formulário. O slide a seguir apresenta cada um dos campos em mais detalhes.
4. Clique no botão *Save*.

NOTA: Somente administradores da organização podem cadastrar novos administradores.





14.

Obtendo um Software Statements Assertion

Uma Software Statements Assertion (SSA) é um JWT assinado do diretório que contém todas as informações sobre um aplicativo que existe em um determinado momento no diretório. Inclui a localização de todas as chaves públicas vinculadas a esta declaração de software e todos os outros metadados de que um banco precisa para validar a legitimidade do aplicativo.



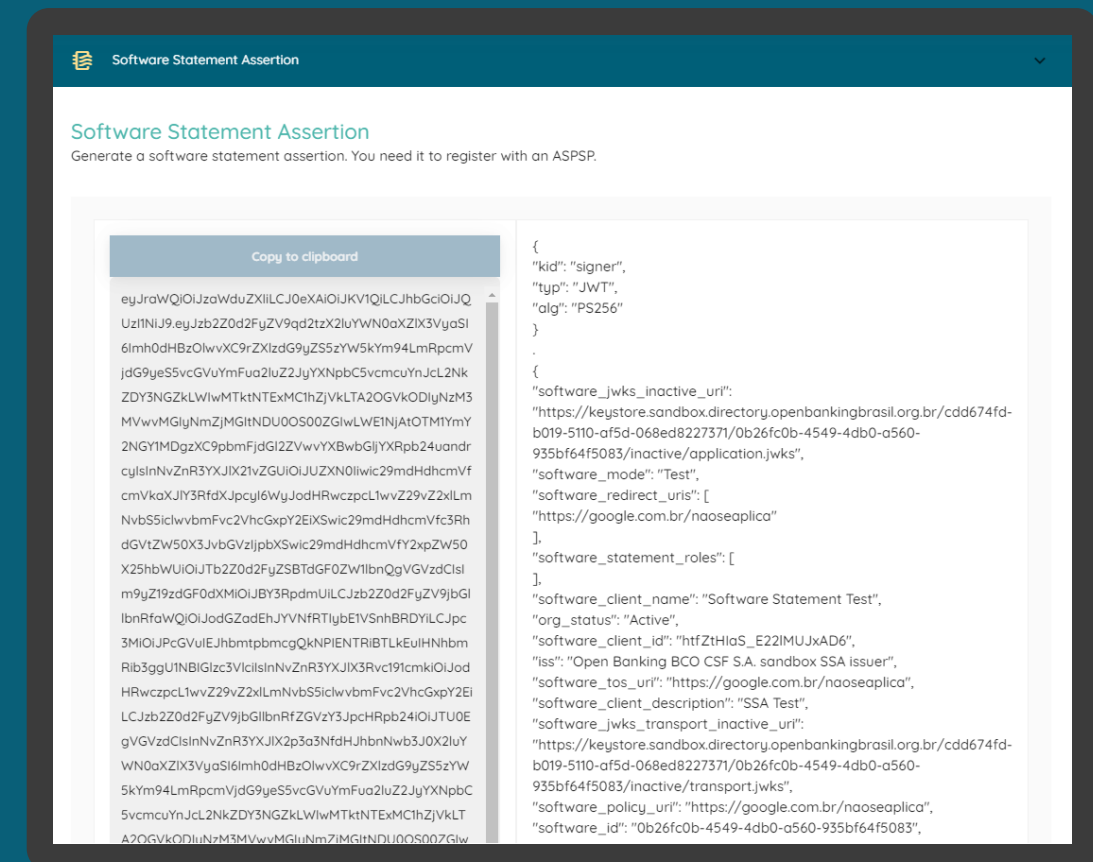
ETAPA 1: Criando uma nova declaração de software assinada

Requisitos

1. Necessário ter criado uma [Criando um Software Statements](#) para sua organização.

ATENÇÃO: Após a geração do SSA os valores do Software Statements serão bloqueados para edição.

1. No Diretório, localize e selecione a sua organização.
2. Vá até o menu *Software Statement*, acesse o artefato criado anteriormente clicando no link *CLIENT NAME*.
3. Na janela *Software Statement Details*, role a página para baixo e selecione o menu *Software Statements Assertion*.
4. Clique no botão *Copy to Clipboard* para copiar o SSA gerado pelo Diretório.





15.

Configurando eventos de notificação no Diretório

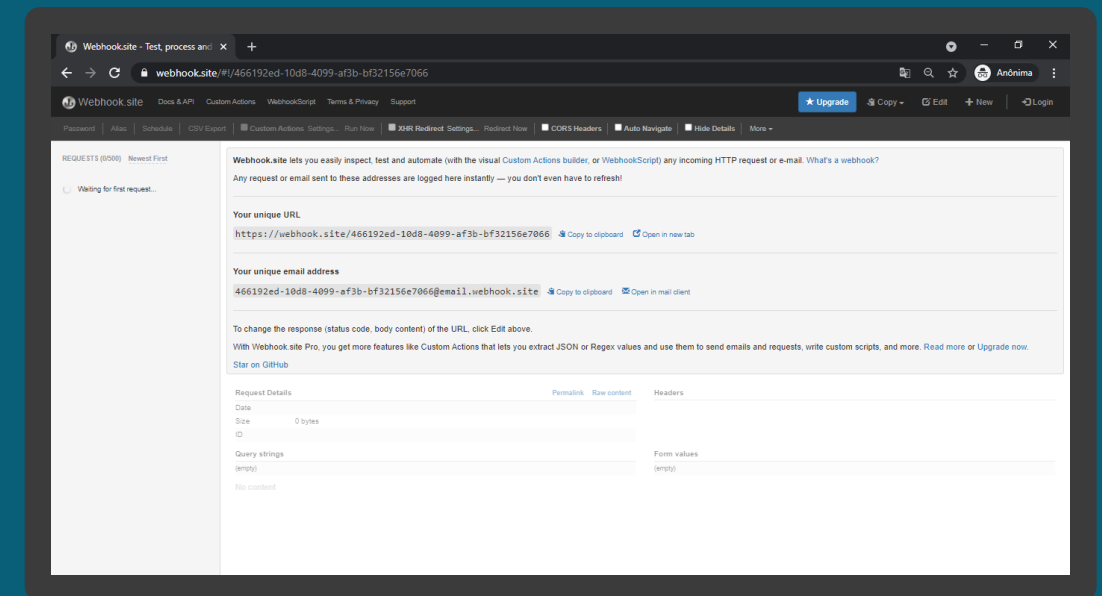
Aqui apresentamos a configuração de *webhook* no Diretório



ETAPA 1: Inscrever-se em um tópico

Requisitos

1. Em seu navegador, navegue até webhook.site e uma URL única e aleatória será gerada automaticamente. Ela poderá ser utilizada para testar e depurar Webhooks e solicitações HTTP.
2. Selecione a URL e copie.

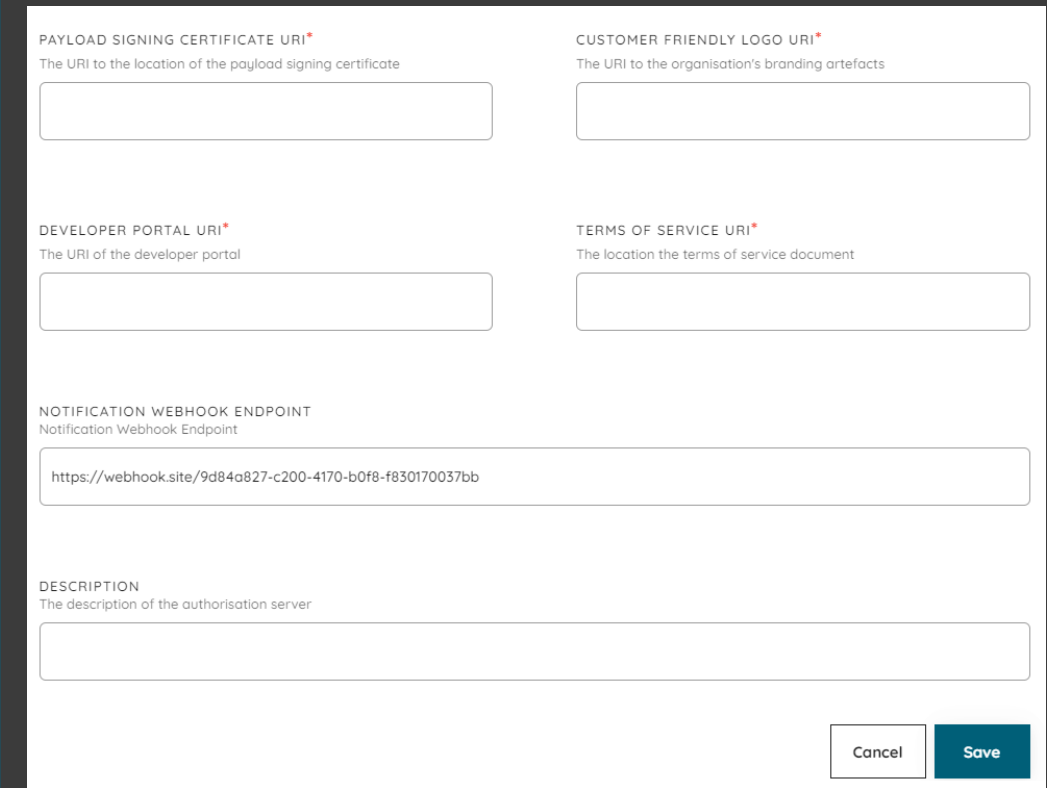




ETAPA 2: Solicitando uma subscrição

Requisitos

1. No Diretório, selecione a sua organização e vá até a página detalhes da organização.
2. Selecione o menu *Authorisation Servers* e em *actions* clique no ícone editar.
3. Na página *Authorisation Server Information* cole a URL obtida na Etapa 1 no campo *Notification Webhook endpoint*.



The screenshot shows a form titled "Authorisation Server Information" with several input fields and buttons. The fields are arranged in a grid-like structure. The first row contains "PAYLOAD SIGNING CERTIFICATE URI*" and "CUSTOMER FRIENDLY LOGO URI*". The second row contains "DEVELOPER PORTAL URI*" and "TERMS OF SERVICE URI*". The third row contains "NOTIFICATION WEBHOOK ENDPOINT". The fourth row contains "DESCRIPTION". At the bottom right, there are "Cancel" and "Save" buttons. The "NOTIFICATION WEBHOOK ENDPOINT" field contains the URL "https://webhook.site/9d84a827-c200-4170-b0f8-f830170037bb".

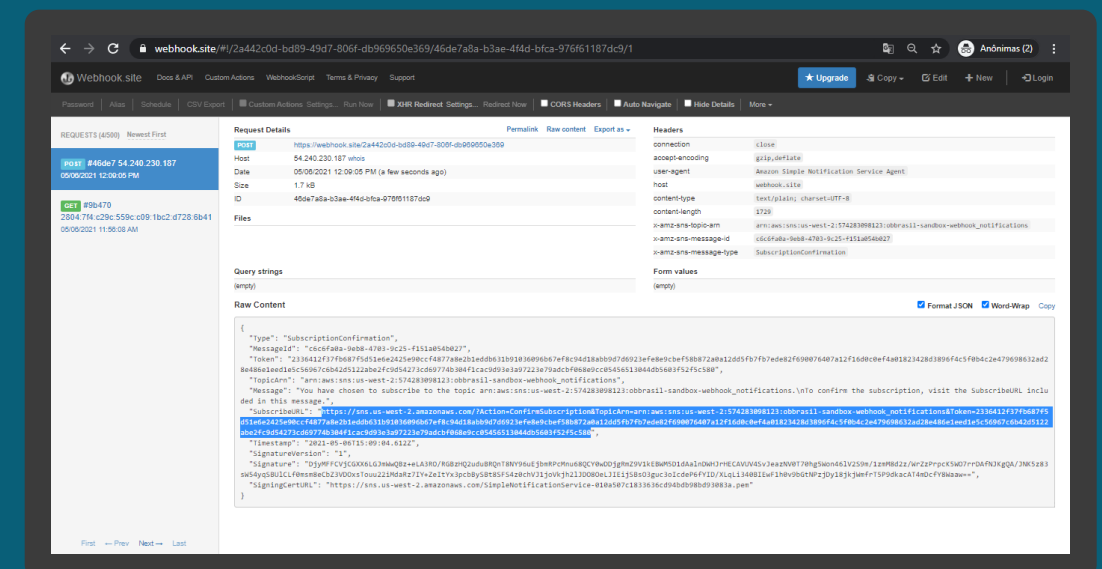
PAYLOAD SIGNING CERTIFICATE URI* The URI to the location of the payload signing certificate	CUSTOMER FRIENDLY LOGO URI* The URI to the organisation's branding artefacts
<input type="text"/>	<input type="text"/>
DEVELOPER PORTAL URI* The URI of the developer portal	TERMS OF SERVICE URI* The location the terms of service document
<input type="text"/>	<input type="text"/>
NOTIFICATION WEBHOOK ENDPOINT Notification Webhook Endpoint	
<input type="text" value="https://webhook.site/9d84a827-c200-4170-b0f8-f830170037bb"/>	
DESCRIPTION The description of the authorisation server	
<input type="text"/>	
<div>Cancel Save</div>	



ETAPA 3: Confirmando uma subscrição

Requisitos

1. De volta ao webhook.site, role para baixo e no campo de texto *Raw Context* selecione e copie a URL em *SubscribeURL* para se inscrever no tópico.
2. Em uma nova aba do navegador, cole a URL obtida no passo anterior.
3. Pronto! A partir daqui, toda e qualquer modificação que ocorra no Diretório será notificada através de eventos.

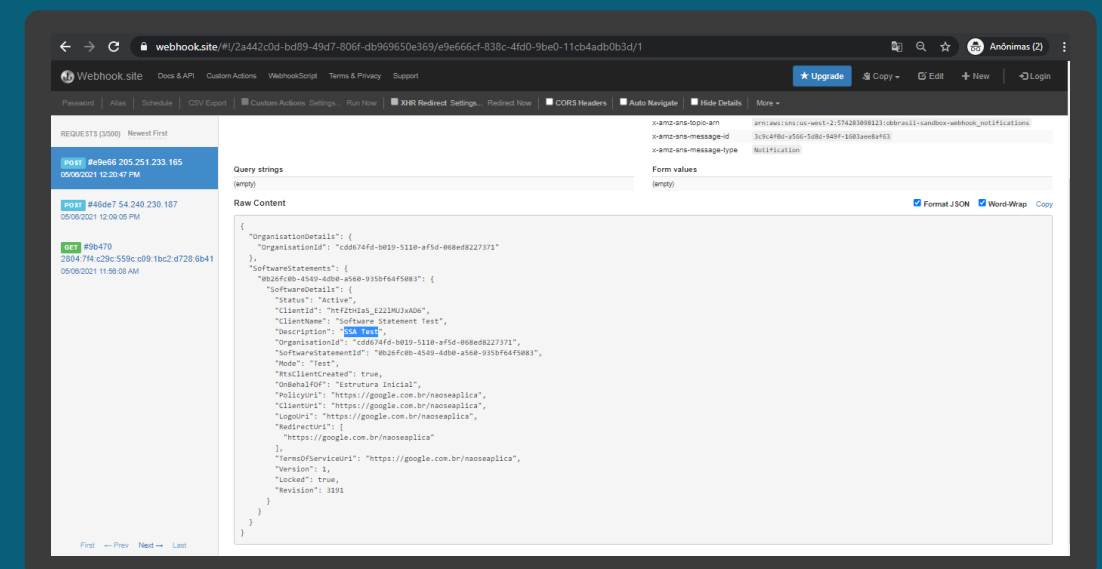




ETAPA 4: Analisando um evento de notificação

Requisitos

1. No Diretório, selecione a sua organização e vá até a página detalhes da organização.
2. Selecione o menu *Software Statement* e em *actions* clique no ícone editar.
3. Na janela *Software Statement Details* vá até o campo *description* e digite qualquer valor e clique no botão Salvar.
4. Neste momento, o Diretório irá enviar uma notificação *push*.
5. De volta ao webhook.site, clique no primeiro evento que surge na lista a esquerda da tela.
6. Role a tela para baixo e no campo de texto *Raw Context* localize o novo valor adicionado no atributo *description*.





16.

Obtendo um token de acesso para as APIs do Diretório

Para acessar as APIs do Diretório do Open Banking, você precisará de um token de acesso. Esta seção descreve as etapas necessárias para adquirir tokens de acesso.



ETAPA 1: Localizando o identificador do cliente

Requisitos

1. Necessário ter criado uma [Criando um Software Statements](#) para sua organização.
2. No Diretório, localize e selecione a sua organização.
3. Vá até o menu *Software Statement*, acesse o artefato criado anteriormente clicando no link *CLIENT NAME*.
4. Na janela *Software Statement Details* localize o campo CLIENT ID, selecione e copie o valor.

The screenshot displays the 'Software Statement Details' page. At the top, there's a header with the AWS logo and 'Software Statement'. Below this, the 'Software Statement Details' section is shown. It includes a 'STATUS' field with the value 'Active'. Below that, there are two columns: 'CLIENT ID' with the value 'htfZtHlaS_E22IMUJxAD6' and 'CLIENT NAME' with the value 'Software Statement Test'. At the bottom, there are two more columns: 'POLICY URI' with the value 'https://google.com.br/naoseaplica' and 'CLIENT URI' with the value 'https://google.com.br/naoseaplica'.

Software Statement Details	
STATUS	
Active	
CLIENT ID	CLIENT NAME
htfZtHlaS_E22IMUJxAD6	Software Statement Test
URIs	
POLICY URI	CLIENT URI
https://google.com.br/naoseaplica	https://google.com.br/naoseaplica



ETAPA 2: Localizando a URI de token no Diretório

Requisitos

1. No navegador, acesse a URI de descoberta de conexão OpenID de acordo com o ambiente utilizado:

Sandbox

<https://auth.sandbox.directory.openbankingbrasil.org.br/.well-known/openid-configuration>

Produção

<https://auth.directory.openbankingbrasil.org.br/.well-known/openid-configuration>

2. Localize o endpoint de token que será utilizado para trocar as credenciais de autenticação para tokens de acesso.

```
{
  "authorization_encryption_enc_values_supported": [
    "A128CBC-HS256",
    "A128GCM",
    "A256CBC-HS512",
    "A256GCM"
  ],
  "request_object_encryption_alg_values_supported": [
    "A128KW",
    "A256KW",
    "dir",
    "ECDH-ES",
    "RSA-OAEP"
  ],
  "request_object_encryption_enc_values_supported": [
    "A128CBC-HS256",
    "A128GCM",
    "A256CBC-HS512",
    "A256GCM"
  ],
  "tls_client_certificate_bound_access_tokens": true,
  "claim_types_supported": [
    "normal"
  ],
  "mtls_endpoint_aliases": {
    "token_endpoint": "https://matls-auth.sandbox.directory.openbankingbrasil.org.br/token",
    "revocation_endpoint": "https://matls-auth.sandbox.directory.openbankingbrasil.org.br/token/revocation",
    "introspection_endpoint": "https://matls-auth.sandbox.directory.openbankingbrasil.org.br/token/introspection",
    "device_authorization_endpoint": "https://matls-auth.sandbox.directory.openbankingbrasil.org.br/device/auth",
    "registration_endpoint": "https://matls-auth.sandbox.directory.openbankingbrasil.org.br/reg",
    "userinfo_endpoint": "https://matls-auth.sandbox.directory.openbankingbrasil.org.br/me",
    "pushed_authorization_request_endpoint": "https://matls-auth.sandbox.directory.openbankingbrasil.org.br/request"
  }
}
```



ETAPA 3: Adicionando certificados SSL por domínio

Requisitos

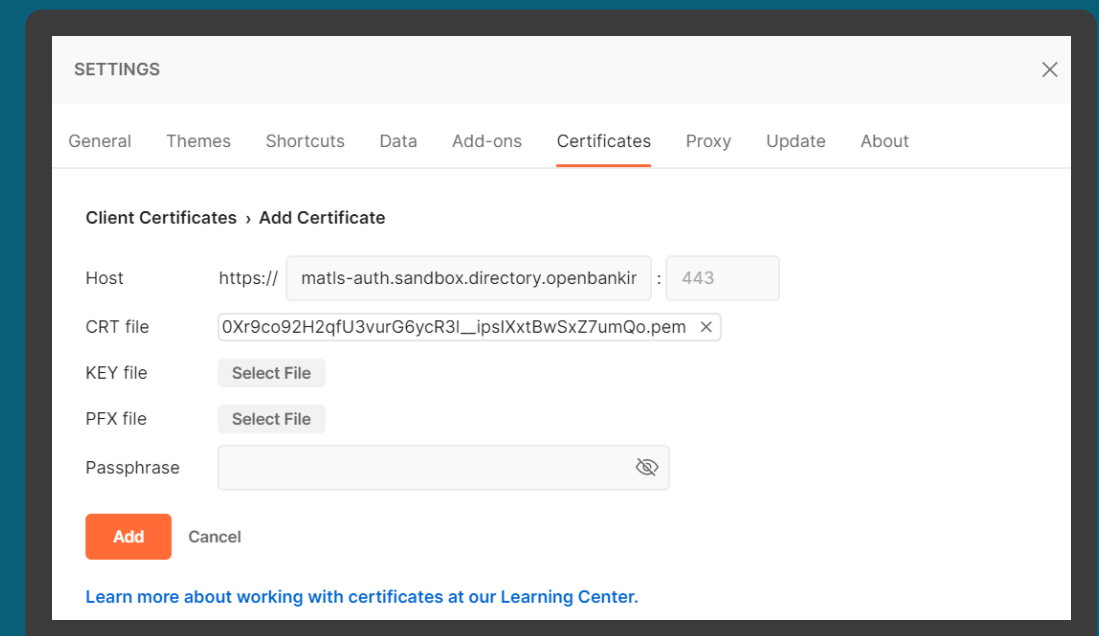
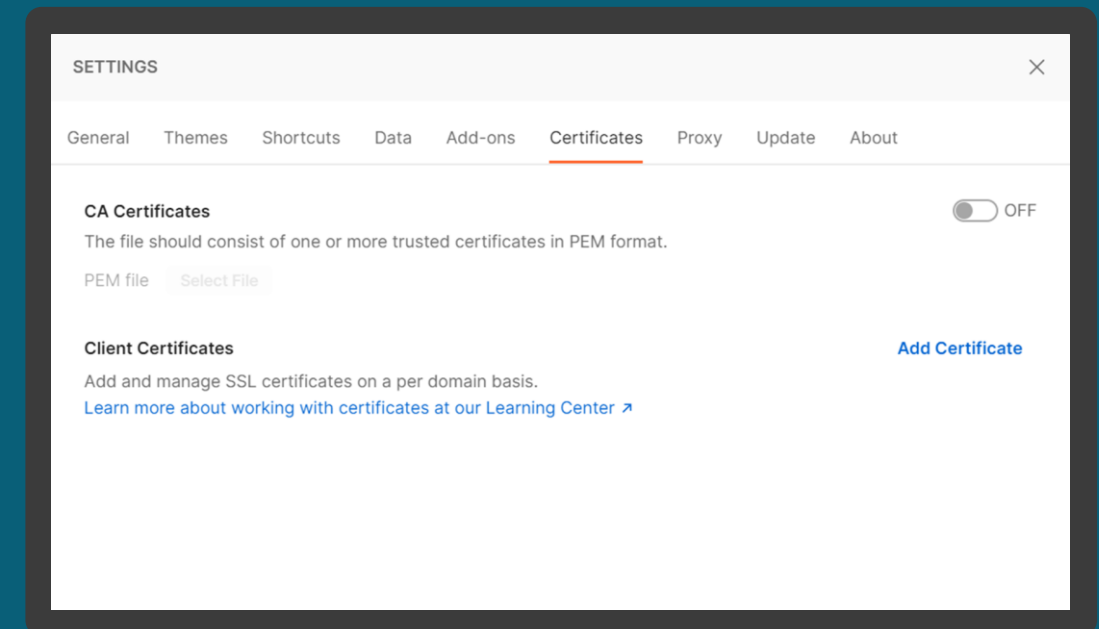
1. Necessário ter criado uma [Criando uma solicitação de Assinatura de Certificado \(CSR\)](#).
2. Para fins ilustrativos será utilizado o [Postman](#) para acessar as APIs do Diretório do Open Banking. Assim, no Postman, selecione o menu *File* e em seguida o menu *Settings*.
3. Na janela *Settings*, selecione o menu *Certificates* e clique no link *Add Certificate*.
4. Na aba *Certificates*, no campo *Host* insira um dos valores descritos a seguir de acordo com o ambiente utilizado:

Sandbox

matls-auth.sandbox.directory.openbankingbrasil.org.br

Produção

matls-auth.directory.openbankingbrasil.org.br

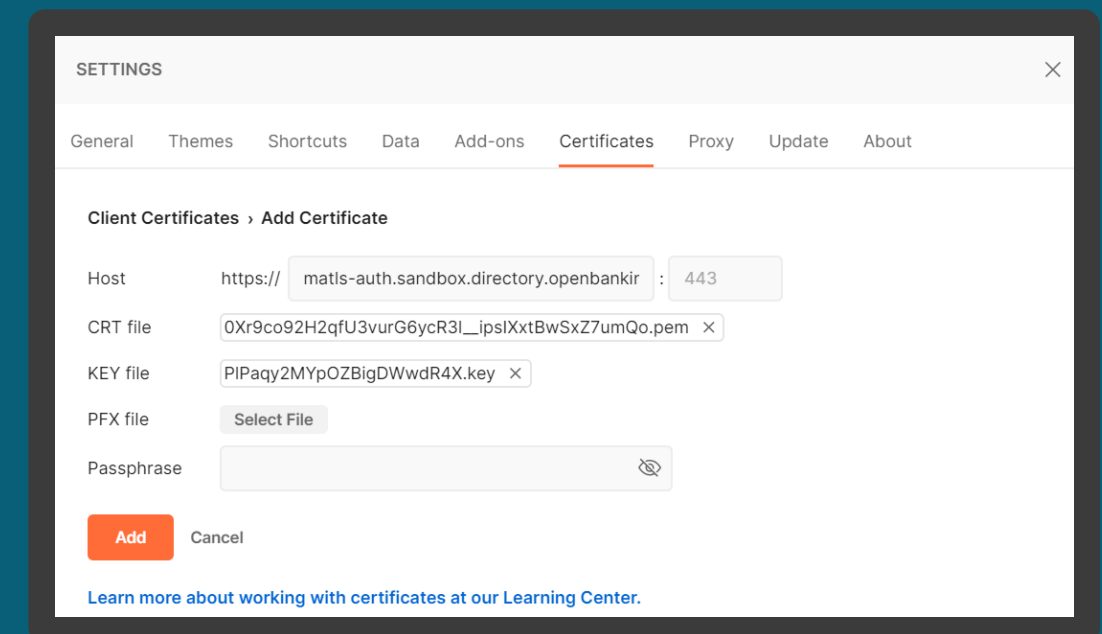




ETAPA 3: Adicionando certificados SSL por domínio

Requisitos

5. Em *CRT file*, clique no botão *Select file*, e localize o <arquivo>.pem obtido na seção [Criando uma solicitação de Assinatura de Certificado \(CSR\)](#).
6. No passo seguinte, clique no botão *KEY File* e localize o <arquivo>.key criado no processo de geração de chaves na seção [Criando uma solicitação de Assinatura de Certificado \(CSR\)](#).
7. Clique no botão *Add*.

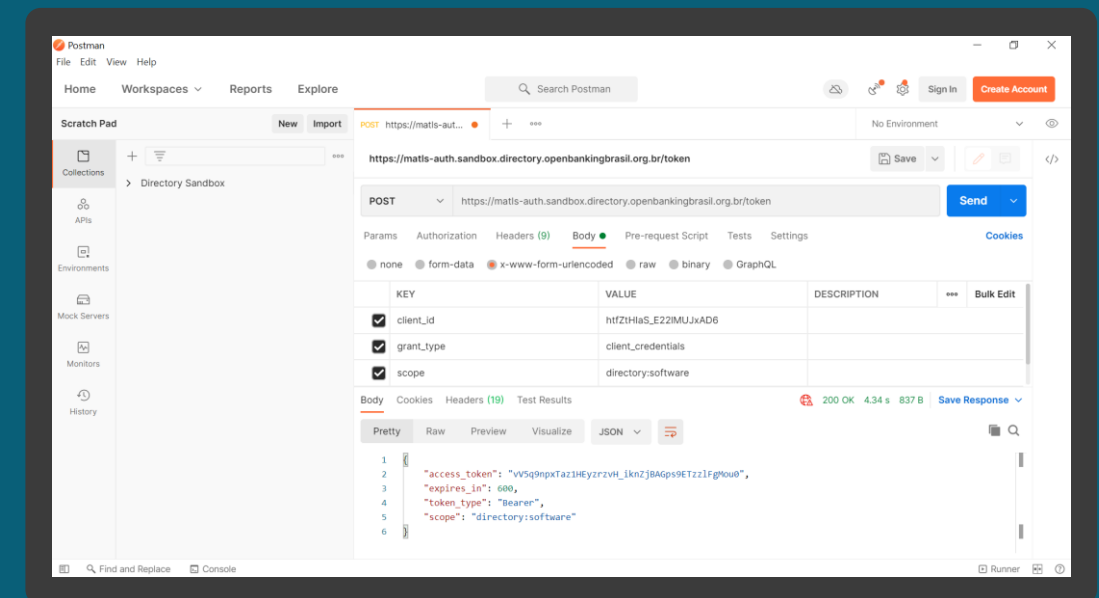




ETAPA 4: Obtendo um token de acesso

Requisitos

1. Para adicionar uma nova requisição a uma coleção, abra uma nova aba e salve a partir daí, ou em *Collection* à esquerda do Postman, clique em ‘...’ na coleção e escolha *Add Request*. Você também pode criar uma solicitação clicando no menu *File > New*, e em seguida *Request*.
2. No campo *Enter request URL*, digite o valor obtido da URI de token mencionado na [etapa 2](#).
3. Defina o tipo da operação para POST.
4. Vá para a guia *Body* e selecione o botão de opção ‘x-www-form-urlencoded’.
5. Insira os parâmetros como descritos a seguir:
client_id = <valor obtido no CLIENT ID na [etapa 1](#)>
grant_type = *client_credentials*
scope = *directory:software*
6. Uma vez que todos os parâmetros e valores estejam preenchidos, clique no botão *Send*.
7. Selecione e copie o valor retornado no atributo *access_token*.





17.

Listando as organizações cadastradas no Diretório via API

Para acessar a API Organisations no Diretório, você precisará de um token de acesso. Esta seção descreve as etapas necessárias para listar e visualizar os detalhes das organizações cadastradas no Diretório.



ETAPA 1: Obtendo detalhes das organizações

Requisitos

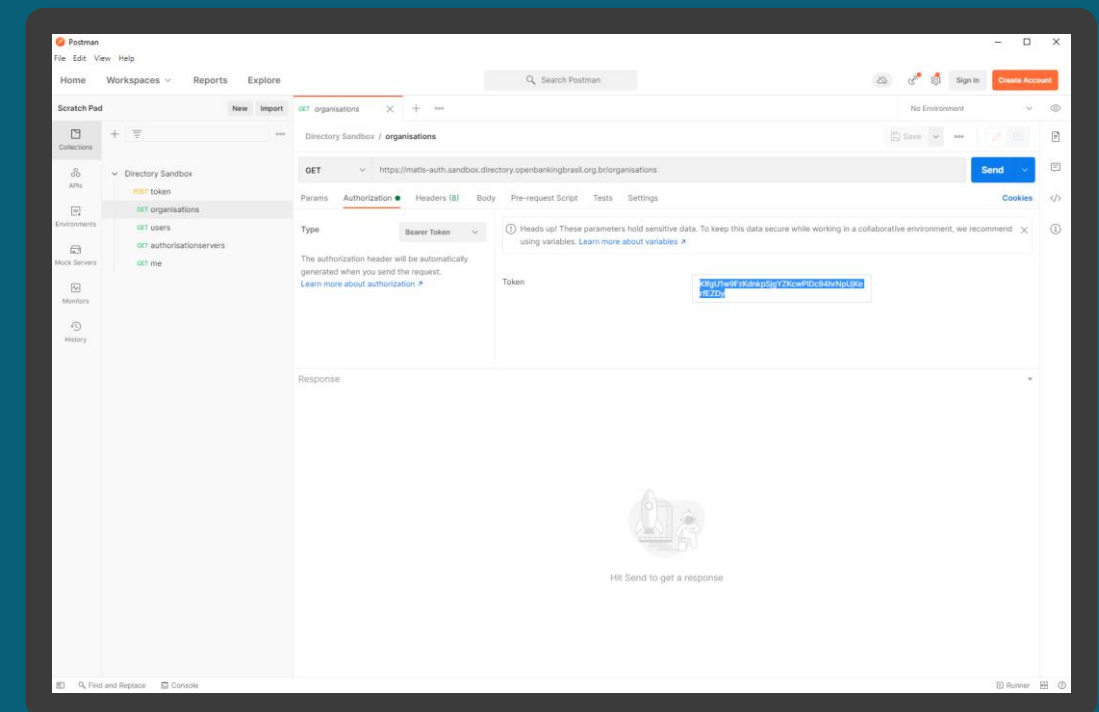
1. Necessário ter um token de acesso. Veja mais detalhes em [Obtendo um token de acesso para acessar as APIs do Diretório](#).
2. Para fins ilustrativos será utilizado o [Postman](#) para acessar as APIs do Diretório do Open Banking. Assim, para adicionar uma nova requisição a uma coleção, abra uma nova aba e salve a partir daí, ou em *Collection* à esquerda do Postman, clique em '...' na coleção e escolha *Add Request*. Você também pode criar uma solicitação clicando no menu *File > New*, e em seguida *Request*.
3. No campo *Enter request URL*, insira um dos valores descritos a seguir de acordo com o ambiente utilizado:

Sandbox

<https://matls-auth.sandbox.directory.openbankingbrasil.org.br/organisations>

Produção

<https://matls-auth.directory.openbankingbrasil.org.br/organisations>



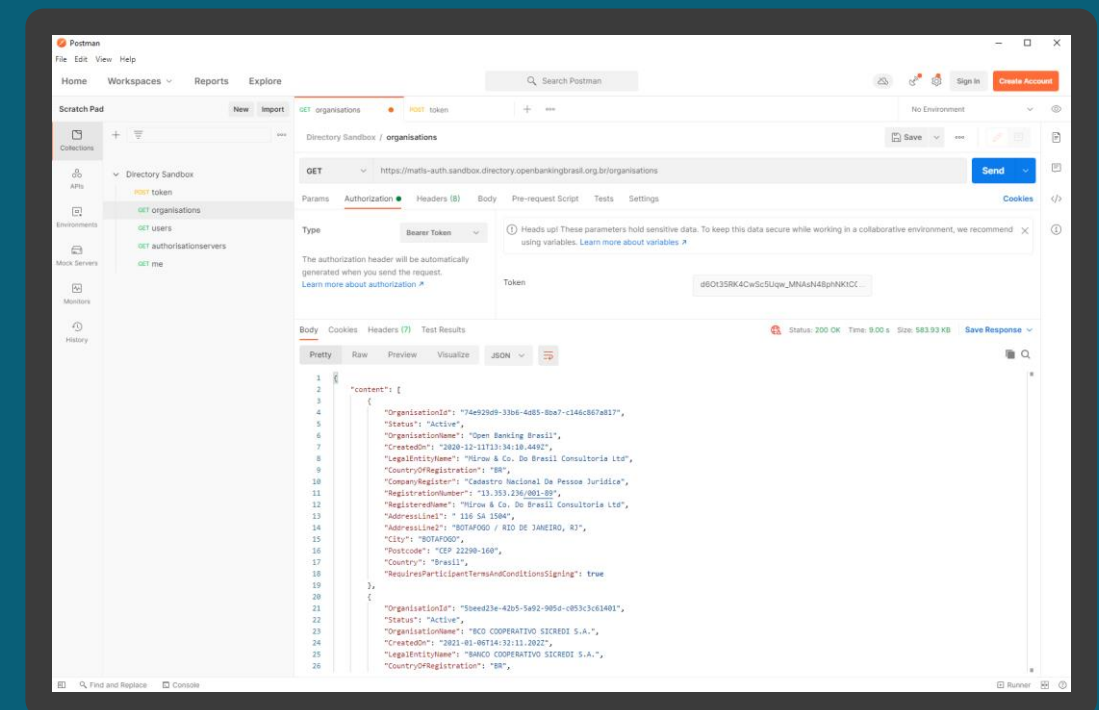


ETAPA 1: Obtendo detalhes das organizações

Requisitos

4. Defina o tipo da operação para GET.
5. Vá para a guia *Authorisation* e na caixa de seleção *Type* selecione a opção *Bearer Token*.
6. Na coluna ao lado, no campo *Token* cole o `access_token` obtido na seção [Obtendo um token de acesso para acessar as APIs do Diretório](#).
7. Uma vez que todos os valores estejam preenchidos, clique no botão *Send*. Você verá a resposta de dados JSON do servidor no painel inferior.

Nota: Para localizar uma organização mãe que pertença a um conglomerado, você poderá percorrer na lista de resposta de dados JSON do servidor, capturando o identificador no atributo *ParentOrganisationReference* das organizações filhas e localizar o mesmo ID na organização cujo o atributo *RegistrationId* contenha este mesmo valor.





18.

Listando os servidores de autorização de uma organização via API

Aqui apresentamos os passos para listar os servidores de autorização de uma organização.



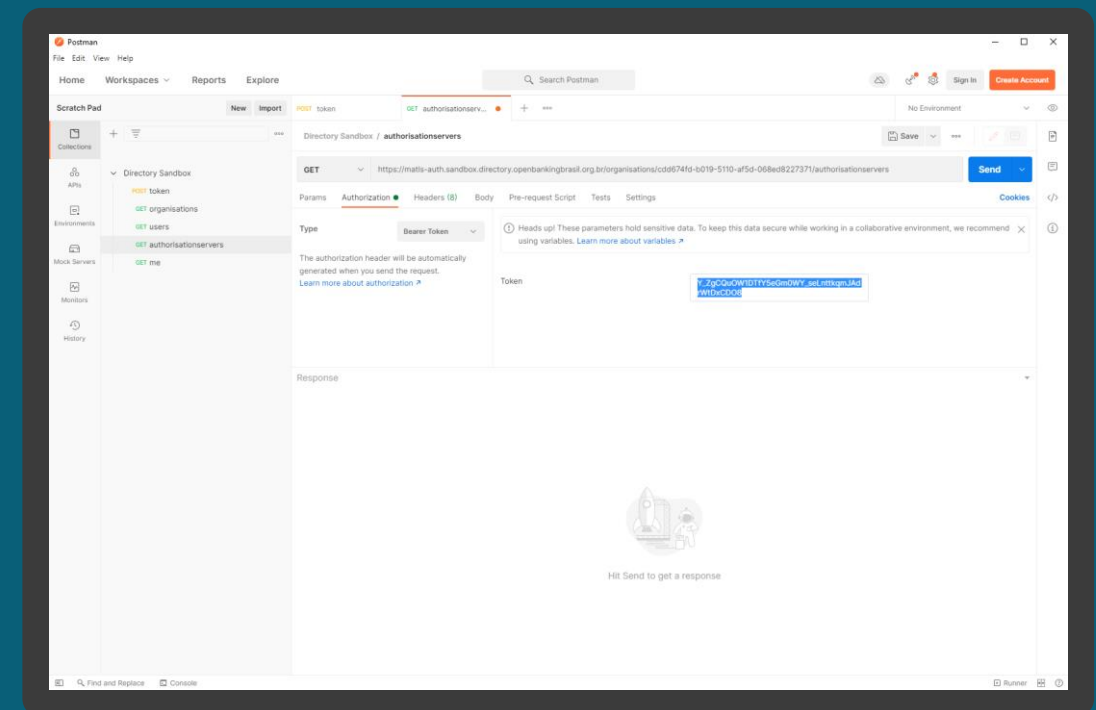
ETAPA 1: Listando os servidores de autorização

Requisitos

1. Necessário ter um token de acesso. Veja mais detalhes em [Obtendo um token de acesso para acessar as APIs do Diretório](#).
2. Necessário ter realizado os passos da sessão [Listando as organizações cadastradas no Diretório via API](#).
3. Para fins ilustrativos será utilizado o [Postman](#) para acessar as APIs do Diretório do Open Banking. Assim, para adicionar uma nova requisição a uma coleção, abra uma nova aba e salve a partir daí, ou em *Collection* à esquerda do Postman, clique em '...' na coleção e escolha *Add Request*. Você também pode criar uma solicitação clicando no menu *File > New*, e em seguida *Request*.
4. No campo *Enter request URL*, insira um dos valores descritos a seguir de acordo com o ambiente utilizado:

Sandbox

https://matls-auth.sandbox.directory.openbankingbrasil.org.br/organisations/<organisation_id>/authorisationervers





ETAPA 1: Listando os servidores de autorização

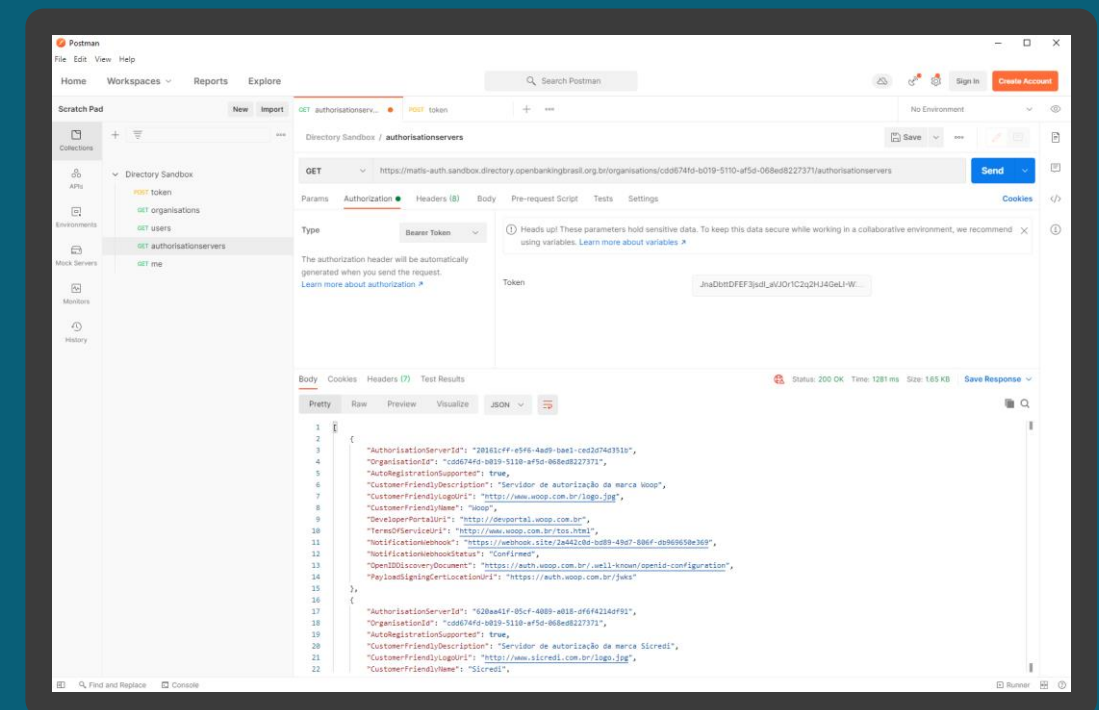
Requisitos

Produção

https://matls-auth.directory.openbankingbrasil.org.br/organisations/<organisation_id>/authorisationservers

5. Defina o tipo da operação para GET.
6. Vá para a guia *Authorisation* e na caixa de seleção *Type* selecione a opção *Bearer Token*.
7. Na coluna ao lado, no campo *Token* cole o `access_token` obtido na seção [Obtendo um token de acesso para acessar as APIs do Diretório](#).
8. Uma vez que todos os valores estejam preenchidos, clique no botão *Send*. Você verá a resposta de dados JSON do servidor no painel inferior.

Nota: Na resposta de dados JSON do servidor o atributo *CustomerFriendlyName* contém o valor da marca e o *CustomerFriendlyLogoUri* o logotipo vinculado a marca.





ETAPA 1: Listando os servidores de autorização

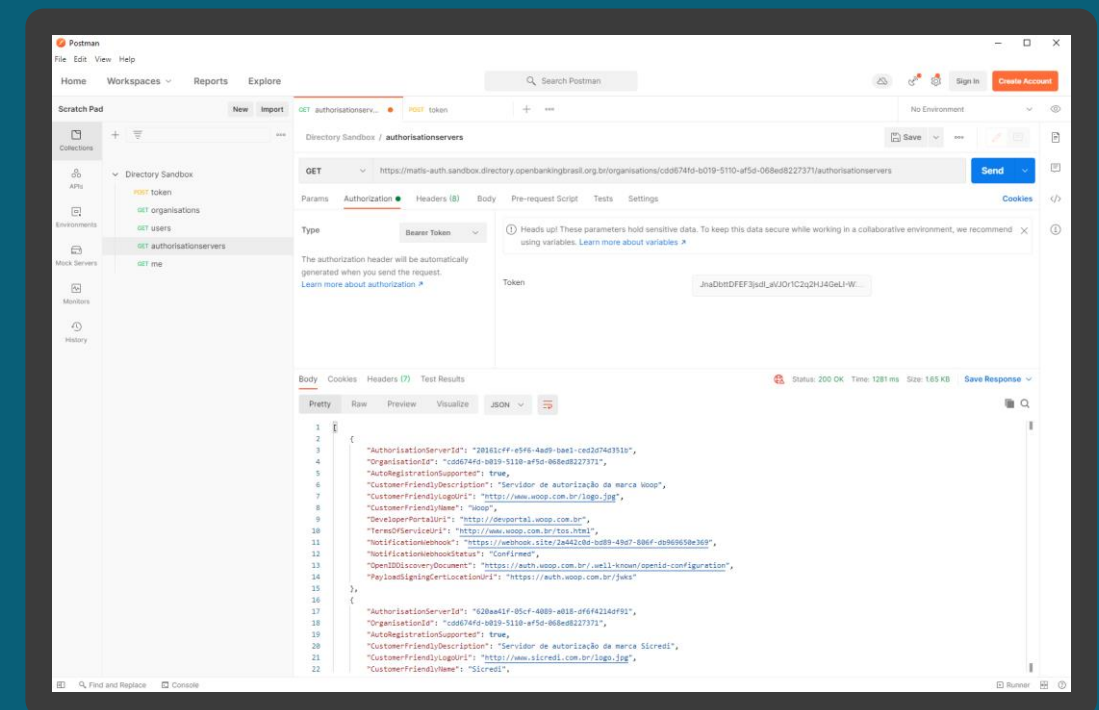
Requisitos

Produção

https://matls-auth.directory.openbankingbrasil.org.br/organisations/<organisation_id>/authorisationservers

5. Defina o tipo da operação para GET.
6. Vá para a guia *Authorisation* e na caixa de seleção *Type* selecione a opção *Bearer Token*.
7. Na coluna ao lado, no campo *Token* cole o `access_token` obtido na seção [Obtendo um token de acesso para acessar as APIs do Diretório](#).
8. Uma vez que todos os valores estejam preenchidos, clique no botão *Send*. Você verá a resposta de dados JSON do servidor no painel inferior.

Nota: Na resposta de dados JSON do servidor o atributo *CustomerFriendlyName* contém o valor da marca e o *CustomerFriendlyLogoUri* o logotipo vinculado a marca.





19.

Obtendo um Software Statement via API

Aqui apresentamos os passos para obter um Software Statement (SS) no Diretório via API.



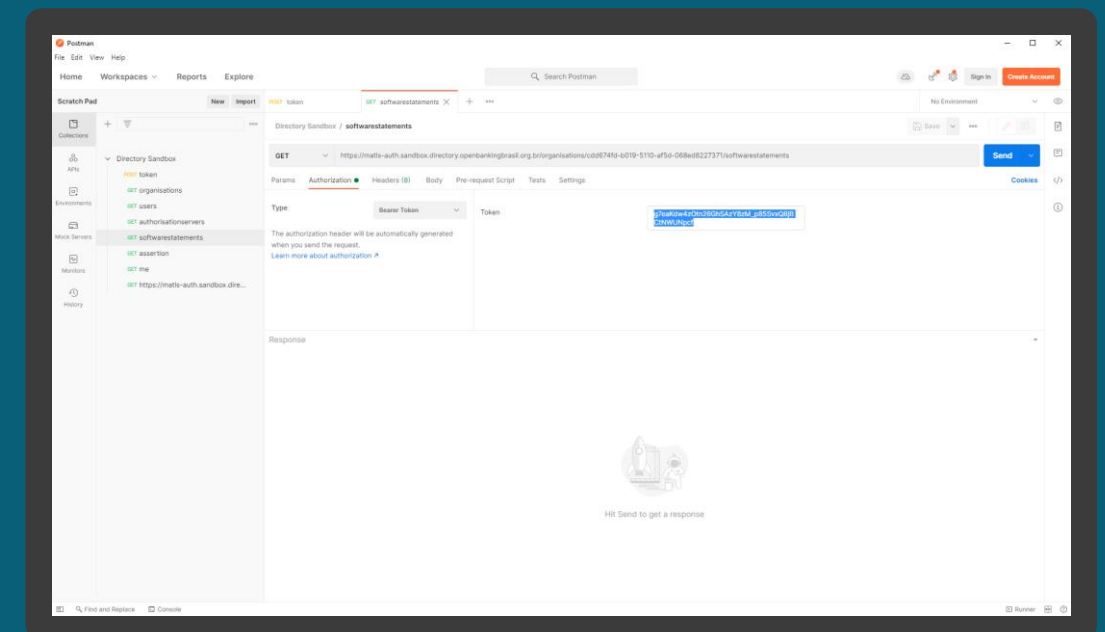
ETAPA 1: Obtendo um SS no Diretório via API

Requisitos

1. Necessário ter um token de acesso. Veja mais detalhes em [Obtendo um token de acesso para acessar as APIs do Diretório](#).
2. Necessário ter realizado os passos da sessão [Listando as organizações cadastradas no Diretório via API](#).
3. Para fins ilustrativos será utilizado o [Postman](#) para acessar as APIs do Diretório do Open Banking. Assim, para adicionar uma nova requisição a uma coleção, abra uma nova aba e salve a partir daí, ou em *Collection* à esquerda do Postman, clique em '...' na coleção e escolha *Add Request*. Você também pode criar uma solicitação clicando no menu *File > New*, e em seguida *Request*.
4. No campo *Enter request URL*, insira um dos valores descritos a seguir de acordo com o ambiente utilizado:

Sandbox

https://matls-auth.sandbox.directory.openbankingbrasil.org.br/organisations/<organisation_id>/softwarestatements





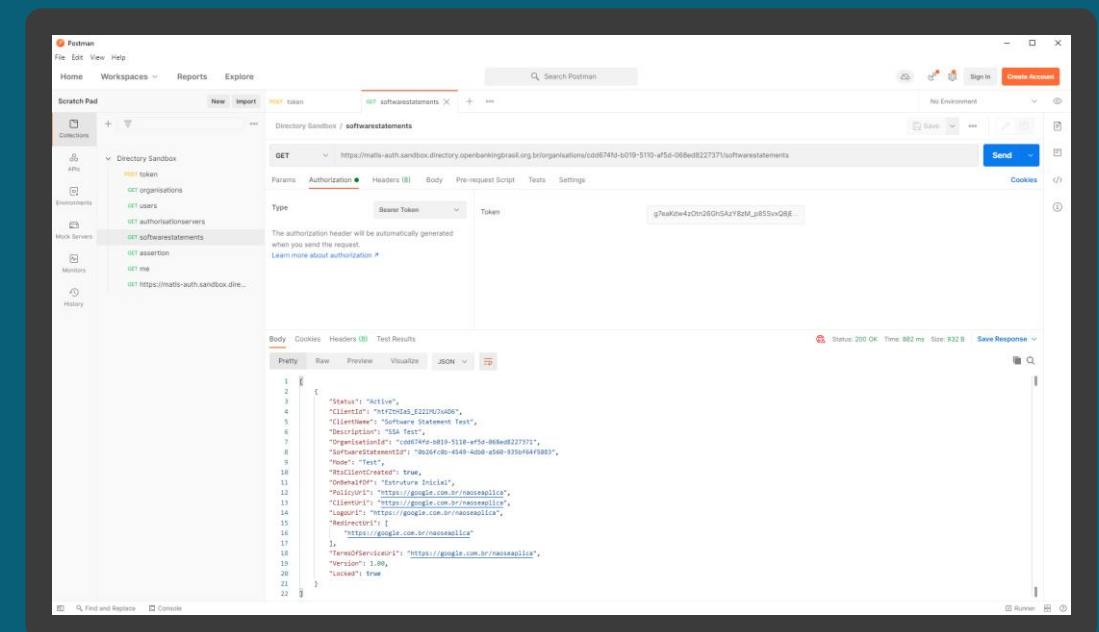
ETAPA 1: Obtendo um SS no Diretório via API

Requisitos

Produção

https://matls-auth.directory.openbankingbrasil.org.br/organisations/<organisation_id>/softwarestatements

5. Defina o tipo da operação para GET.
6. Vá para a guia *Authorisation* e na caixa de seleção *Type* selecione a opção *Bearer Token*.
7. Na coluna ao lado, no campo *Token* cole o `access_token` obtido na seção [Obtendo um token de acesso para acessar as APIs do Diretório](#).
8. Uma vez que todos os valores estejam preenchidos, clique no botão *Send*. Você verá a resposta de dados JSON do servidor no painel inferior.





20.

Obtendo um Software Statement Assertion via API

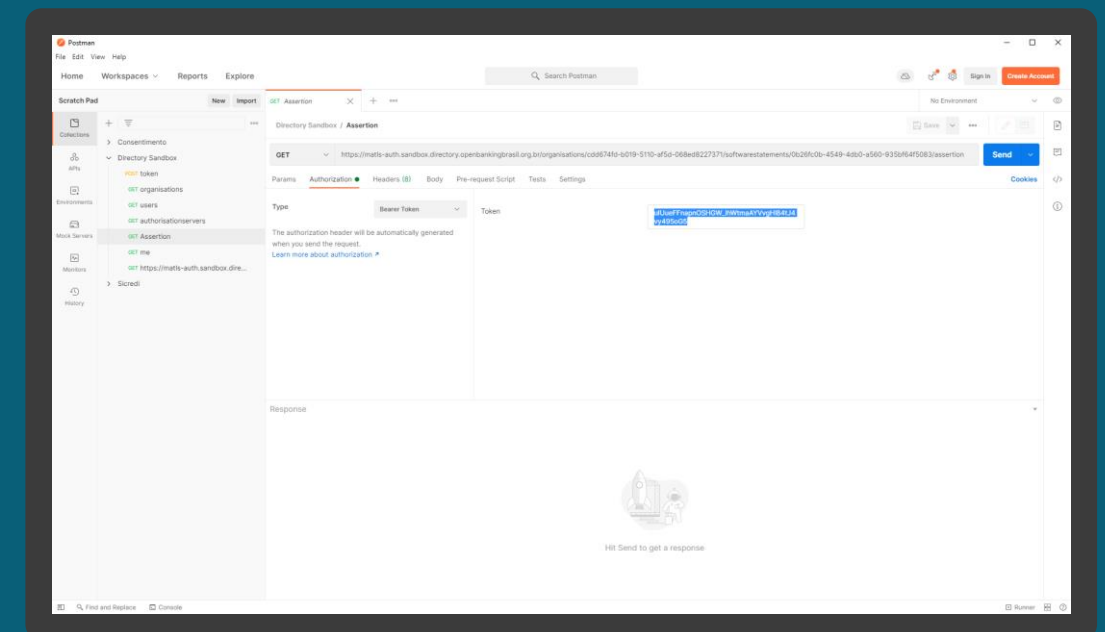
Aqui apresentamos os passos para obter um Software Statement Assertion (SSA) no Diretório via API.



ETAPA 1: Obtendo um SSA do Diretório via API

Requisitos

1. Necessário ter um token de acesso. Veja mais detalhes em [Obtendo um token de acesso para acessar as APIs do Diretório](#).
2. Necessário ter realizado os passos da sessão [Listando as organizações cadastradas no Diretório via API](#).
3. Necessário ter realizado os passos da sessão [Obtendo um Software Statement via API](#).
4. Para fins ilustrativos será utilizado o [Postman](#) para acessar as APIs do Diretório do Open Banking. Assim, para adicionar uma nova requisição a uma coleção, abra uma nova aba e salve a partir daí, ou em *Collection* à esquerda do Postman, clique em '...' na coleção e escolha *Add Request*. Você também pode criar uma solicitação clicando no menu *File > New*, e em seguida *Request*.
5. No campo *Enter request URL*, insira um dos valores descritos a seguir de acordo com o ambiente utilizado:





ETAPA 1: Obtendo um SSA do Diretório via API

Requisitos

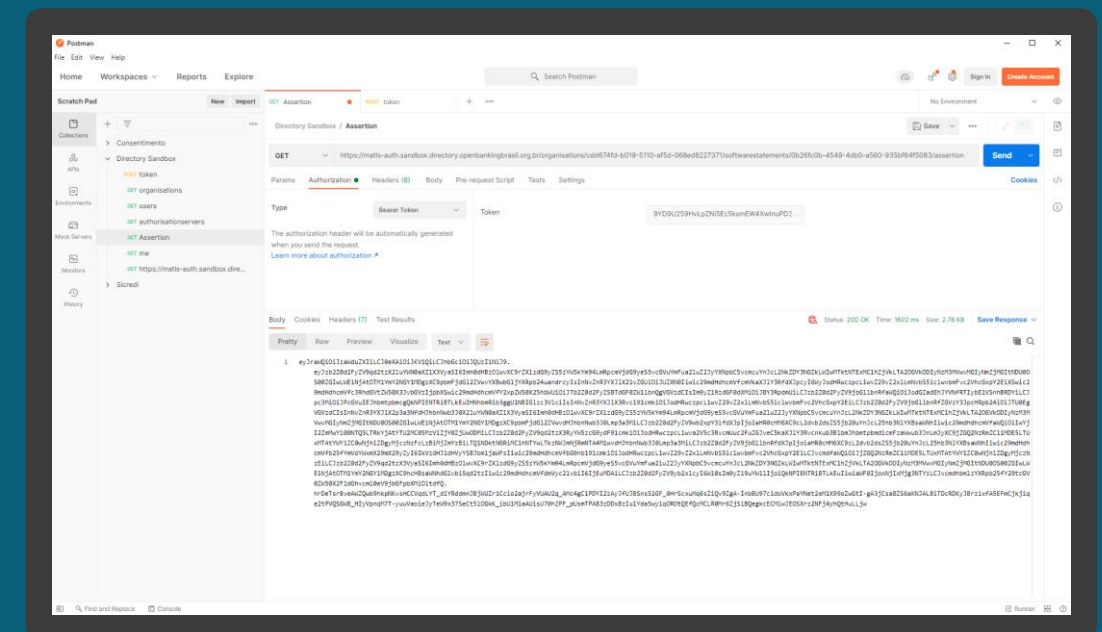
Sandbox

https://matls-auth.sandbox.directory.openbankingbrasil.org.br/organisations/<organisation_id>/softwarestatements/<software_id>/assertion

Produção

https://matls-auth.directory.openbankingbrasil.org.br/organisations/<organisation_id>/softwarestatements/<software_id>/assertion

6. Defina o tipo da operação para GET.
7. Vá para a guia *Authorisation* e na caixa de seleção *Type* selecione a opção *Bearer Token*.
8. Na coluna ao lado, no campo *Token* cole o *access_token* obtido na seção [Obtendo um token de acesso para acessar as APIs do Diretório](#).
9. Uma vez que todos os valores estejam preenchidos, clique no botão *Send*. Você verá a resposta de dados JSON do servidor no painel inferior.





21.

Como obter suporte ao Diretório

Aqui apresentamos as formas de contato para suporte ao Diretório Central.



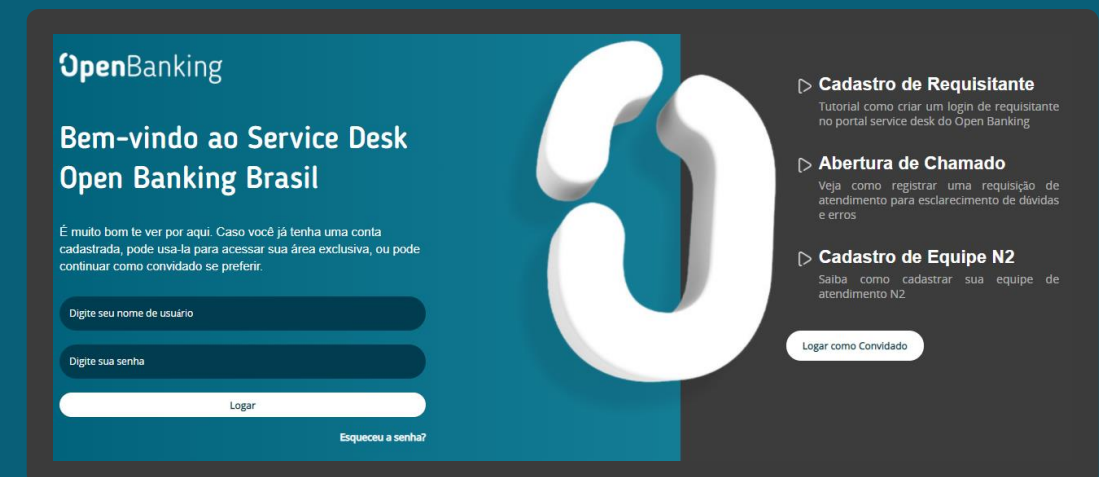
Service Desk

Todas as consultas, problemas ou solicitações de suporte precisam ser roteados por meio do Service Desk.

O Service Desk do Open Banking Brasil pode ser acessado pelo endereço:

<https://servicedesk.openbankingbrasil.org.br/>

É possível abrir chamados de Solicitação de Informações, Melhorias e incidentes de indisponibilidade ou problemas de performance.





22.

Anexos



Anexos

Modelos de Segurança



MODELO DE SEGURANÇA

Poderes dos Usuários no Diretório

	Can Access Directory	Can Edit Org Contacts	Can Add Roles and Domain Claims	Can Issue/Sign TnCs	Can Add S.S.	Can Add/Manage A.S.	Can Edit ICP-BR Certs	Can Add Org Admin	Can Add Primary Technical Contact	Can Add Secondary Technical Contact	Can Add Primary Business Contact	Can Add Secondary Business Contact	Can Add Primary Service Desk Contact	Can Add Secondary Service Desk Contact	Can Add Primary Dispute Contact	Can Add Secondary Dispute Contact	Can Add Primary Portal Contact	Can Add Secondary Portal Contact	Can Add Primary Centralized Platform	Can Add Secondary Centralized Platform
Public	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No
Global Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Org Admin	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Primary Technical Contact	Yes	No	No	No	Yes	No	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Secondary Technical Contact	Yes	No	No	No	Yes	No	Yes	No	No	No	No	No	No	No	No	No	No	No	No	No
Primary Business Contact	Yes	No	No	No	Yes	No	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Secondary Business Contact	Yes	No	No	No	Yes	No	Yes	No	No	No	No	No	No	No	No	No	No	No	No	No
Primary Service Desk Contact	Yes	No	No	No	No	No	No	No	No	No	No	No	No	Yes	No	No	No	No	No	No
Secondary Service Desk Contact	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No
Primary Dispute Contact	Yes	No	No	No	No	No	No	No	No	No	No	No	No	No	No	Yes	No	No	No	No
Secondary Dispute Contact	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No
Primary Portal Contact	Yes	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	Yes	No	No
Secondary Portal Contact	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No
Primary Centralized Platform Contact	Yes	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	Yes
Secondary Centralized Platform Contact	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No



Anexos

Recomendações para receptores



Recomendações para busca Identifica Marca

Complemento ao Guia de Experiencia para Receptores de Dados

Exibir a(s) marca(s) em função do nome da mesma (Marca do Authorisation Server) e da literal que o cliente informou.

Caso sejam identificados mais de uma marca de mesmo nome, exibir uma única vez para o cliente.

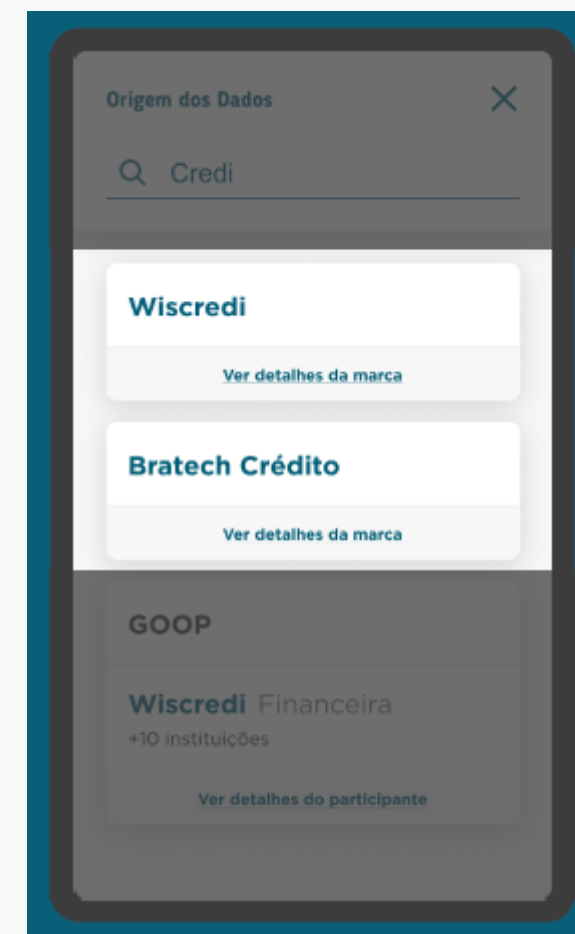
Validar se a marca/Authorisation Servers possui os recursos (família de API's) necessários para a jornada.

Em “ver detalhes da marca” exibir todas as organizações que estão relacionadas a ela:

- Se a marca estiver em mais do que uma organização, exibir todas as organizações que a mesma está cadastrada;
- Organização que é hierarquicamente inferior a organização (mãe) que a marca está cadastrada, desde que a mesma (filha) não possua uma marca cadastrada para ela.

Para saber as instituições hierarquicamente inferiores e necessário utilizar o campo parente. No mesmo será indicado o CNPJ da instituição mãe, se a mesma for uma filha.

Se for mãe, terá o campo sem dado.





Recomendações para busca Identifica Marca

Complemento ao Guia de Experiencia para Receptores de Dados

Exibir a(s) marca(s) em função do nome da mesma (Marca do Authorisation Server) e da literal que o cliente informou.

Caso sejam identificados mais de uma marca de mesmo nome, exibir uma única vez para o cliente.

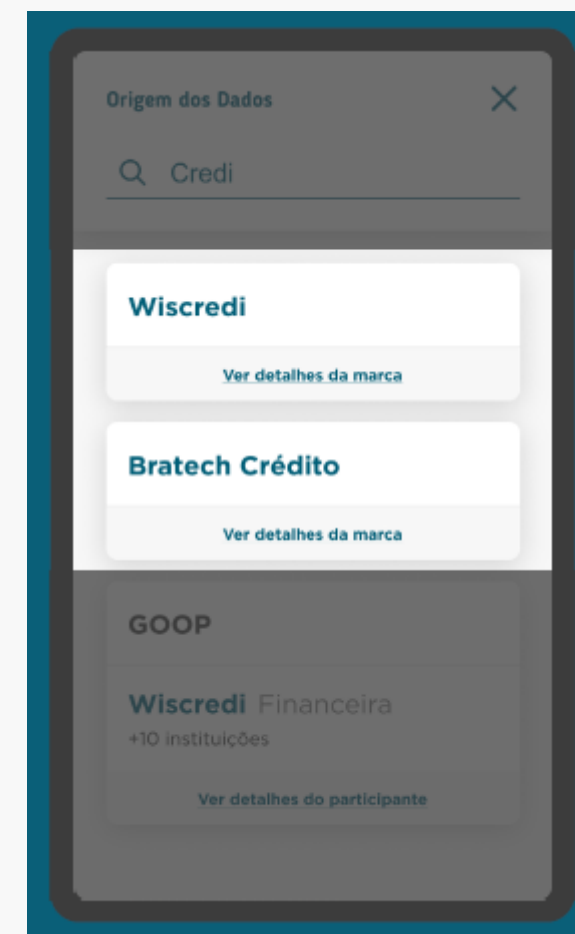
Validar se a Authorisation Servers / marca possui os recursos (família de API's) necessários para a jornada.

Em “ver detalhes da marca” exibir todas as organizações que estão relacionadas a ela:

- Se a marca estiver em mais do que uma organização, exibir todas as organizações que a mesma está cadastrada;
- Organização que é hierarquicamente inferior a organização (mãe) que a marca está cadastrada, desde que a mesma (filha) não possua uma marca cadastrada para ela.

Para saber as instituições hierarquicamente inferiores e necessário utilizar o campo parente. No mesmo será indicado o CNPJ da instituição mãe, se a mesma for uma filha.

Se for mãe, terá o campo sem dado.





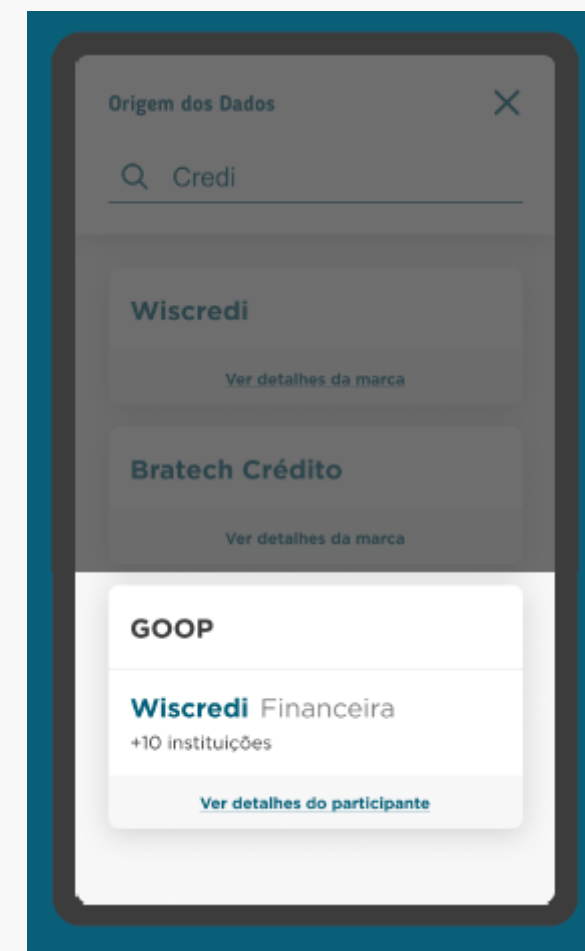
Recomendações para busca Identifica Instituição

Complemento ao Guia de Experiencia para Receptores de Dados

Exibir a(s) marca(s) em função do nome da mesma (Marca do Authorisation Server) e da literal que o cliente informou.

Exibir a(s) instituição(ões) em funções do nome da organização e da literal que o cliente informou.

Aplicar a mesma regra utilizada para exibir as instituições de uma marca para demonstrar quantas instituições estão associadas a marca retornada, quando a busca identificar uma instituição.





Recomendações para busca Identifica Instituição

Complemento ao Guia de Experiencia para Receptores de Dados

No detalhamento da marca, exibir a marca informada no
Authorisation Server

A descrição da marca cadastrada no Authorisation Server.

E para a instituições que participam da marca, aplicar a mesma regra
utilizada para exibir as instituições de uma marca.

Maiores informações:

<https://github.com/OpenBanking-Brasil/specs-seguranca/blob/main/aspsp-user-guide-ptbr.md>

<https://github.com/OpenBanking-Brasil/specs-seguranca/blob/main/tpp-user-guide-ptbr.md>

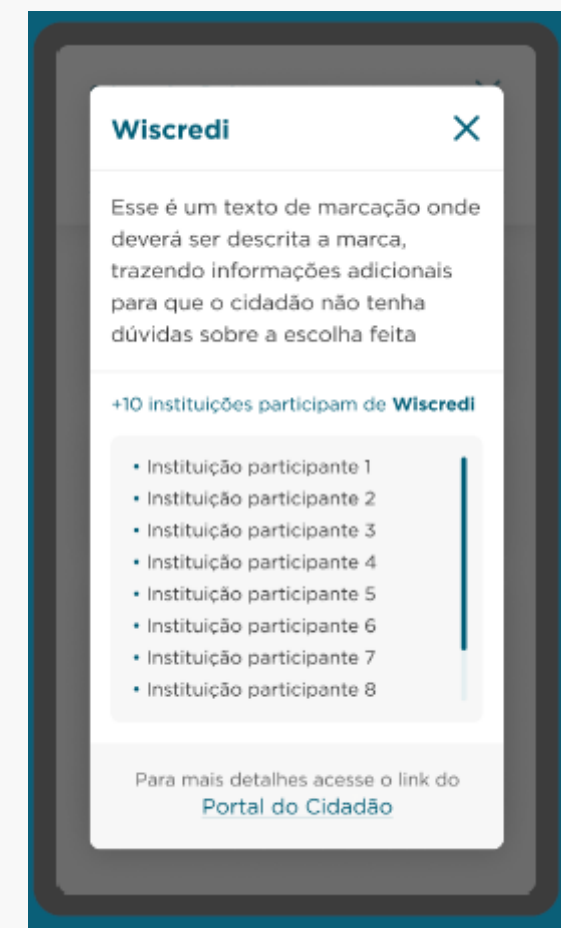




Tabela da dados utilizado na recomendação

Organização

Dado	UI Diretório	API
Nome	LEGAL NAME (ING) NOME LEGAL (PT)	LegalEntityName
CNPJ	REGISTRATION NUMBER-CNPJ (ING) NÚMERO DE REGISTRO – CNPJ (PT)	RegistrationNumber
Mãe	PARENT ORGANISATION REFERENCE ID (ING) NÚMERO DE REGISTRO DA ORGANIZAÇÃO MÃE – CNPJ (PT)	ParentOrganisationReference



Tabela da dados utilizado na recomendação

Authorisation Server

Dado	UI Diretório	API
Marca	CUSTOMER FRIENDLY SERVER NAME (ING) NOME DO SERVIDOR (PT)	CustomerFriendlyName
Descrição	DESCRIPTION (ING) DESCRIÇÃO (PT)	CustomerFriendlyDescription



Anexos

Alterações da versão



ALTERAÇÕES DA VERSÃO

- Adição: foi adicionado um novo detalhamento apresentando os [Tipos de Usuários](#).
- Adição: foi adicionado no rodapé do slide [Cadastramento de Conglomerado](#) uma nota que caso a organização faça parte de um conglomerado é fundamental referenciar as organizações filhas com a organização mãe.
- Adição: foi adicionada uma nova seção [Cadastrando Contatos de Notificação](#).
- Adição: foi adicionada uma nova seção [Cadastrando reivindicações de domínio de autoridade](#).
- Adição: foi adicionada uma nova seção [Cadastrando reivindicações de autoridade](#).
- Adição: foi adicionada uma nova seção [Criando uma nova reivindicação de autoridade de software](#).
- Alteração: a seção Criando uma solicitação de Assinatura de Certificado (CSR) em Sandbox foi ajustada para [Criando certificados de transporte e assinatura em Sandbox](#).



ALTERAÇÕES DA VERSÃO

- Adição: foi adicionado a seção [Carregando certificados emitidos por autoridade de certificação em Produção](#).
- Adição: foi adicionado a seção [Modelo de Segurança – Poderes dos Usuários no Diretório](#).
- Alteração: campo "Description" no cadastro do Authorisation Server agora é obrigatório, para maiores detalhes [Cadastrando um Authorisation Server](#).

Atualização da versão 02/07/2021

- Alteração: foi adicionado recomendações e casos de uso para exemplificar o [cadastramento de marcas](#).
- Alteração: foi alterado o detalhamento do campo “Descrição” do [Authorisation Server](#).
- Adição: foi adicionado uma descrição do [logotipo](#).
- Adição: foi adicionado a seção [Recomendações para receptores](#) com recomendações para a montagem de telas de experiencia de usuário dado a estrutura de dados do Diretório.



ALTERAÇÕES DA VERSÃO

Atualização da versão 09/07/2021

- Alteração: Foi incluído recomendação para cadastramento de recurso tanto da Fase 1 quanto da Fase 2 em [Cadastrando recursos de uma API](#).
- Alteração: Foi alterado a descrição do campo Customer Friendly Server Name do [Cadastrando um Authorisation Server](#).
- Alteração: Foi alterado a descrição do campo Client Name do [Criando um Software Statements](#).
- Alteração: Adicionado um ponto de atenção em [Obtendo um Software Statements Assertion](#).
- Alteração: Adicionado um ponto de atenção em [Criando certificados de transporte e assinatura em Sandbox](#).

OpenBanking