

# Conformidade Funcional

Acesso a plataforma e criação  
de plano de testes





# CONTEÚDO DO GUIA

## 01.

### Criação de um plano de testes

ETAPA 1: Acessando a plataforma de conformidade

ETAPA 2: Preenchimento do plano de testes

ETAPA 3: Encaminhamento de problemas ou dúvidas

## 02. - Opcional

### Emissão dos certificados de transporte e assinatura no Sandbox do diretório de participantes

ETAPA 1: Registrando um usuário no Diretório Sandbox

ETAPA 2: Acessando uma organização

ETAPA 3: Criando uma nova declaração de software

ETAPA 4: Criando o CSR para os certificados BRCAC e BRSEAL

ETAPA 5: Criando um novo certificado de transporte BRCAC

ETAPA 6: Criando um novo certificado de transporte BRSEAL



01.

# Criação de um plano de testes

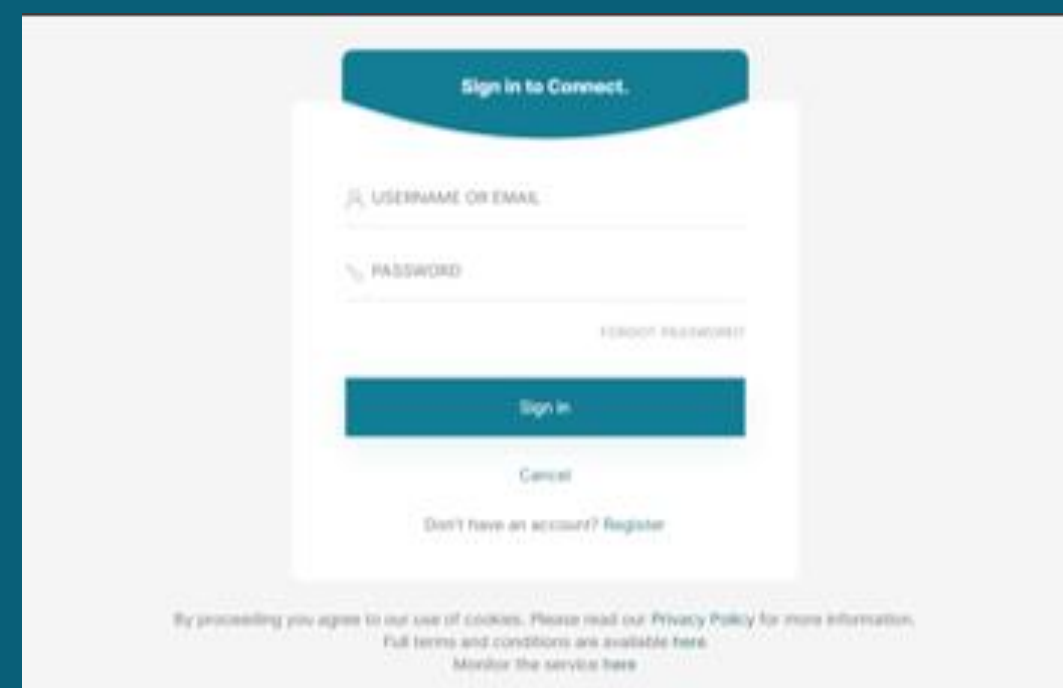
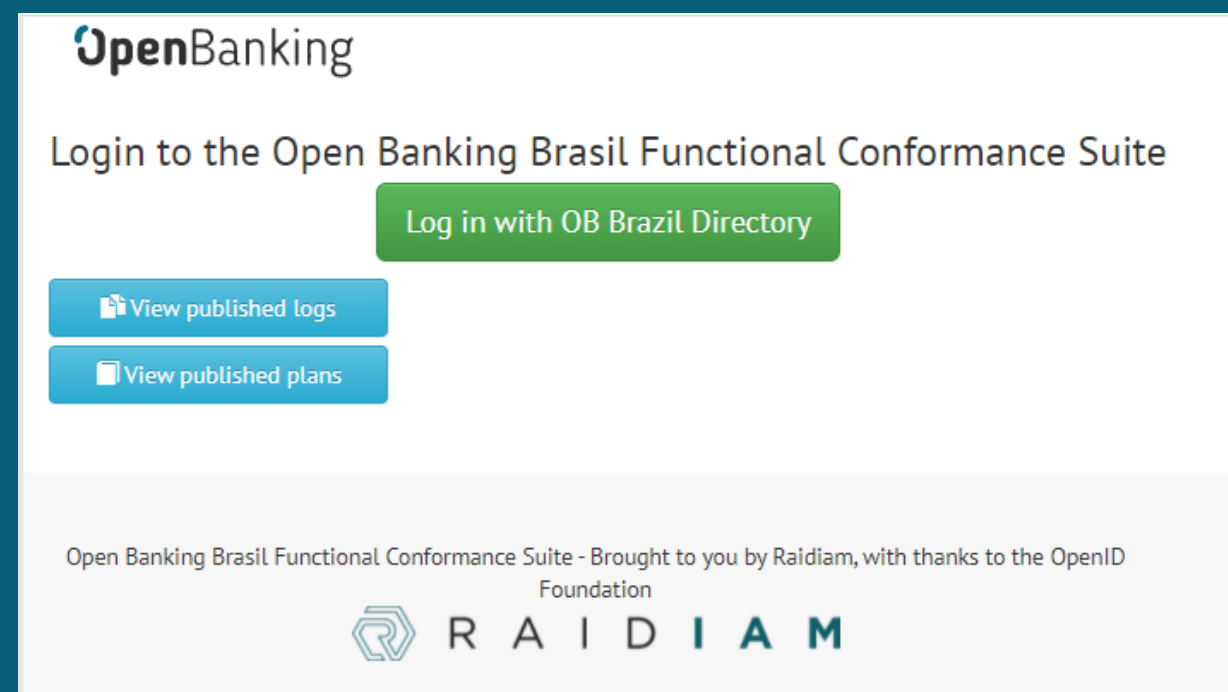
Acesso a plataforma do Open Banking Brasil de conformidade e criação de um novo plano de testes



ETAPA 1: Acessando a plataforma de conformidade

## Requisitos

1. No navegador, digite a URL referente ao motor de conformidade:  
<https://web.conformance.directory.openbankingbrasil.org.br/login.html>
2. Clicar em Log in with OB Brazil Directory
3. Você será redirecionado para a pagina de Log in do Sandbox, preencha a página com as credencias criadas na etapa anterior





ETAPA 2: Preenchimento do plano de testes

## Requisitos

1. Após a conexão clicar em “Create a new test plan”

1

 Create a new test plan

 View all available test logs

 View published test logs

 View all available test plans

 View published test plans

 View API Documentation



ETAPA 2: Preenchimento do plano de testes

## Requisitos

- 2. Test Plan:** Selecionar alguns dos testes disponibilizados no menu Open Banking Brasil Functional Tests
- 3. Client Authentication Type:** Selecionar o tipo de autenticação de cliente compatível com seu software
- 2. Request Object Method:** O método a ser usado para passar o objeto de solicitação ao servidor de autorização. Selecione 'by\_value' a menos que você saiba que seu servidor suporta o endpoint de 'solicitação de autorização enviada' ('PAR') conforme definido aqui:  
<https://tools.ietf.org/html/draft-ietf-oauth-par>
- 3. FAPI Profile:** Selecionar openbanking\_brazil
- 4. Fapi Response Mode:** Selecionar plain\_response

**OpenBanking**

Please see [OpenID Foundation Certification Instructions](#).

Test Plan	Functional tests for accounts API	2
Client Authentication Type	mtls	3
Request Object Method	pushed	4
FAPI Profile	openbanking_brazil	5
FAPI Response Mode	plain_response	6



ETAPA 2: Preenchimento do plano de testes

## Requisitos

- 7. Alias:** Escrever o nome desejado para o plano de testes
- 8. Description:** Escrever a descrição desejada para o plano de testes
- 9. Publish:** Selecionar “No” para não tornar os resultados do teste público para todos
- 10. DiscoveryUrl:** Adicionar o *well-know Discovery endpoint* do servidor de autorização :  
`https:xxx/.well-known/openid-configuration`
- 11. Client\_id:** Adicionar o `client_id` do *software statement*
- 12. Scope:** Escopos a serem usados na solicitação de autorização, por exemplo, ‘openid accounts’
- 13. Jwks:** Inserir o `jwks` relativo ao certificado de assinatura. É possível converter o `.key` em `jwk` utilizando, por exemplo, o seguinte [repositório](#). Válido notar que o `jwk` deve também conter os argumentos `alg` : “PS256” e o argumento `kid`

The screenshot shows the 'Configure Test' interface with the 'JSON' form selected. The 'Test Information' section contains the following fields:

Field	Value	Callout
alias	obbsb	7
description	Trust Platform (Directory) Open Banking	8
publish	No	9
discoveryUrl	https://auth.sandbox.directory.openbank	10
client_id	yQx5B3YzgvVhdnXqelUv	11
scope	openid profile	12
jwks	["keys":[{"alg":"PS256","kty":"RSA","n":"3a0... ioYcUbgfkdYzf5fMWtDBAR7LLoWQwtA... oohqN3xQz0XUvZ7VgpyPkiaU8veYjJIdNARy... dB2ndkr9bA2Q4GGkxryJHrag46vB1FJzHv0KPv6... HgKB1CaXlxGxORvf0RQEpzkr144tjHLfMt1uPT4... zvDv67MC4MCQMN3WpryBwxrakXsXfNY76sku0... u_4pcYZrPYt5Z_2V0kGG-lnGQvD0f4gi8KtSZt1Sv... z5visXOZePk","dp":"RILmuAEu8kn_Vs1w0fMXH5... LSRddGSm0eTzbDYrEEea2YTrFqoWMYH37SB08V	13



## ETAPA 2: Preenchimento do plano de testes

# Requisitos

- 14. Mtls.cert:** Adicionar as informações do certificado de transporte
- 15. Mtls.key:** Adicionar a chave privada do certificado de transporte
- 16. Mtls.ca:** Adicionar os certificados do Root CA do diretório e do issuer CA do diretório. Supondo que seja utilizado o PKI do diretório, este campo pode ser encontrado no apêndice deste documento

TLS certificates for client (used to make MTLs connections)

mtls.cert	-----BEGIN CERTIFICATE----- MIIGRTCCBS2gAwIBAgIUUs0BztW2mZLUuWjGMYMk/WGgswDQYJKoZIhvcNAQEL BQAwcTElMAkGA1UEBhMCQlIxHDAaBgNVBAoTE09wZW4gQmFua2luZyBCcmFzaWw FTATBgNVBAsTDE9wZW4gQmFua2luZzEtMjZzEnMCA1UEAxMkT3BibCYW5raW5nI TkRCT1ggSXNzdWluZyBDQSAtIExMB4XDTEwMDMyOTE5MzYyOTYyOTYyOTYyOTYy MzYyOTYyOTYyOTYyOTYyOTYyOTYyOTYyOTYyOTYyOTYyOTYyOTYyOTYyOTYyOTYy BgNVBAsTJDc0ZTkyOWQ5LTMzYjYyOTYyOTYyOTYyOTYyOTYyOTYyOTYyOTYyOTYy A1UEAxMkMDExMTQ4YzgtNzJmNi00NDkxLTg5YTU0TU0yZmZlZmZlZmZlZmZlZmZl BgkqhkiG9w0BAQEFAAOCAQ8AMIIBCGKCAQEAAuYir88lua2GcMdXbKcQqfmlhBs pyaLkAdZ9EvNH4aDrs3KNSjRlyYX/pjOWwpx1hCiysQokAwler/nolDXSbcT6n L4ROZwi212wLkqVXKzc+9ivQN+QG007QggDaBRJztp72gK3sZQOYFvD3K0V8tAMd -----END CERTIFICATE-----
mtls.key	-----BEGIN PRIVATE KEY----- MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKggggSkAgEAAoIBAQC5givyw5rYyYy 1dspxBcP+uYiEGynJoksp1n0580fhoOuzco1KNEVjghf+mM5bCnHWEKLLKxCiQDA h6v+eiUNdJtxPqcvhE5nCLbXbAuSpVcrNz72K9A35AY7TtCCoNoFEnO2nvaArel A5gW8PcrXY0Ax3woIH52EYO7TIGI68cxMq+b+8QE/GleWdCj3XPr0BZRBfHmH8L u6jJlUxUi2cXYxa3K3rd23TTq6KBzkhfdWQilUvGb+FE7mF+RgZnrZBoluMu086 aSlAE19gpE2Z98KnvithV7xA4/4oatq5bB6EgagoNEM1Jo72o/u9Oif/rSipvGuE U4CZsS9PAgMBAECgEAH74EY0yeVkv3gpeDTw7tbo20rFYxikz464G1RLYLvU8 5DRotdXcshBLP8AxaGINF6tRRprZ18l/8u3RG4GFQ1U48XCucC74al+d9JvEIK2 LbDgVyMcF9QutMtBpnh7lc6YejeEtMuh3Y8F4TcONBtlwUufPeOofXghwFTRak5 mgSkUzU2gCicLZdzyQrftEzqYUqiXyvfb5kVnh2g/sO/0PgIj09RvwFNzBk9p/rh -----END PRIVATE KEY-----
mtls.ca	-----BEGIN CERTIFICATE----- MIIEajCCA1KgAwIBAgIUdIYzEFdw7QJcrySyq6liEwZFTFAwDQYJKoZIhvcNAQEL BQAwazELMAkGA1UEBhMCQlIxHDAaBgNVBAoTE09wZW4gQmFua2luZyBCcmFzaWw FTATBgNVBAsTDE9wZW4gQmFua2luZzEtMjZzEnMCA1UEAxMkT3BibCYW5raW5nI b3QgU0FOREIPWCAAtIExMB4XDTEwMDMyOTE5MzYyOTYyOTYyOTYyOTYyOTYy cTElMAkGA1UEBhMCQlIxHDAaBgNVBAoTE09wZW4gQmFua2luZyBCcmFzaWwxF BgNVBAsTDE9wZW4gQmFua2luZzEtMjZzEnMCA1UEAxMkT3BibCYW5raW5nI TkRCT1ggSXNzdWluZyBDQSAtIExMIIBjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCGK AQEA6fX+272mHX5QAcDaWkVHFwJnDicORNJU3OuNyeuOYhVXJWYdrXe30+cV+P S39faMj/nfem3GfBE7XnObWA/8ksxSfrg1BUBJDge4YBBw+vflI3A0g1fk9wJ3H Glnsv4serRJ/ISJtfsOuRNugX+RrbkT/T0tup4vGd3Kl2sbwUdDjokulNIHANEo DRkOzra+9Wbt71EBld0ZuPZztpaWhm6a53c47QID35ivkCAxiZuHfScrvHo1V -----END CERTIFICATE-----

14

15

16





ETAPA 2: Preenchimento do plano de testes

## Requisitos

17. **resourceUrl:** Especificar a url do recurso que será utilizado para execução dos teste. Por exemplo:  
`https://api.edbank.com.br/open-banking/accounts/v1/accounts`
18. **ConsentUrl:** Especificar a url do do consentimento. Por exemplo:  
`https://api.edbank.com.br/open-banking/consents/v1/consents`
19. **brazilCpf:** O valor 'CPF' a ser usado na solicitação de criação de consentimento.
20. **Create Test Plan:** Finalizar a criação do plano de testes

The screenshot shows a form titled "Resource" with three input fields and a "Create Test Plan" button. The fields are: "resourceUrl" with value "https://api.edbank.com.br/open-banking/accounts/v1/accounts", "consentUrl" with value "https://api.edbank.com.br/open-banking/consents/v1/consents", and "brazilCpf" with value "06098692564". The button is labeled "Create Test Plan".

Resource	
resourceUrl	https://api.edbank.com.br/open-banking/accounts/v1/accounts
consentUrl	https://api.edbank.com.br/open-banking/consents/v1/consents
brazilCpf	06098692564

Create Test Plan



## ETAPA 3: Problemas ou dúvidas

# Requisitos

1. Caso seja reportado algum problema na criação, execução ou interpretação dos testes realizados pedimos que seja aberto um ticket na plataforma de Service Desk do Open Banking:  
<https://servicedesk.openbankingbrasil.org.br>
2. Reforçamos que problemas relativos ao acesso no Sandbox do diretório de participantes devem ser enviados ao e-mail [cadastro@openbankingbr.org](mailto:cadastro@openbankingbr.org)
3. Para a abertura de chamados pedimos que consultem o vídeo:  
<https://youtu.be/bhMOtliGjKc>
4. A plataforma também dispõe de um F.A.Q. com dúvidas relativas ao processo de certificação (acessível após realização do login):  
[https://servicedesk.openbankingbrasil.org.br/KBF AQTree.jsp?&menuFlag=ssp&notAddingIndexJSP=true#\[object%20Object](https://servicedesk.openbankingbrasil.org.br/KBF AQTree.jsp?&menuFlag=ssp&notAddingIndexJSP=true#[object%20Object)

OpenBanking

## Bem-vindo ao Service Desk Open Banking Brasil

É muito bom te ver por aqui. Caso você já tenha uma conta cadastrada, pode usá-la para acessar sua área exclusiva, ou pode continuar como convidado se preferir.

Logar

[Esqueceu a senha?](#)



▷ **Cadastro de Requisitante**  
Tutorial como criar um login de requisitante no portal service desk do Open Banking

▷ **Abertura de Chamado**  
Veja como registrar uma requisição de atendimento para esclarecimento de dúvidas e erros

▷ **Cadastro de Equipe N2**  
Saiba como cadastrar sua equipe de atendimento N2

[Logar como Convidado](#)



02.

# Emissão de certificado de transporte no Sandbox do diretório de participantes

Instruções gerais de como realizar a geração dos certificados de transporte e assinatura BRCAC e BRSEAL para um cliente (Software Statement)



ETAPA 1: Registrando um usuário no Diretório Sandbox

## Requisitos

1. No navegador, digite a URL referente ao ambiente Sandbox

<https://web.sandbox.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." It features two input fields: "USERNAME OR EMAIL" and "PASSWORD". Below the password field is a link for "FORGOT PASSWORD?". A prominent teal "Sign in" button is centered below the fields, with a "Cancel" link underneath it. At the bottom, there is a link that says "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." It includes several input fields: "FIRST NAME" and "FAMILY NAME" (split into two columns), "EMAIL ADDRESS", a phone number field with a dropdown menu showing "+55" and a "PHONE NUMBER" label, "PASSWORD", "CONFIRM PASSWORD", and "NATIONAL ID (CPF)". There is a toggle switch for "Do you possess an e-signature certificate?". A teal "Register" button is positioned below the fields, with a link "Already have an account? Sign in." at the bottom.



# 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	<a href="mailto:Joao.silva@wizcredi.com.br">Joao.silva@wizcredi.com.br</a>
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 1: Registrando um usuário no Diretório Sandbox

## 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 +55000000000000

PHONE NUMBER VERIFICATION CODE

Verify

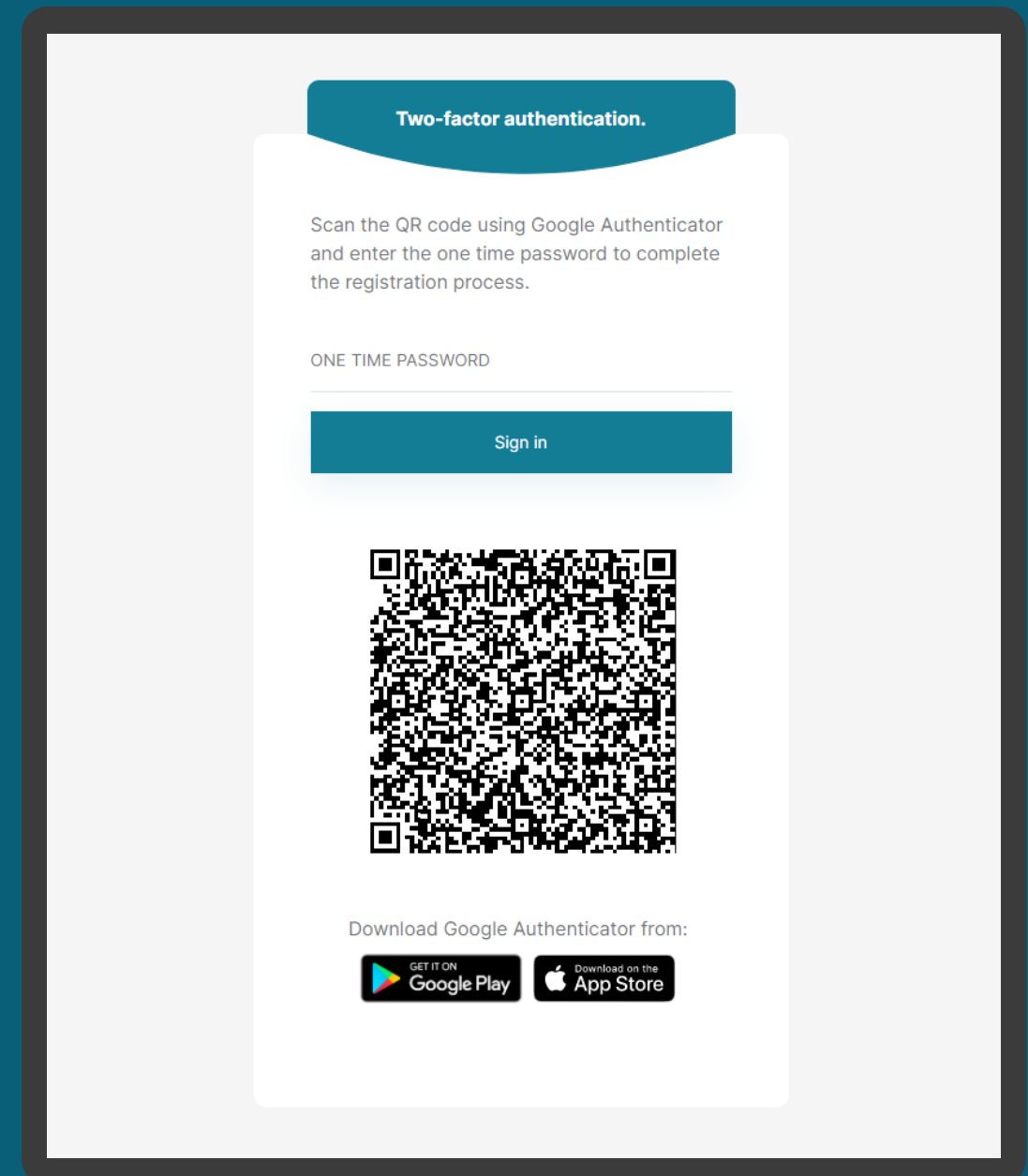
Resend OTP



ETAPA 1: Registrando um usuário no Diretório Sandbox

## Requisitos

5. 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.
6. Digitalize o QR Code que aparece na página e no aplicativo de autenticação, copie e cole a senha de uso único (OTP).
7. Clique no botão *Sign-In*

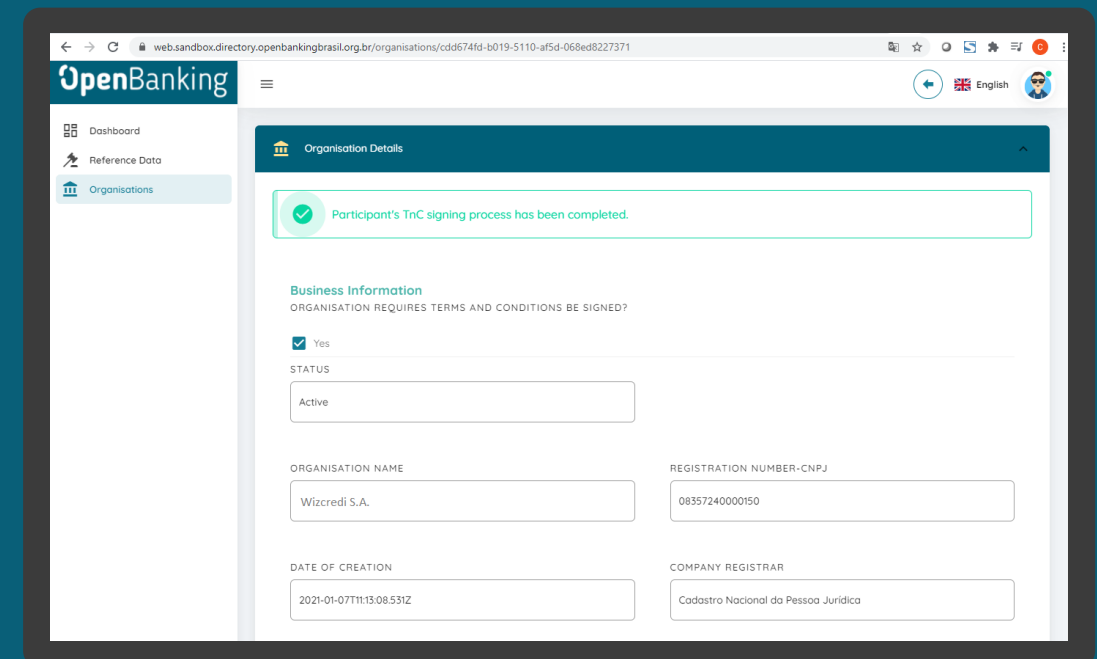
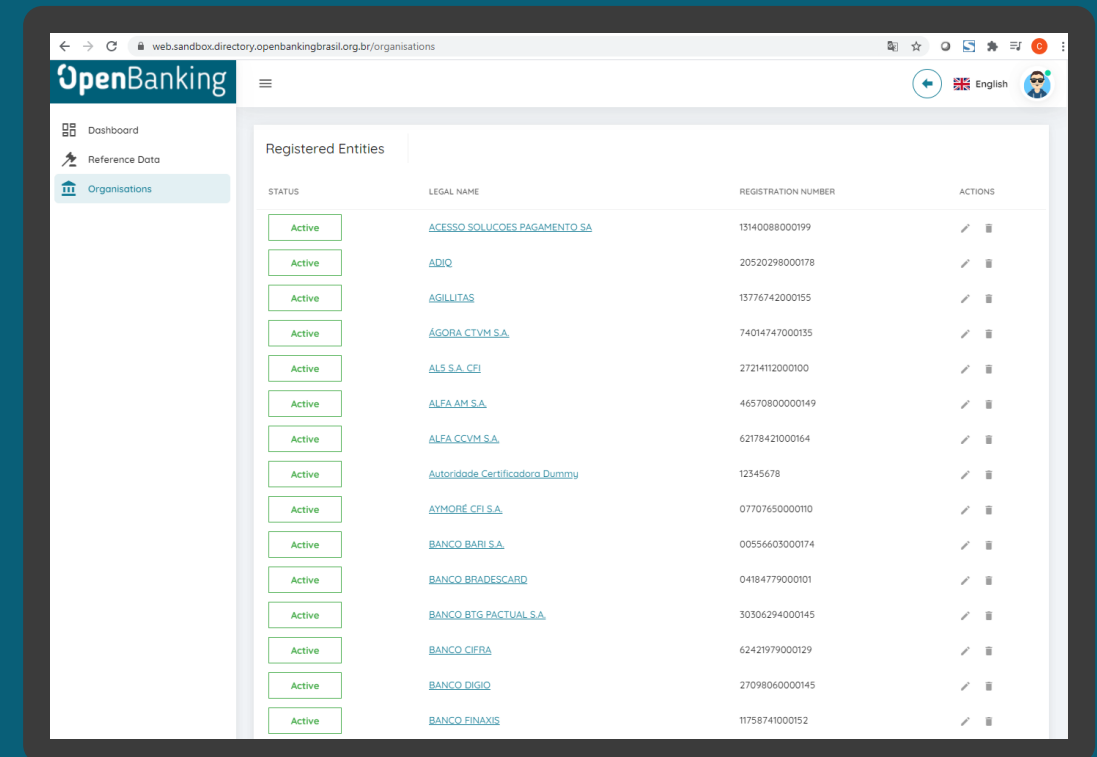




ETAPA 2: Acessando uma organização

## Requisitos

1. No Diretório, localize e selecione a sua organização – É possível utilizar a barra de busca para localizar a instituição
2. Clique no nome da organização para acessá-la



Caso você receba uma mensagem de “Não autorizado” ao tentar acessar a plataforma, você deverá requisitar que o administrador da organização que realizou o cadastro da instituição no Open Banking te adicione como novo administrador ou como contato técnico

Caso a conta do iniciador de cadastro não esteja mais disponível, pedimos que entre em contato conosco pelo e-mail

[cadastro@openbankingbr.org](mailto:cadastro@openbankingbr.org)





ETAPA 3: 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.

The screenshot shows a web form titled "New Software Statement" with a close button (X) in the top right corner. The form is organized into several sections:

- Active:** A checked checkbox.
- Software Statement Details:**
  - MODE\*:** A dropdown menu with the description "The operational status of the software statement".
  - VERSION\*:** A text input field with the description "The software statement's version number".
  - ENVIRONMENT\*:** A text input field with the description "The operational environment of the software statement".
- URIs:**
  - CLIENT NAME\*:** A text input field with the description "The common name of the software statement's client".
  - CLIENT URI\*:** A text input field with the description "The URI to the software statement's client".
  - POLICY URI\*:** A text input field with the description "The URI to the software statement's policy document".
  - LOGO URI\*:** A text input field with the description "The URI to the software statement's branding artefacts".



# 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*		Wizcredi S.A
Client URI*	O site ou URI raiz do recurso	<a href="https://www.wizcredi.com.br/info.html">https://www.wizcredi.com.br/info.html</a>
Policy URI	Deve ser definido como uma sequência de texto que representa uma URI única de política.	<a href="https://www.wizcredi.com.br/policy.html">https://www.wizcredi.com.br/policy.html</a>
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.	<a href="https://www.wizcredi.com.br/logo.svg">https://www.wizcredi.com.br/logo.svg</a>
Redirect URI*	Os URIs de redirecionamento devem ser definidos como uma string de texto que representa uma URI único de redirecionamento.	<a href="https://www.wizcredi.com.br/cb1">https://www.wizcredi.com.br/cb1</a> <a href="https://www.wizcredi.com.br/cb2">https://www.wizcredi.com.br/cb2</a>
Terms of Service URI	Deve ser definido como uma string de texto que representa uma URI única dos Termos de Serviço.	<a href="https://www.wizcredi.com.br/tos.html">https://www.wizcredi.com.br/tos.html</a>
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>

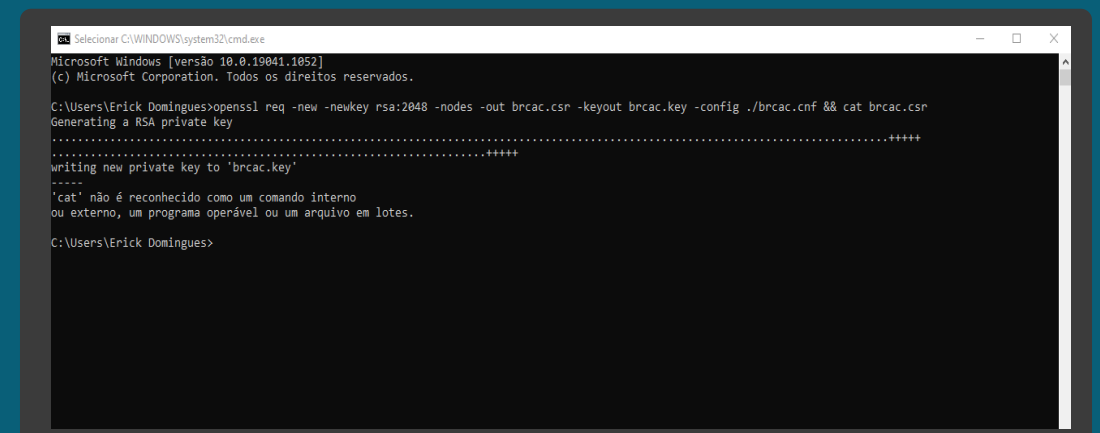
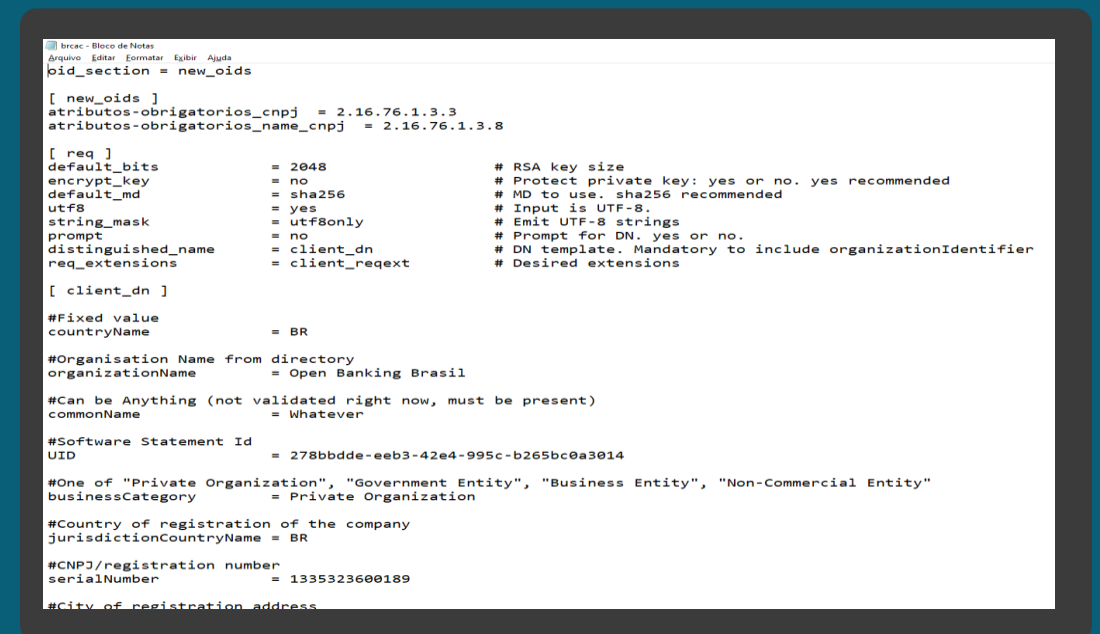
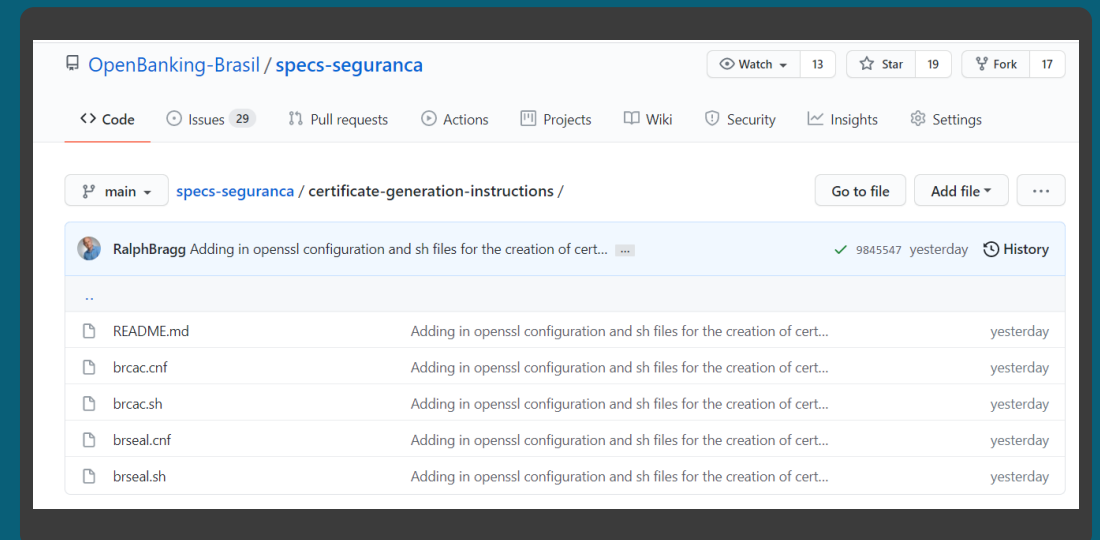
\* Campos obrigatórios.



## ETAPA 4: Criando o CSR para os certificados BRCAC e BRSEAL

# Requisitos

1. Para a próxima etapa será necessária a criação dos *Certificate Signing Request (CSR)* e das chaves privadas (KEY) tanto do certificado de transporte (BRCAC) quanto do certificado de assinatura (BRSEAL) a serem utilizados para o teste
2. Os arquivos de suporte para a geração destes podem ser encontrados em [link](#)
3. Usando sua própria geração de chaves e políticas de gerenciamento, um par de chaves públicas privadas deve ser criado. O exemplo abaixo utiliza o [OpenSSL](#) e apenas para fins ilustrativos
4. Descarregue os quatro arquivos no seu computador
5. Edite ambos os arquivos .cnf de forma que as informações contidas nestes sejam paralelas tanto com a organização quanto com o *Software Statement* recém criado
6. Edite ambos os arquivos .sh para que referenciem o caminho dos arquivos .cnf (./brcac.cnf)
7. Execute os dois arquivos .sh através do prompt de comando para a geração do par CSR/KEY

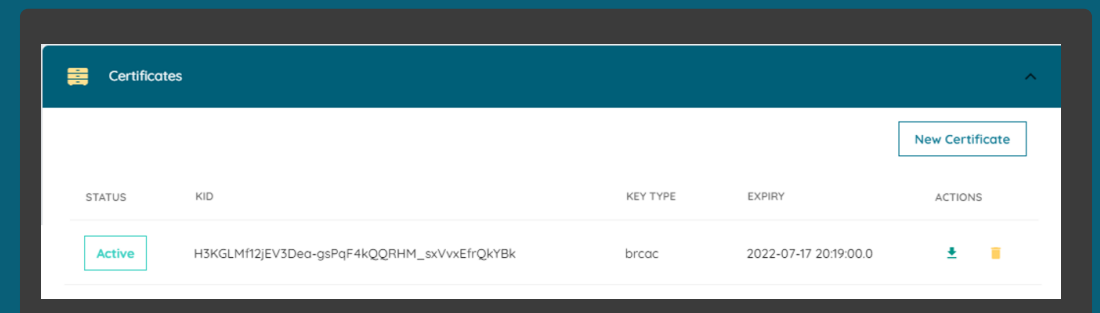
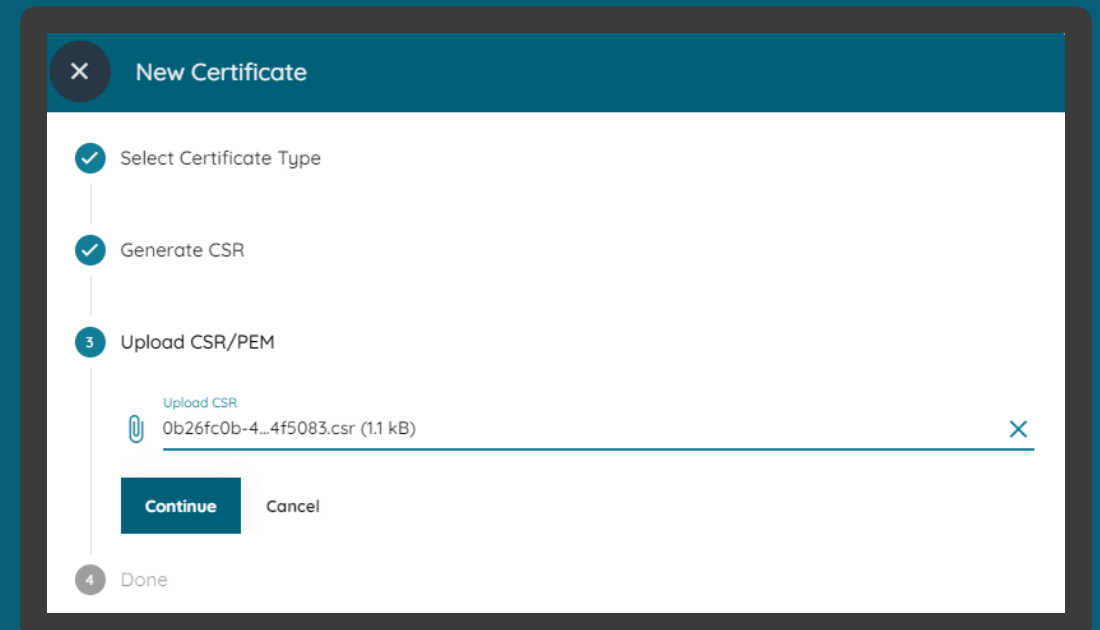
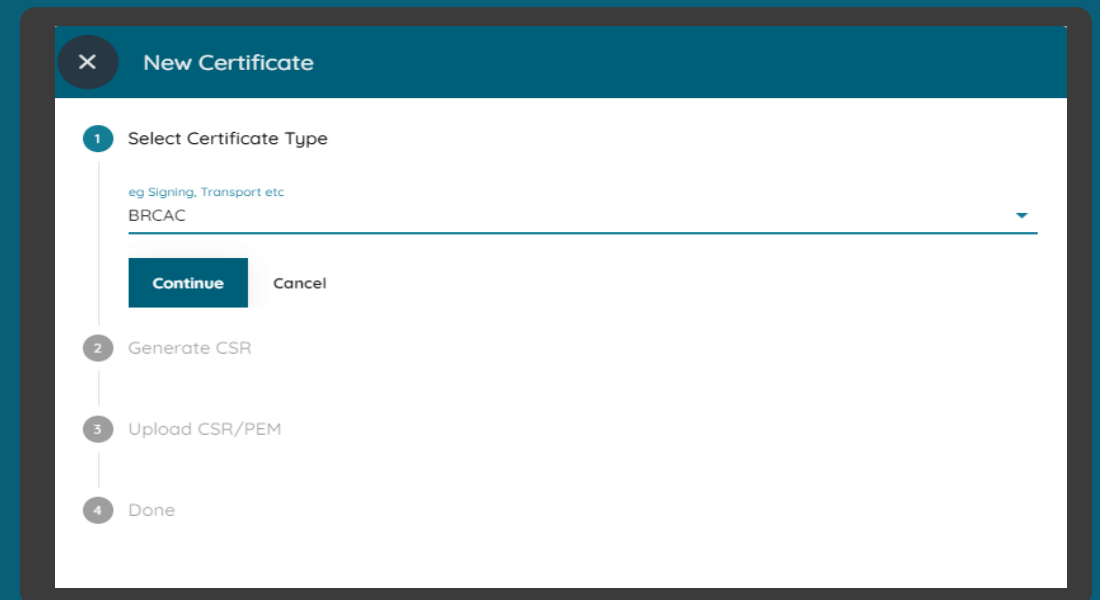




ETAPA 5: Criando um novo certificado de transporte BRCAC

## 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. Vá para a etapa *Upload CSR/PEM* e localize o <arquivo>.csr gerado pela execução do passo anterior e clique no botão *Continue*
7. Na tela anterior de *certificates*, vá até *actions* e clique na seta de *download*. Salve o <arquivo>.pem em uma pasta local





ETAPA 6: Criando um novo certificado de assinatura BRSEAL

## Requisitos

1. No Diretório, selecione a sua organização e vá até a página detalhes da organização.
2. Selecione o menu *Organisation Certificates* e clique em *New Organisation Certificate*
3. Na janela *New Organisation Certificate*, na caixa de seleção *Select Certificate Type* selecione a opção *BRSEAL* e clique no botão *Continue*.
4. Vá para a etapa *Upload CSR/PEM* e localize o <arquivo>.csr gerado pela execução do passo anterior, referente ao certificado BRSEAL, e clique no botão *Continue*
5. Na tela anterior de *certificates*, vá até *actions* e clique na seta de *download*. Salve o <arquivo>.pem em uma pasta local

