

# Guia de certificação de conformidade

Versão 5 - 08/11/2021

## 1. 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 visa auxiliar os profissionais envolvidos no negócio e no desenvolvimento desse serviço, facilitando e esclarecendo dúvidas relacionadas ao processo de teste e certificação de suas APIs. Clique [aqui](#) para uma visão completa do Open Banking Brasil.

O objetivo deste guia é demonstrar de forma prática a execução dos testes necessários para obtenção das certificações pertinentes para a entrada em produção no ecossistema do Open Banking Brasil. Esse guia é complementar a outras documentações disponibilizadas pela governança e não fazem parte do escopo deste, quaisquer detalhamentos relacionados a experiência do usuário/desenvolvedor, definições de segurança e especificação de APIs.

**Disclaimer:** Estão previstos versionamentos contínuos deste guia ao longo dos primeiros meses de implementação do Open Banking no Brasil. O escopo inicial deste guia é a orientação de uso da ferramenta provida pela **Open ID Foundation (OIDF)** (“Motor de Conformidade de Segurança”) para teste e certificação do escopo de segurança e da ferramenta disponibilizada pela Estrutura de Governança para teste e certificação de conformidade de APIs (“Motor de Conformidade Funcional”), enquanto as instruções para uso da Implementação de Referência (“Mock Bank”) serão disponibilizadas em uma versão futura desse guia.

### 1.1 Objetivos e Conceitos Gerais

Para a entrada segura e assertiva no Ecossistema do Open Banking, a Estrutura de Governança irá disponibilizar um conjunto de ferramentas e infraestrutura para suportar o processo de testes e homologação dos produtos e serviços desenvolvidos pelas Instituições Participantes.

Serão disponibilizados ambientes que permitam aos participantes:

- Realizar testes da camada de segurança de suas aplicações e posterior certificação destas aplicações utilizando a estrutura criada e mantida pela **Open ID Foundation** (“Motor de Conformidade de Segurança”);
- Submeter, ainda em tempo de desenvolvimento, suas implementações das APIs do Open Banking a testes automatizados funcionais (“Motor de Conformidade Funcional”); e,
- Acessar implementações de exemplo das APIs do Open Banking que simule uma Instituição Participante de Referência, com implementação completa de cada API (“Implementação de Referência”).

Uma implementação de versão de API do Open Banking só poderá ser registrada no ambiente produtivo do Diretório caso tenha sido certificada nos testes de segurança e conformidade, cujo detalhamento para execução será apresentado nesse guia.

## 1.2 Escopo

Para garantir que as implementações das instituições estão seguindo os padrões conforme as especificações previstas para o Open Banking Brasil, o escopo mínimo dos testes irá abranger aspectos de segurança e também aspectos funcionais: os primeiros objetivarão avaliar se os requisitos não funcionais das APIs, em particular, segurança, estão sendo atendidos por suas implementações, enquanto que os últimos visarão avaliar se as implementações estão aderentes às [especificações](#) das APIs do ambiente.

Dentro do escopo previsto pelos motores de conformidade, destacamos, de maneira não exaustiva, as principais validações executadas:

- Segurança
  - o Perfil FAPI BR
  - o DCR – Dynamic Client Registration
  - o Perfil FAPI BR *Relying Parties*
  - o Perfil DCR BR *Relying Parties* – A ser detalhado em versão posterior do guia
  - o Perfil CIBA BR - A ser detalhado em versão posterior do guia

### Funcionais

- o Estrutura das URLs
- o Cabeçalhos
- o Códigos de Resposta
- o Escopos e Permissões
- o Schema / Estrutura da API

## 1.3 Ferramentas

- **Motor de Conformidade de Segurança / Testes de Segurança / – Foco da versão atual deste Guia**

Ferramenta disponibilizada pela **Open ID Foundation** que implementa o perfil de segurança do Open Banking Brasil. Através desta plataforma é possível a validação de toda camada de segurança das aplicações da Instituição Participante.

- **Motor de Conformidade Funcional / Testes de Conformidade / ‘Conformance Suite’ – Foco da versão atual deste Guia**

Ferramenta disponibilizada pela Estrutura de Governança para realização de testes de conformidade de especificações de API da Instituição Participante.

- **Implementação de Referência / Banco de referência / Banco Modelo / ‘Mock Bank’ – Não detalhado nessa versão do Guia**

## 2. Políticas Gerais

### 2.1 Participantes

A governança do Open Banking Brasil convencionou que todos os participantes, para publicarem suas APIs para o ecossistema (“Transmissores” ou “Detentores de Conta”), devem possuir as devidas certificações que seus sistemas estão seguindo os padrões criados. Estas certificações estão divididas em certificações de segurança e certificações funcionais.

As certificações de segurança englobam dois aspectos: O perfil FAPI e o processo de DCR. A certificação de segurança é obrigatória para os participantes que publicarão suas APIs no ecossistema e não há distinção de fases para esta certificação, ou seja, o certificado de segurança cobre as APIs de todas as fases.

Já para a certificação funcional, é necessário ser feita englobando cada grupo de API que deseje-se publicar no ecossistema. Atualmente, tem-se as seguintes APIs:

- Fase 2: Consentimento, Dados Cadastrais (PF), Dados Cadastrais (PJ), Recursos, Contas, Cartão de Crédito, Operações de Crédito - Empréstimos, Operações de Crédito - Financiamentos, Operações de Crédito - Adiantamento a Depositantes e Operações de Crédito - Direitos Creditórios Descontados;
- Fase 3: Pagamentos

Para as instituições que participarão no ecossistema realizando o consumo de dados (Receptores) ou como iniciadores de pagamento (Iniciadores de Transação de Pagamento), temos um procedimento diferente: É necessário realizar uma certificação de segurança específica, focada no perfil chamado de ‘relying party’. Atualmente, esta certificação de segurança está dividida:

- Fase 2 (Receptores): A certificação não é obrigatória na data deste documento. Esta certificação será revisada no futuro, apesar de haver testes disponíveis para a API de Contas;
- Fase 3 (Iniciadores de Transação de Pagamento): A certificação de relying party, que engloba os módulos FAPI e DCR, será obrigatória para todos que desejam realizar a iniciação de pagamento.

É importante ressaltar que uma vez que a instituição realize suas certificações, ela passa a ter que seguir a convenção estabelecida, incluindo: Processos de recertificações, cronogramas para novos certificados, atualizações de APIs entre outros

### 2.2 Objeto de certificação

#### 2.2.1 Ambiente Prod vs. Pré-Prod

Ambas as certificações funcionais e de segurança poderão ser realizadas em ambiente produtivo ou pré-produtivo (homologação), ficando a cargo do participante a escolha.

Caso se opte pelo uso de um ambiente pré-produtivo, este deverá ser um espelho do ambiente de produção, possuindo a mesma arquitetura, elementos de rede e versões de software existentes em produção.

Após a realização dos testes, todos os dados utilizados, incluindo chaves públicas e privadas dos certificados e os dados do cliente do teste serão disponibilizados no ecossistema, ficando visível aos demais participantes do ecossistema e passíveis de auditoria. Desta forma, caso a instituição opte por realizar a certificação em ambiente produtivo, ela deve estar ciente e é responsável por revogar os certificados utilizados durante os testes e da necessidade da obtenção do consentimento dos clientes.

## 2.2.2 Quantidade de Certificações para entrada no Open Banking

As instituições deverão obter as certificações abaixo:

Tipo	Nome	Quando	Custo	Emissor
Segurança	FAPI: BR-OB ADV	Obrigatório para a Fase 2 e 3	Sim	OIDF
Segurança	FAPI – CIBA: BR-OB	Data a ser definida pela convenção	Sim	OIDF
Segurança	FAPI: BR-DCR ADV	Obrigatório para Fase 2 e 3	Incluso no FAPI: BR	OIDF
Funcional	Conformidade funcional OBB	Obrigatório para todas APIs (obtida por grupo de APIs)	Não	OBB
Segurança	FAPI: BR-RP ADV	Obrigatório para iniciadores de pagamento Fase 3	Sim	OIDF
Segurança	FAPI: BR-RP DCR	Obrigatório para iniciadores de pagamento Fase 3	Incluso no FAPI: BR-RP	OIDF
Segurança	FAPI -CIBA: BR-RP ADV	A necessidade de certificação dos RP ainda está em definição – Atualização do guia a ser realizada após definição	Sim	OIDF

## 2.3 Prazos

### 2.3.1 Fase 2

Para publicação das APIs no Diretório Central é mandatório a certificação de todas as famílias de APIs da FASE 2, em breve será disponibilizado a certificação funcional das APIs da FASE 1.

Para o *go-live* da Fase 2 as instituições deverão seguir o cronograma de certificação referenciado no link abaixo, que contempla tanto a certificação de conformidade de segurança, quanto a certificação de conformidade funcional:

<https://openbanking-brasil.github.io/areadesenvolvedor/#certificacao-de-conformidade>

Ressaltamos que as datas descritas devem ser seguidas apenas pelas instituições obrigatórias da Fase 2 ou que se voluntariaram para participar do *go-live* e realizaram a requisição de certificação junto com a OIDF, através da estrutura inicial do Open Banking, durante o mês de maio.

### 2.3.2 Fase 3

Para o *go-live* da Fase 3 as instituições deverão seguir o cronograma de certificação referenciado no link abaixo, que contempla tanto a certificação de conformidade de segurança, quanto a certificação de conformidade funcional:

<https://openbanking-brasil.github.io/areadesenvolvedor/#certificacao-de-conformidade>

Reforçamos que as instituições que já se certificaram no perfil FAPI e DCR com a ODF para a Fase 2 não precisarão se certificar novamente para a Fase 3.

### 2.3.3 Validade/Recertificação

A certificação de segurança terá validade indeterminada, devendo ser certificada apenas em duas situações:

- Adoção do ecossistema de uma nova versão do FAPI, neste caso deve-se seguir calendário de versionamento publicado pelos squad de versionamento;
- Mudanças internas na arquitetura da instituição, com troca de sistemas/soluções que suportam o uso do FAPI e FAPI-CIBA. Neste caso cabe a instituição avaliar a necessidade de uma recertificação.

As certificações funcionais possuem uma validade determinada e a recertificação deverá acontecer nas seguintes situações:

- Vencimento da validade do certificado;
  - Fase 2: É estimada uma validade de 3 meses para os certificados funcionais emitidos dentro dos primeiros 12 meses de operação da fase 2
  - Os cronogramas de recertificação serão publicados em datas próximas aos vencimentos dos certificados, para que as instituições se preparem
- Nova versão da API. Neste caso deve-se seguir os prazos a serem definidos e comunicados pelo comitê de versionamento
- Mudanças internas na arquitetura da instituição, com troca de sistemas/soluções que atendem a entrega da API. Neste caso cabe a instituição avaliar a necessidade de uma recertificação.

#### 2.3.3.1 Recertificação logo após período escalonado da Fase 2

Conforme orientações da estrutura do Open Banking, ao final do período de lançamento escalonado da Fase 2 do Open Banking, está previsto um período para recertificação obrigatória das instituições participantes da Fase 2. Para detalhes do cronograma, acessar a página da Área do Desenvolvedor: <https://openbanking-brasil.github.io/areadesenvolvedor/#certificacao-de-conformidade>

Essa primeira etapa de recertificação engloba melhorias e GAPs mapeados durante as primeiras semanas de operação (período escalonado), tanto das especificações das interfaces e perfis de segurança quanto dos motores de certificação.

Todas as instituições participantes da Fase 2 deverão se recertificar no escopo funcional, bem como no módulo do DCR de Segurança dentro do cronograma apresentado no Portal, sem necessidade de recertificação no módulo FAPI de Segurança.

## 2.4 Custos

### 2.4.1 Certificações

A certificação de segurança FAPI Brasil 1.0 das instituições financeiras participantes do Open Banking Brasil será realizada pela OpenID Foundation.

Conforme consta em sua página oficial, os custos de cada certificado possuem valores tabelados, possuem diferenciação para membros e não membros, e são pagos diretamente à OpenID Foundation. Até junho/2021, a tabela de preços da certificação FAPI apresenta os valores a seguir (fonte <https://openid.net/certification/fees/>):

- US\$ 1.000 para instituições associadas; ou
- US\$ 5.000 para instituições não associadas

Em vista do benefício de acessar custos reduzidos de certificação, pode ser de interesse de algumas instituições se associar à OpenID Foundation. A seguir, apresentamos algumas informações importantes que podem ajudar as IFs a realizar o processo de associação, caso desejado.

A certificação FAPI – Brasil engloba não só as variações dessa certificação, mas também o teste DCR – Brasil. Dessa forma é necessário apenas um pagamento para a realização dos dois testes mandatórios para a Fase 2.

Caso a instituição deseje realizar a certificação FAPI-CIBA ou *Relying Parties* será necessário um novo pagamento referente a uma nova certificação

A certificação FAPI e DCR para Relying Parties Fase 3 terá custo total de US\$ 1.000 para as instituições participantes. Dessa forma, será necessário apenas um pagamento para a realização dos dois certificados de segurança para Relying Party (FAPI + DCR).

### 2.4.2 Associação como membro da OpenID Foundation (opcional)

Para as instituições interessadas em se associar à OpenID Foundation, os custos variam conforme o porte e característica da instituição, conforme a tabela apresentada abaixo:

#### **Tabela: Custos de associação à OI DF**

Os custos de associação seguem a tabela da OI DF que podem ser encontrados no link abaixo:

<https://openid.net/foundation/members/registration>

Para se associar, a instituição deve fazer o procedimento diretamente pelo site da OpenID Foundation em:

<https://openid.net/foundation/members/registration>

Os benefícios de se tornar um membro, bem como demais informações, podem ser acessados em:

<https://openid.net/foundation/benefits-members/>

### 2.4.3 Associação como membro da comunidade Relying Party

O canal do Slack do Open Banking Brazil RP Community foi criado como um espaço seguro para os membros da comunidade aprenderem, compartilharem conselhos, identificarem, remediarem e corrigirem problemas com apoio da comunidade do Open Banking Brasil (reguladores e membros do GT de segurança, instituições financeiras, equipe de certificação ODF e membros de GTs).

O canal do Slack do Open Banking Brasil RP Community propõe inicialmente os seguintes canais:

#certification-instructions

#fapi-rp-certified-libraries

#introduce-yourself

#reference-implementations

#rp-tpv-support

#testing-instructions

Os registros ao canal Slack devem corresponder ao contato principal da organização e respectivo endereço de e-mail.

A adesão à comunidade dá acesso à taxa de certificação FAPI Relying Party de USD\$ 1.000 (um mil dólares) para qualquer BR RP / TPP que se registrar canal do Slack do Open Banking Brazil RP Community conforme os passos abaixo:

A) É necessário um membro do RP / TPP para ingressar no canal do Slack do Open Banking Brazil RP Community através do link: [https://join.slack.com/t/openbankingbr-z4z3977/shared\\_invite/zt-y3v8d81d-K7cC631dmA\\_Z4LKqXc\\_JvA](https://join.slack.com/t/openbankingbr-z4z3977/shared_invite/zt-y3v8d81d-K7cC631dmA_Z4LKqXc_JvA)

B) Assim que o RP / TPP entrar no canal Slack, o membro precisa se apresentar e apresentar sua organização por meio do subcanal #introduce-yourself através deste link: <https://app.slack.com/client/T02GHDV50AU/D02KK75QM51>

C) Em seguida, enviar mensagem direta para mike.leszcz ou Filip Skokan no Slack selecionando o nome no menu à esquerda com uma solicitação do código de desconto da taxa de certificação RP / TPP.

D) Assim que o código de desconto for recebido, acesse este link <https://openid.net/foundation/members/certifications/new> e inclua o código de desconto na Etapa

Uma opção de pagamento alternativa é pagar por meio de Chicago Advisory Partners. Se esta for sua preferência, você ainda precisa se cadastrar no canal Slack, apresentar-se e entrar em contato com: [administrativo@openbankingbr.org](mailto:administrativo@openbankingbr.org). Para garantir a adesão, solicitamos que o pedido seja feito com 30 dias de antecedência.

### 3. Processo de testes e certificação

#### 3.1 Pré-requisitos

##### 3.1.1 Criação de conta no Sandbox do diretório de participantes

Para realizar o acesso ao motor de conformidade funcional é necessário a criação de um utilizador no Sandbox do diretório de participantes, acessível através do link abaixo:

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

O processo de criação de uma conta no Sandbox do diretório de participantes pode ser conferido através da documentação de referência do diretório, acessível em:

<https://openbanking-brasil.github.io/areadesenvolvedor/#diretrizes-tecnicas-do-diretorio>

Não é necessário estar associado a nenhuma organização para acessar o motor de conformidade, ou seja, não é necessário ser nem administrador nem contato técnico de nenhuma instituição. Aqui o Sandbox do diretório é utilizado apenas como *Identity Provider* para o acesso ao motor de certificação.

Diferente do motor de conformidade, o motor da OI DF pode ser acessado utilizando uma conta do Google ou uma conta do GitLab.

### 3.1.2 TPP de testes e Registro do Cliente (DCR)

Para a realização dos testes de conformidade é necessário o uso de uma TPP de testes e o registro de dois Clientes na sua instituição através do processo de DCR. A instituição pode optar por utilizar uma TPP de exemplo já cadastrada no diretório ou criar a sua própria TPP seguindo as instruções do [Guia de Operações do Diretório](#). Os dados da TPP e exemplos de configurações do motor podem ser obtidos em <https://gitlab.com/openid/conformance-suite/-/wikis/Brazil-Example-Configuration>.

Instruções de como realizar o processo de DCR estão disponíveis no Portal do Desenvolvedor <https://openbanking-brasil.github.io/areadesenvolvedor/#dynamic-client-registration>.

Nota: os certificados de transporte e assinatura utilizados na criação da TPP de testes deverão ser utilizados no preenchimento dos campos do motor de conformidade.

### 3.1.3 Exposição das APIs

Como tanto o motor de segurança da OI DF quanto o motor de conformidade funcional do Open Banking estão implementados em servidores proprietários é importante notar que os *Authorization Servers* que serão testados devem estar expostos na Internet e com acesso configurado apenas aos certificados criados para fins de testes.

Após a finalização e publicação dos testes os certificados de transporte e assinatura ficam integralmente disponibilizados para consulta, dessa forma, é importante garantir que os dois certificados sejam invalidados após sua disponibilização.

O endereço IP do servidor do motor da OI DF pode ser encontrado no rodapé da página do motor de conformidade de segurança. Para o motor de conformidade funcional, no dia 25/06, o endereço IP era: 194.168.4.100#53. Essa informação será disponibilizada também no rodapé da página nas versões futuras.

### 3.1.4 Geração das massas de dados

Para a realização dos testes, as instituições financeiras deverão configurar diversas massas de dados que serão objeto dos testes. Como o motor de conformidade tem o seu código fonte disponível para todo ecossistema, é possível identificar as massas de dados de referência utilizadas nos testes no seguinte diretório do motor de certificação:



<https://gitlab.com/obb1/certification/-/tree/master/src/test/resources/jsonResponses>

### 3.1.5 Cadastro do A.S

Para se habituar ao Sandbox do Diretório de Participantes a instituição pode optar por cadastrar o seu Authorization Server nesse ambiente. Esse cadastro não é necessário para a execução dos testes, podendo a instituição apenas inserir os endpoints dos seus recursos, incluindo o endpoint .well-known, diretamente nas plataformas dos testes de conformidade.

Para realizar o cadastro do Authorization Server pedimos que consulte o guia de utilização do diretório central:

<https://openbanking-brasil.github.io/areadesenvolvedor/documents/OpenBankingGuiaOperacaoDiretorioCentral.pdf>

## 3.2 Funcionais

### 3.2.1 Acesso ao Motor de Conformidade Funcional

Em posse dos *endpoints* referentes ao Authorization Server a ser testado e após a criação e configuração dos certificados necessários a próxima etapa é realizar a configuração do plano de testes no motor de conformidade funcional. O participante tem a possibilidade de realizar os testes no motor que está hospedado pelo Open Banking Brasil ou pode também fazer *download* da ferramenta para execução dos testes em ambiente local. Para obtenção do certificado consultar a sessão 3.2.3

- O link para acesso ao Motor de Conformidade Funcional *online* é:

<https://web.conformance.directory.openbankingbrasil.org.br/login.html>

- O link para acessar o repositório do Motor de Conformidade Funcional para *download* e *setup* local é:

<https://gitlab.com/obb1/certification/>

- Um passo a passo para preenchimento do plano de testes pode ser encontrado em:

[https://openbanking-brasil.github.io/areadesenvolvedor/documents/Guia\\_OBB.pdf](https://openbanking-brasil.github.io/areadesenvolvedor/documents/Guia_OBB.pdf)

### 3.2.2 Execução dos testes

Ao realizar o acesso ao Motor de Conformidade Funcional e realizar o preenchimento dos campos necessários, é possível iniciar os testes para validação de conformidade funcional. O motor provê ao usuário resultado dos testes em tempo real e indica pontos de sucesso e pontos de falha, permitindo uma correção das implementações do participante de maneira assertiva, caso necessário.

Para execução dos testes, foi realizado um *Workshop* demonstrando o uso da ferramenta em tempo real, cujo link para acesso ao vídeo é:

[1º Workshop ferramenta de certificação funcional \(15/06/2021\)](#)

O participante não tem limitação do número de testes que pode executar e nem dos horários, dado que a ferramenta está disponível 24/7.

Após a conclusão da bateria de testes com sucesso, o participante pode iniciar o processo de requisição do certificado de conformidade funcional.

Caso a instituição deseje, como o motor de conformidade funcional está disponibilizado em formato *Open Source*, também é possível rodar os testes localmente, sem risco de exposição de dados sensíveis. É possível consultar a documentação relativa a esse processo em:

<https://gitlab.com/obb1/certification/-/wikis/Running-the-conformance-suite-locally>

<https://gitlab.com/openid/conformance-suite/-/wikis/Developers/Build-&-Run>

Também foi disponibilizado um vídeo demonstrando a execução local dos testes, que pode ser descarregado a partir do seguinte endereço: <https://we.tl/t-uc7ubl60m5>.

Com a ferramenta executando localmente, também é possível utilizá-la para fazer uma checagem dos *payloads* que estão sendo gerados pelas aplicações da instituição. Para isto, basta:

- Salvar um arquivo .json da resposta da aplicação contendo todo o *payload* que se deseja testar;
- Alterar o arquivo .json equivalente dentro dos arquivos do motor de conformidade:
  - Navegar até: `certification/src/test/resources/jsonResponses`
  - Encontrar o teste que deseja substituir o arquivo (`account`, `creditCard` etc);
  - Substituir o .json do teste (Para teste `account`, é `accountListResponse.json`)
- Após realizar as substituições, basta executar o comando para refazer o build da ferramenta:
  - `mvn clean package` caso esteja executando localmente sem container;
  - `docker-compose -f builder-compose.yml up` caso esteja executando localmente via container
- Ao executar o comando de build da ferramenta, ela realiza testes unitários nos arquivos .json presente nas pastas. O sucesso e/ou falha destes testes será exibido em forma de *output*
  - Caso o build tenha sido executado com sucesso, o teste unitário dos arquivos .json ocorreu com sucesso (*Payloads* validados);
  - Caso haja algum erro nos arquivos, o build não será realizado

### 3.2.3 Pedido de certificação funcional

Utilizando-se do motor de conformidade funcional, o participante deverá atingir a marca de 100% de sucesso nos testes antes do pedido de certificação. Com esta marca de sucesso, o participante deve então fazer o resultado de seus testes ficar público. Um exemplo de resultado de testes publicados pode ser acessado em:

<https://web.conformance.directory.openbankingbrasil.org.br/log-detail.html?log=yxaJTHHQjF4to64&public=true>

É importante ressaltar que este resultado deve ser atingido no motor de conformidade funcional hospedado pelo Open Banking Brasil, logo testes executados localmente não são válidos para pedido de certificação.

Para a submissão dos resultados dos testes executados pedimos que seja seguido o seguinte guia, disponibilizado atualmente em inglês:

### Guia de submissão de pedido de certificação

O pedido submetido será avaliado pelo time da Raidiam/OBB e a publicação do resultado deste pedido de certificação será publicado em portal do Open Banking Brasil.

Após a publicação do certificado de conformidade funcional, o participante está apto à publicação de suas APIs no ambiente de produção do Open Banking Brasil.

#### **3.2.4 Status da certificação funcional**

O status “CONDITIONAL PASS” pode ser emitida a critério da Estrutura de Governança quando houver uma ambiguidade potencial na especificação. Nesta situação uma instituição está retornando uma resposta divergente da maioria dos participantes do Open Banking. Um “CONDICIONAL PASS” só será emitido se a interpretação alternativa tiver pouco ou nenhum impacto nas operações de um Consumidor de Dados ou TPP. Uma instituição com um “CONDICIONAL PASS” deve enviar uma recertificação dentro de 2 semanas, demonstrando que a resposta subjacente foi tratada.

O status “IN REVISION” pode ser emitido quando a Estrutura de Governança foi informada da não conformidade com as especificações que podem afetar a interoperabilidade. As instituições com o status “IN REVISION” serão notificadas e deverão refazer seus testes em prazo a ser estabelecido pela estrutura em função do problema de interoperabilidade.

Um status “PASS\*” pode ser emitido quando a Estrutura de Governança receber uma submissão técnica que está em conformidade, no entanto, a instituição requerente não forneceu comprovação precisa da documentação de conformidade. Este estado temporário está disponível apenas para envios de recertificação.

O status “PASS” será emitido quando a Estrutura de Governança receber uma submissão técnica em conformidade e a instituição requerente forneceu comprovação precisa da documentação de conformidade. Os certificados no status “PASS” podem ter seu status alterado para “IN REVISION” quando um problema técnico não mapeado anteriormente for identificado e este for considerado altamente crítico para o ambiente de interoperabilidade do ecossistema.

### **3.3 Segurança**

#### **3.3.1 Passo-a-Passo dos Testes**

Necessário executar dois testes:

- FAPI1-Advanced-Final: Authorization Server test
- FAPI1-Advanced-Final: Brazil Dynamic Client Registration Authorization server test

1) Acessar <https://www.certification.openid.net/> e realizar o login.

2) Clicar "Create a new Plan Test".

2.1) No campo "Test Plan", selecionar "FAPI1-Advanced-Final: Authorization Server test"

- 2.1.1) No campo "Client Authentication Type", selecionar **private\_key\_jwt** ou **mtls**.
- 2.1.2) No campo "Request Object Method", selecione a opção da sua instituição.
- 2.1.3) No campo "FAPI Profile", selecionar o **openbanking\_brazil**.
- 2.1.4) No campo "FAPI Response Mode", selecione a opção da sua instituição.
- 2.1.5) Preencher os campos das seções: Test Information, Server, Client, TLS certificates for client (used to make MTLS connections), Second client, Second client TLS certificates e Resource.
- 2.1.6) Após a criação do "Test Plan", vão ser exibidos todos os testes que devem ser executados.
- 2.1.7) Exemplo de caso de uso de execução:

<https://gitlab.com/openid/conformance-suite/-/wikis/Brazil-Example-Configuration>

3) Clicar "Create a new plan test".

3.1) No campo "Test Plan", selecionar " FAPI1-Advanced-Final: Brazil Dynamic Client Registration Authorization server test "

3.1.1) No campo "Client Authentication Type", selecione a opção da sua instituição.

3.1.2) No campo "Request Object Method", selecione a opção da sua instituição.

3.1.3) No campo "FAPI Response Mode", selecione a opção da sua instituição.

3.1.4) Preencher os campos das seções: Test Information, Server, Client, TLS certificates for client (used to make MTLS connections), Resource e Directory.

3.1.5) Após a criação do "Test Plan", vai ser exibido o teste a ser executado.

3.1.6) Exemplo de como executar:

<https://gitlab.com/openid/conformance-suite/-/wikis/Brazil-DCR-Example-Configuration>

Mais informações no site da OIDF: <https://openid.net/certification/instructions/>

Descrição dos campos:

- Test Plan: Selecionar alguns dos testes disponibilizados no menu Open Banking Brasil Functional Tests
- Client Authentication Type: Selecionar o tipo de autenticação de cliente compatível com seu software
- 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>
- Alias: Escrever o nome desejado para o plano de testes
- Description: Escrever a descrição desejada para o plano de testes
- Publish: Selecionar "No" para não tornar os resultados do teste público para todos
- DiscoveryUrl: Adicionar o well-known Discovery endpoint do servidor de autorização: <https://xxx/.well-known/openid-configuration>
- Client\_id: Adicionar o client\_id do software statement criado no Sandbox do diretório de participantes

- Scope: Escopos a serem usados na solicitação de autorização, por exemplo, 'openid accounts'
- Jwks: Inserir o jwks relativo ao certificado de assinatura criado para assinar os objetos do cliente e se private\_key\_jwt para autenticação do cliente
- Organisation\_jwks: chave BRSEAL gerado para assinatura das mensagens de pagamento. Pode ser igual ao Jwks
- Mtls.cert: Adicionar as informações do certificado de transporte BRCAC (.pem)
- Mtls.key: Adicionar a chave privada do certificado de transporte BRCAC (.key)
- Mtls.ca: Adicionar os certificados do Root CA do diretório e do issuer CA do diretório. Supondo que seja utilizado o PKI do diretório
- ResourceUrl: Especificar a url do recurso que será utilizado para execução dos testes. Por exemplo: <https://api.edbank.com.br/openbanking/accounts/v1/accounts>
- consentUrl: Especificar a url do do consentimento. Por exemplo: <https://api.edbank.com.br/openbanking/consents/v1/consents>
- brazilCpf: O valor 'CPF' a ser usado na solicitação de criação de consentimento.
- BrazilCnpj: O valor 'CNPJ' a ser usado na solicitação de criação de consentimento.
- Resource server organization id: O id da organização que provê o recurso, conforme o diretório. Deve ser preenchido quando utilizada a API de pagamentos
- Authorization server organization id: Valor do 'organization id' do authorization server, conforme registrado no diretório (aplicável somente para 'scope' que contém 'payments').
- Payment consent request JSON: JSON de uma solicitação de consentimento de pagamento. Será utilizado como body do request enviado ao endpoint de consentimento de pagamento (aplicável somente para 'scope' que contém 'payments').
- Payment initiation request JSON: JSON de uma solicitação de pagamento PIX. Será utilizado como body do request enviado ao endpoint de iniciação de pagamento (aplicável somente para 'scope' que contém 'payments').
- Discovery Endpoint: URL para o diretório OpenBanking. Por exemplo: <https://auth.sandbox.directory.openbankingbrasil.org.br/.well-known/openid-configuration>
- Directory ClientID: client\_id para este cliente no OpenBanking Directory. É empregado para obter um token de acesso para recuperar a Software Statements.
- Directory API base: URL base para o OpenBanking Directory Sandbox. Por exemplo: <https://matls-api.sandbox.directory.openbankingbrasil.org.br/>
- Directory keystore base: O caminho para o keystore do diretório. Para sandbox usar "https://keystore.sandbox.directory.openbankingbrasil.org.br/"
- <https://openid.net/2021/04/14/guest-blog-financial-grade-api-fapi-explained-by-an-implementer-updated/>
- <https://gitlab.com/openid/conformance-suite/-/wikis/home>
- [https://openid.net/certification/fapi\\_op\\_testing/](https://openid.net/certification/fapi_op_testing/)

A OIDF também disponibiliza na sua plataforma o teste FAPI - RP (*Relying Parties*) que permite o teste das receptoras de dados (ou Iniciadores de Transação de Pagamento). A execução do teste é recomendada, porém não é mandatória para o go-live da Fase 2, enquanto que as iniciadoras de transação de pagamento (fase 3) deverão obter suas certificações de segurança Relying Party em data a ser formalizada pela convenção.

Mais detalhes sobre os testes de RP podem ser encontrados em:

[https://openid.net/certification/fapi\\_rp\\_testing/](https://openid.net/certification/fapi_rp_testing/)

Em caso de dúvidas ou problemas na execução dos testes, favor consultar o item 4.3: Suporte – Motor de Segurança

### 3.3.2 Pedido de certificação de segurança

Para realizar o pedido de certificação de segurança junto a OIDF o participante deverá consultar as instruções contidas no endereço: [https://openid.net/certification/op\\_submission/](https://openid.net/certification/op_submission/)

### 3.3.2 Documentação adicional OIDF

Além das especificações dos perfis FAPI, citadas no final desse Guia, a OIDF também recomenda a consulta do artigo, “FAPI explicada por um desenvolvedor”, para as instituições que buscam a certificação FAPI. Esse artigo pode ser acessado pelo seguinte link:

[FAPI Explicada por um desenvolvedor](#)

## 4. Suporte

### 4.1 Glossário

**Open ID Foundation (OIDF):** *A OpenID Foundation é uma organização internacional sem fins lucrativos, voltada para desenvolvedores e empresas. Tem como objetivo auxiliar a comunidade fornecendo a infraestrutura necessária e ajuda a promover e apoiar a adoção ampliada do OpenID.*

**Motor de Conformidade de Segurança:** *Ferramenta disponibilizada pela Open ID Foundation que implementa o perfil de segurança do Open Banking Brasil. Através desta plataforma é possível a validação da camada de segurança das aplicações da Instituição Participante.*

**Motor de Conformidade Funcional:** *Ferramenta disponibilizada pela Estrutura de Governança para realização de testes de conformidade de especificações de API da Instituição Participante.*

**Implementação de Referência:** *Implementação de exemplo das APIs do Open Banking Brasil, simulando uma Instituição Participante de Referência.*

**Estrutura de Governança:** *Estrutura responsável pela governança do processo de implementação no País do Sistema Financeiro Aberto (Open Banking).*

**Instituições Participantes:** *Todas as instituições autorizadas a funcionar pelo Banco Central do Brasil e que se cadastram para participar do Open Banking Brasil, conforme regulamento vigente.*

**Diretório:** *O Diretório de Participantes é o ambiente no qual uma instituição autorizada a funcionar pelo Banco Central do Brasil formaliza sua participação no ambiente do Open Banking,*

**Sandbox do Diretório:** *O Sandbox do Diretório de Participantes é uma implementação cópia do diretório de participantes para a realização de testes. Esse ambiente possui uma base de dados e PKI completamente independente do Diretório produtivo*

**Relying Parties (RP):** *Termo em inglês que se refere a aplicação que interagem com os servidores de autorização das instituições financeiras. No Escopo do Open Banking estamos falando das receptoras de dados para a Fase 2 e das iniciadoras de pagamentos para a Fase 3*

**FAPI (Financial-grade API):** *Especificação técnica de API e define requisitos técnicos adicionais para o setor financeiro*

**Dynamic Client Registration (DCR):** *O Perfil de Registro de Cliente Dinâmico de Financial-grade API (FAPI) do Open Banking Brasil é um perfil que visa fornecer diretrizes de implementação específicas*

*para segurança e interoperabilidade que podem ser aplicadas à identificação, registro e gerenciamento de Clientes OAuth operando no ecossistema Brasil Open Banking.*

**CIBA (Client Initiated Backchannel Authentication):** *A autenticação de backchannel iniciada pelo cliente (CIBA) é um dos padrões mais recentes da OpenID Foundation. São categorizados como "fluxo desacoplado" e permite novas maneiras de obter o consentimento do usuário final* Canais para Dúvidas

Para suportar as instituições em caso de dúvidas sobre o processo de certificação o Open Banking Brasil dispõe de FAQ e de uma equipe de *service desk* responsável por solucionar problemas obtidos durante a utilização tanto da ferramenta da OpenID Foundation quanto para a ferramenta para testes funcionais do OBB.

## 4.2 Service Desk

A equipe de suporte do processo de conformidade utiliza a mesma infraestrutura do Service Desk do Open Banking, acessível através do link: <https://servicedesk.openbankingbrasil.org.br/Login.jsp>

A abertura de chamados pode ser realizada tanto pelos usuários logados, atrelados a alguma instituição financeira, quanto para usuários não logados. O processo para abertura de um chamado de um usuário logado pode ser conferido através do tutorial em vídeo, abaixo:

<https://youtu.be/bhMOtliGjKc>

A equipe de suporte do processo de conformidade está disponível para solucionar questões relacionados a:

- Dúvidas gerais relacionadas a política de certificação
- Suportar na abertura e acompanhamento do pedido de certificação
- Interpretação de erros encontrados no log de testes
- Configuração dos planos de testes nas plataformas de certificação
- Documentação relativa ao processo de certificação

A equipe de suporte não tem irá fornecer suporte técnico relacionado à como o participante deve construir sua implementação do Open Banking.

Dentro da plataforma os chamados podem ser abertos em uma série de categorias diferentes. Para dúvidas, questões e problemas relativas ao motor de conformidade temos a seguinte lista de categorias que podem ser utilizadas:

- Incidentes -> Conformidade
  - APIs: Problemas causados por ambiguidade ou inconsistências nas especificações das APIs
  - Motor de Conformidade: Problemas na criação, execução e divergência com especificações nas plataformas da OIDF e do Open Banking
- Solicitação de Informações -> Conformidade
  - APIs: Interpretação e questões relativas as especificações das APIs
  - Motor de Conformidade: Dúvidas com criação, execução e interpretação dos resultados dos testes
  - Política de certificação: Questionamentos sobre prazos, regulação e custeio
- Enviar pedido de certificação

- Comentado no item “Submissão de certificados”, no menu acima

A equipe de atendimento do motor de conformidade está disponível 8x5, ou seja, oito horas por dia apenas em dias úteis F.A.Q.

Também é disponibilizado um FAQ relativo à política de certificação que pode ser consultado em:

<https://openbanking-brasil.github.io/areadesenvolvedor/#faq-testes-e-homologacao>

Pedimos que os participantes, antes de abrirem um chamado, consultem se a sua dúvida não está contemplada dentro do FAQ de certificação.

#### 4.3 Suporte – Motor de conformidade de Segurança

Em caso de dúvidas sobre a execução dos testes de conformidade de segurança pedimos que entrem em contato pelo email [certificate@oidf.org](mailto:certificate@oidf.org).

Para relatar possíveis bugs ou alterações necessárias, pedimos que sejam abertos tickets em <https://gitlab.com/openid/conformance-suite/-/issues/new>

#### 4.4 Especificações

As especificações referentes ao Open Banking podem ser encontradas em sua integralidade no portal do Desenvolver, acessível através do Link:

<https://openbanking-brasil.github.io/areadesenvolvedor>

#### 4.5 Links de Apoio

FAPI Especificações

[Financial-grade API Security Profile 1.0 — Part 2: Advanced](#)

FAPI Motor de testes e certificação

[How to run conformance tests for FAPI-RW OPs](#)

[How to request certification after successfully completing conformance testing for FAPI-RW and FAPI-CIBA OPs](#)

[Financial-grade API \(FAPI\), Explained by an Implementer – Updated](#)

[FAPI Explicada por um desenvolvedor](#)

Service Desk

<https://servicedesk.openbankingbrasil.org.br/index.jsp#/Dashboard.jsp>

FAQ – Testes e homologação



<https://openbanking-brasil.github.io/areadesenvolvedor/documents/FAQ%20-%20Testes%20e%20Homologa%C3%A7%C3%A3o.pdf>

#### Diretório de Participantes e Sandbox

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

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

#### Motores de conformidade

<https://web.conformance.directory.openbankingbrasil.org.br/login.html>

<https://www.certification.openid.net/login.html>

#### Repositórios dos motores de conformidade

<https://gitlab.com/obb1/certification>

<https://gitlab.com/openid/conformance-suite/-/wikis/home>

#### Workshops dos testes de conformidade funcional e de segurança

[1° Workshop com OpenID Foundation \(17/05/2021\)](#)

[2° Workshop com OpenID Foundation \(24/05/2021\)](#)

[3° Workshop com OpenID Foundation - Motor de certificação de segurança](#)

[1° Workshop ferramenta de certificação funcional \(15/06/2021\)](#)

[Workshop com OpenID Foundation - FAPI Brasil e DCR - Fase 3 \(03/08/2021\)](#)