Guia de certificação de conformidade

Versão 7 - 12/09/2022

1. Introdução

O Open Finance 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 Finance 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 Finance Brasil. Esse guia é complementar a outras documentações disponibilizadas pela governança e não fazem parte do escopo deste, quaisquer detalhamentos relacionados a experiencia do usuário/desenvolvedor, definições de segurança e especificação de APIs.

Observações: Estão previstos versionamentos contínuos deste guia ao longo dos primeiros meses de implementação do Open Finance 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 Finance, 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 Finance a testes automatizados funcionais (“Motor de Conformidade Funcional”); e,
- Acessar implementações de exemplo das APIs do Open Finance que simule uma Instituição Participante de Referência, com implementação completa de cada API (“Implementação de Referência”).

Uma implementação de versão de API do Open Finance 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
    - Perfil FAPI BR
    - DCR – Dynamic Client Registration
    - Perfil FAPI BR *Relying Parties*
    - Perfil DCR BR *Relying Parties* – A ser detalhado em versão posterior do guia
    - Perfil CIBA BR - A ser detalhado em versão posterior do guia

  Funcionais
    - Estrutura das URLs
    - Cabeçalhos
    - Códigos de Resposta
    - Escopos e Permissões
    - 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 Finance 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***

Implementação de exemplo das APIs do Open Finance Brasil, simulando uma Instituição Participante de Referência

2. Políticas Gerais

2.1 Participantes

A governança do Open Finance 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 se deseja publicar no ecossistema. Atualmente, tem-se as seguintes APIs:

- Fase 2: Consentimento, Dados Cadastrais (PF), Dados Cadastrais (PJ), Resources, 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 engloba os módulos FAPI e DCR e será obrigatória para todos que desejam atuar como receptores de dados;
- 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.

A certificação RP para a Fase 3 (Iniciadores de Transação de Pagamento) é válida também para a Fase 2 (Receptores), mas o inverso não é verdadeiro.

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 uma 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 Finance

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
Funcional	Limites Operacionais	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

Para go-live das APIs em ambiente produtivo é mandatório que todas as certificações de segurança e funcionais tenham sido emitidas e devidamente publicadas no Diretório Central. Instruções para o procedimento podem ser obtidas em: https://openbankingbrasil.atlassian.net/wiki/spaces/OB/pages/9634736/Guia+de+Opera+o+do+Diret+rio+Central

2.3.3 Validade/Recertificação

2.3.3.1 Política de expiração de certificações de segurança emitidas pela OpenID Foundation (FAPI, DCR e RP)

As regras descritas na política abaixo são válidas para todas as certificações de segurança emitidas pela OpenID Foundation (OIDF) no contexto do Open Finance (FAPI, DCR, RP e, futuramente, CIBA).

Validade

- Serão necessárias recertificações quando houver:
    - Exigência da Estrutura do Open Finance motivada por mudança de versão de documentações OIDF ou no FAPI-BR, independente do tempo desde a última certificação
        - As mudanças na documentação serão analisadas pela Estrutura do Open Finance e a necessidade de recertificação será comunicada para as instituições
    - Alteração de tecnologia e/ou infraestrutura de produção utilizada pela instituição, independente do tempo desde a última certificação:
        - Plataforma de hospedagem (Ex.: AWS, Azure, Google);
        - Tecnologias de plataforma OFB (Ex.: mudança de solução de mercado para desenvolvimento interno);
    - A certificação anterior completar 12 meses desde a data de submissão.

Submissão

- O pedido de certificação deve ser submetido e pago até a data de expiração e todo o processo deve ser concluído em até 60 dias após a data de expiração.
- A cobrança da certificação é realizada por submissão, portanto, no momento da nova submissão, recomendamos que seja submetido o pedido de FAPI (private key, MTLS, PAR) e DCR juntos.

Exceção para certificações FAPI e DCR emitidas até 27/06/2022

Para as certificações FAPI e DCR emitidas até 27/06/2022, em caráter de exceção, será considerado o prazo de expiração mais longo dentre as duas.
Exemplo: Instituição com

- Certificações realizadas:
    - § FAPI em 15/06/2021,
    - § DCR em 30/11/2021 e
    - § RP em 15/12/2021
- Prazo para obter nova certificação:
    - § FAPI e DCR até 30/11/2022
    - § RP até 15/12/2022.

O prazo de expiração no Diretório (campo “expiration date of certification”) não será atualizado conforme a exceção, mas pedimos que as instituições considerem as políticas aqui informadas.

Pagamento via Chicago Advisory

Foi definido que o pagamento de certificações OIDF poderá ser intermediado, em caso de exceção, pela Chicago.

Nesse caso, no momento da nova submissão, selecionar a opção "Pagamento intermediado pela Chicago" no formulário de submissão de certificação no site da OIDF e enviar um e-mail ao financeiro@chicagoadvisory.com.br com as seguintes informações:

- Solicitação da instituição contendo o motivo para consideração de exceção
- Invoice contendo o valor da certificação e dados bancários do fornecedor (OIDF)

A Chicago analisará o pleito e tendo aprovação, enviará:

- Nota de débito e o boleto para pagamento da instituição, além de demonstrativo do cálculo incluindo impostos
- A cotação do dólar (base no dia da nota de débito)
- Informação sobre prazo para pagamento (até 20 dias)

Após identificação do recebimento do pagamento pela instituição, será realizado o pagamento para a OIDF através da Chicago

Caso haja diferença de cotação no fechamento do câmbio, será realizada devolução à instituição ou enviada nota de débito ou boleto complementar para pagamento da diferença.

Informações sobre quais certificações são necessárias e o valor a ser pago à OIDF devem ser obtidas no documento de Orientações à certificação, através de tickets no service desk ou discutidos diretamente com a OIDF, estando a Chicago disponível apenas para apoiar na operacionalização do pagamento.

Para evitar a necessidade de intermediação da Chicago em um procedimento que ocorrerá com base no mínimo anual e que é uma exceção ao Regulamento de Contratações, pedimos que as instituições que possuem dificuldades internas para realizar o pagamento diretamente para a OpenID, como cadastro de fornecedor estrangeiro, regularizem esse processo o mais breve possível.

Maiores informações sobre certificações
https://openbankingbrasil.atlassian.net/wiki/spaces/OB/pages/1738043/Diretrizes+T+cnicas+de+Certifica+o+de+Conformidade

Maiores informações sobre certificações:
https://openbankingbrasil.atlassian.net/wiki/spaces/OB/pages/1738043/Diretrizes+T+cnicas+de+Certifica+o+de+Conformidade

Maiores informações sobre OpenID Foundation - https://openid.net/certification/

2.3.3.2 Política de expiração de certificações funcionais

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

- Vencimento da validade do certificado (a definir);
- 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.
- Sempre que o ecossistema julgar necessário, neste caso serão comunicados os motivos, quais certificações precisarão ser refeitas e prazo.

2.4 Custos

2.4.1 Certificações

A certificação de segurança FAPI Brasil 1.0 das instituições financeiras participantes do Open Finance 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. A tabela de preços da certificação FAPI estão disponíveis em: https://openid.net/certification/fees/.

A certificação FAPI – Brasil engloba não só as variações dessa certificação, mas também o teste DCR – Brasil. Dessa forma, realizando ambas as certificações em um único pedido, 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.

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.

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 OIDF

Os custos de associação seguem a tabela da OIDF 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/

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

É necessário estar associado a alguma organização participante no Diretório (produção ou sandbox) para acessar o motor de conformidade funcional, ou seja, é necessário ser administrador ou contato técnico de alguma instituição.

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

https://openbankingbrasil.atlassian.net/wiki/spaces/OB/pages/9634736/Guia+de+Opera+o+do+Diret+rio+Central

Diferente do motor de conformidade funcional, o motor da OIDF 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://openbankingbrasil.atlassian.net/wiki/spaces/OB/pages/1737964/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 OIDF quanto o motor de conformidade funcional do Open Finance 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 OIDF pode ser encontrado no rodapé da página do motor de conformidade de segurança. Para o motor de conformidade funcional, no dia 25/06/2021, 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 ambiente do Diretório de Participantes a instituição pode optar por cadastrar o seu Authorisation Server em Sandbox. 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 Authorisation Server pedimos que consulte o guia de utilização do diretório central:

https://openbankingbrasil.atlassian.net/wiki/spaces/OB/pages/9634736/Guia+de+Opera+o+do+Diret+rio+Central

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 Finance 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/

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. Materiais de apoio estão disponíveis em:

https://openbankingbrasil.atlassian.net/wiki/spaces/OB/pages/1738043/Diretrizes+T+cnicas+de+Certifica+o+de+Conformidade

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

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 Finance 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 Finance Brasil.

Após a publicação do certificado de conformidade funcional, o participante está apto à publicação de suas APIs no ambiente de produção do Open Finance 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 Finance. 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 Finance 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 -know 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/

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 dos testes é mandatória para receptoras da Fase 2 e iniciadoras de transação de pagamento da Fase 3.

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

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/**

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 acessa 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 Finance 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 Finance 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 Finance).*

Instituições Participantes: *Todas as instituições autorizadas a funcionar pelo Banco Central do Brasil e que se cadastram para participar do Open Finance 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 Finance,*

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 Finance 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 Financal-grade API (FAPI) do Open Finance 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 Finance.*

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 Finance 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 Finance, 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 Finance.

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 Finance
- 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.

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 Finance podem ser encontradas em sua integralidade no portal do Desenvolver, acessível através do Link:

https://openbankingbrasil.atlassian.net/wiki/spaces/OB/pages/8683521/Especifica+es+de+APIs

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://openbankingbrasil.atlassian.net/wiki/spaces/OB/pages/1639437/FAQ+-+Testes+e+Homologa+o

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

Materiais complementares

https://openbankingbrasil.atlassian.net/wiki/spaces/OB/pages/1738043/Diretrizes+T+cnicas+de+Certifica+o+de+Conformidade