



Visão Geral do Ecossistema



Owned by [Eloisa de Oliveira Santos \(Unlicensed\)](#) ...

Jun. 19, 2023 • 8 min read

Em sua essência, o Open Finance Brasil é um ecossistema de compartilhamento de dados onde os clientes de bancos e outras instituições financeiras desejam compartilhar suas informações de conta ou dar permissão para que os pagamentos sejam executados em seu nome com serviços de terceiros e o Open Insurance Brasil utiliza os padrões de segurança do Open Finance Brasil.

Há uma série de funções necessárias para vincular qualquer sistema de identificação, autenticação e autorização, independentemente do setor. Todas essas funções são necessárias, mas várias funções podem ser desempenhadas por cada participante. Em geral, o usuário final ("Subject"), está dando a um sistema ("Client") uma autorização ("Access Token") para acessar um recurso protegido mantido pelo provedor ("Resource Server"). Isso exige que o Subject e o Client sejam identificados e autenticados e que a autorização seja confirmada.

As regras exatas e os requisitos legais para cada função em um setor específico formam um framework de confiança ("Trust Framework"). Cada ecossistema requer um conjunto padronizado de regras e requisitos legais que abrangem todas as funções e obrigações das interações acima. A combinação de quem fornece qual(is) função(ões), os níveis aos quais eles devem desempenhar essas funções e os padrões pelos quais essas operações devem ser definidas por um framework de confiança específico do setor.

Diferentes frameworks de confiança terão diferentes opções de implementação, mas um framework de confiança comum é um pré-requisito para transformar um 'setor' em um 'ecossistema'. Um framework de confiança comum reduz significativamente a complexidade e custos, aumenta a escalabilidade e a interoperabilidade dentro do setor, bem como abre opções para o tipo de padronização intersetorial que o Open Insurance Brasil está buscando.

Diferentes implementações podem ser definidas para setores, com diferentes prós / contras e custos associados para diferentes participantes. Cada uma das

implementações propostas pode ser usada para qualquer setor se os pré-requisitos corretos estiverem em vigor. A solução certa dependerá do apetite e alinhamento de

Área do / **Visão Geral do Ecossistema**



A implementação de um mecanismo comum para o Open Insurance Brasil exigirá um compromisso com a simetria entre os setores para incluir detalhes específicos do setor nos princípios do framework de confiança.

É necessário fazer escolhas técnicas para garantir que qualquer implementação forneça uma base estrita e consistente para ter credibilidade, mas mantenha a flexibilidade para se adaptar às necessidades futuras. Isso implica padrões de código-fonte aberto amplamente disponíveis, amplamente compreendidos e que foram experimentados e testados. Além de habilitar uma gama de parceiros e fornecedores que podem apoiar qualquer construção técnica, o que significa que continuará havendo espaço para desenvolvimento comercial de soluções.

Participantes de um Ecossistema de Compartilhamento de Dados

Nos ecossistemas de Open Insurance voltados para o consumidor que estamos considerando, temos três participantes principais:

- O cliente (user)
- A instituição transmissora de dados (provider), que oferece serviços de seguros
- A instituição receptora de dados (TPP - Third Party Provider), que oferece uma proposta de Open Insurance para o cliente:

Em todos os casos a seguir, assumimos:

- Um cliente possui uma conta para um serviço principal ou conjunto de recursos numa instituição transmissora de dados
- Uma instituição receptora de dados oferece ao cliente uma proposta habilitada por meio do compartilhamento inteligente de dados
- O cliente dá consentimento à instituição receptora de dados para fins de entrega dessa proposta
- A instituição transmissora de dados tem a obrigação de salvaguardar os dados do cliente, mas também de compartilhá-los quando instruído.

O ecossistema também possui provedores de serviços de confiança, que são entidades que fornecem garantia técnica a ambas instituições (transmissoras e receptoras) de que todos estão autorizados a participar do ecossistema.

Os **padrões** técnicos necessários para dar suporte ao framework de confiança devem atender todos os requisitos a seguir:

Área do / **Visão Geral do Ecossistema**



- Autenticação quando exigida de todos os participantes entre si
- Confirmação de autorização de todos os participantes em um ecossistema de compartilhamento de dados

Os **serviços** técnicos necessários para suportar um ecossistema devem habilitar todos os requisitos acima **em uma base e modo contínuos**, isto é, não apenas em um único ponto de registro.

Princípios de Especificação e Requisitos de Alto Nível

O Open Insurance Brasil adotou os seguintes princípios e requisitos de alto nível no que diz respeito às normas técnicas.

- Consentimento
 - Os clientes devem estar sempre no controle de quem tem acesso aos seus dados e para quais fins eles estão sendo usados.
- Minimização de dados
 - Os clientes devem ser capazes de compartilhar apenas os dados de que precisam, pelo tempo que for necessário.
- Segurança
 - Uma modelagem de ameaças foi produzido avaliando todas as fraquezas potenciais nos processos de comunicação.
 - Todos os pontos fracos identificados foram corrigidos.
- Identificação
 - Todos os participantes devem ter segurança na identificação de todos os atores do ecossistema.
- Autenticação
 - Todos os participantes devem comunicar as etapas que foram executadas para autenticar cada participante no ecossistema e em que nível isso foi executado.
- Integridade e não repúdio
 - Todos os participantes devem ser capazes de provar que as mensagens não foram adulteradas e, na verdade, foram enviadas apenas por um participante legítimo.

Além dos requisitos de alto nível, os seguintes princípios também foram adotados.

Área do / Visão Geral do Ecossistema



- Envolver-se com outros órgãos de normalização para aprender com experiências anteriores sobre o que funcionou, o que não funcionou, e o que pode ser feito melhor.
- Assegurar o amplo suporte da indústria para garantir o máximo de chances de sucesso e, mais importante, a segurança do cliente.
- Solicitar feedback com antecedência e com frequência, reconhecer que serão necessárias várias iterações para desenvolver um padrão.
- O framework de confiança que sustenta o ecossistema de compartilhamento de dados, que é o Open Insurance Brasil, é um framework técnico que precisa ser flexível o suficiente para permitir que os participantes e o ecossistema inovem, cresçam e se desenvolvam, enquanto permanecem interoperáveis.

Todos os participantes devem ter certeza de que todos os atores do ecossistema estão lidando com seus dados com segurança tempo todo. Isso requer que todos os participantes testem publicamente seus sistemas quanto à conformidade com as especificações e disponibilizem os resultados de seus testes de conformidade para exame público de outros participantes.

Este é um requisito aplicável à instituições participantes transmissoras e receptoras de dados.

Principais Padrões de Segurança

Estrutura de Autorização OAuth 2.0

O ecossistema de compartilhamento de dados definido pelo Brasil consiste em muitos padrões diferentes, todos girando em torno de conceitos, funções e obrigações que foram tecnicamente definidos no [OAuth 2.0 Authorization Framework](#).

A estrutura de autorização OAuth 2.0 permite uma aplicação de terceiros (third-party application) obter acesso limitado a um serviço HTTP, seja em nome do proprietário de recurso (resource owner) por meio da orquestração de uma interação de aprovação entre o proprietário do recurso e o serviço HTTP, ou permitindo a aplicação de terceiros obter acesso em seu próprio nome.

A especificação base OAuth 2.0 não fornece, por si só, informações suficientes para atender a todas as necessidades definidas pelo framework de confiança do Open

Área do / Visão Geral do Ecossistema



transmissora para uma receptora, e os mecanismos de autenticação que foram definidos na especificação original não são seguros o suficiente para atender aos requisitos de uma indústria altamente regulamentada.

OpenID Connect - A Camada de Identidade para a Internet

Este perfil herda todas as obrigações do OAuth 2.0

OpenID Connect é um conjunto de especificações simplificadas que fornecem uma estrutura para interações de identidade por meio de APIs do tipo REST. A implementação mais simples do OpenID Connect permite que clients de todos os tipos, incluindo baseados em navegador, celulares e clients javascript, solicitem e recebam informações sobre identidades e sessões atualmente autenticadas. O conjunto de especificações é extensível, permitindo que os participantes também suportem, opcionalmente, criptografia de dados de identidade, descoberta do OpenID Provider e gerenciamento avançado de sessão, incluindo logout.

O grupo de trabalho OpenID Foundations Connect tem sido o guardião do Padrão de Identidade “de fato” da Internet por muitos anos, trabalhando em várias especificações que se baseiam no framework de autorização OAuth 2.0, adicionando recursos e requisitos de suporte para melhorar a segurança do framework em si.

Open ID Connect Core: é um perfil do OAuth 2.0, o que significa que herda todos os requisitos e obrigações do OAuth 2.0, mas define o conceito de um `id_token` e introduz novos mecanismos de autenticação.

Open ID Connect Discovery: apresenta o conceito de um documento de descoberta usado por *OpenID Connect (OIDC) Providers* para anunciar como os *clients* OAuth 2.0 podem se comunicar com eles e quais recursos e opções o OIDC Provider oferece suporte.

RFC7591: além de definir o processo de registro dinâmico de *clients* OAuth, esta especificação apresenta o conceito de Software Statement (“Declaração de Software”), que pode ser usada para fornecer informações sobre um *client* que é atestado por um serviço de terceiros. Outros atributos de metadados também são definidos no OpenID Connect Registration Specification:

Esta especificação define mecanismos para registrar dinamicamente *clients* OAuth 2.0 com *Authorization Servers* (servidores de autorização). Pedidos de registro

Área do / **Visão Geral do Ecossistema**



identifier para ser usado no *Authorization Server* e os valores de metadados registrados para o *client*. O *client* pode então usar esta informação de registro para se comunicar com o *Authorization Server* usando o protocolo OAuth 2.0. Esta especificação também define um conjunto de campos de metadados do *client* e valores para os *clients* usarem durante o registro.

[RFC7592](#): Esta especificação define métodos de gerenciamento de *dynamic client registration* (registros de cliente dinâmico) do OAuth 2.0 para casos de uso em que as propriedades de um *client* registrado necessitam ser alteradas durante a vida do *client*.

As especificações acima são especificações básicas cuja leitura obrigatória sustenta o framework de confiança do Open Insurance Brasil. Entretanto, eles ainda são insuficientes para atender a todos os requisitos e princípios descritos anteriormente.

OpenID Financial Grade 1.0: Baseline

Este perfil herda todas as obrigações do OpenID Connect Core

Reconhecendo as ameaças e riscos restantes que não foram tratados pelo OpenID Connect Core, o grupo de trabalho Financial Grade tem como foco criar uma especificação que visa identificar e endereçar os pontos fracos na especificação OpenID Connect, essencialmente criando um perfil para casos de uso que exigem alto nível segurança.

O perfil Baseline foi originalmente planejado para ser mais facilmente implementado por clients e OpenID Providers às custas de alguns elementos de segurança e, como tal, não oferece o mesmo grau de proteção contra violação de solicitação e resposta.

OpenID Financial Grade 1.0: Avançado

Este perfil herda todas as obrigações do OpenID FAPI 1.0: Baseline

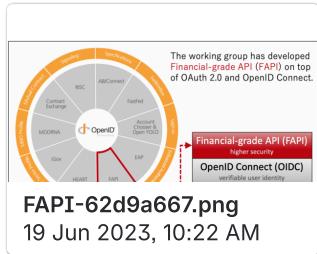
O [FAPI 1.0: Advanced profile](#) é atual padrão ouro para API Security, fornecendo um framework de especificação que foi usado como ponto de partida para a criação de uma especificação para o Open Insurance Brasil.

Este padrão especifica um perfil de segurança avançado do OAuth que é adequado para ser usado para proteger APIs com alto risco inerente. Os exemplos incluem

Área do / Visão Geral do Ecossistema



especifica os controles contra ataques, como: violação de solicitação de autorização, violação de resposta de autorização, incluindo injeção de código, injeção de estado e phishing de solicitação de token.



Sobre o uso de JARM

O suporte ao JARM é opcional aos transmissores e detentores de contas (ASPSP) e, portanto, as instituições que optarem pelo uso do JARM devem, no processo de certificação de segurança, atestar também o suporte a outro profile que não considere o uso do padrão JARM, ou seja, deve também se certificar com um dos profiles listados na tabela a seguir.

Perfil da certificação OIDF

BR-OB Adv. OP w/ MTLS

BR-OB Adv. OP w/ Private Key

BR-OB Adv. OP w/ MTLS, PAR

BR-OB Adv. OP w/ Private Key, PAR

