Open Banking

Secure Sharing of your financial data with OpenID Connect protocol

Ciro Bologna
Principal Access Management Engineer

What is Open Banking?

Open Banking is a brand new, **secure** way for consumers including small businesses to **share** information, allowing new and existing companies to offer super-fast payment methods and innovative banking products and applications.

Open Banking doesn't mean you are going to share your password and let someone else enter your bank account.

The customer is at centre of this ecosystem, and explicit consent is required to share for a limited amount of time the account or transactional data to other applications for different use cases

Source: openbanking.org.uk

Where is the idea coming from?

Talking about Open Banking you will often hear reference to **PSD2**. It is the second Payments Services Directive which modernises **European** payment regulation businesses in the EU to have greater control over their financial data.

A bank regulatory change has triggered the discussion on how to make easier for both established large banks and new financial services providers to offer new products, services, and a better choice for the customers, and they agreed on creating a standard **API** to be accessed and consumed by software developers.

It has been adopted first in the UK, then in EU but also Australia, Japan, Singapore etc.

Why would you share your financial data? 1/2

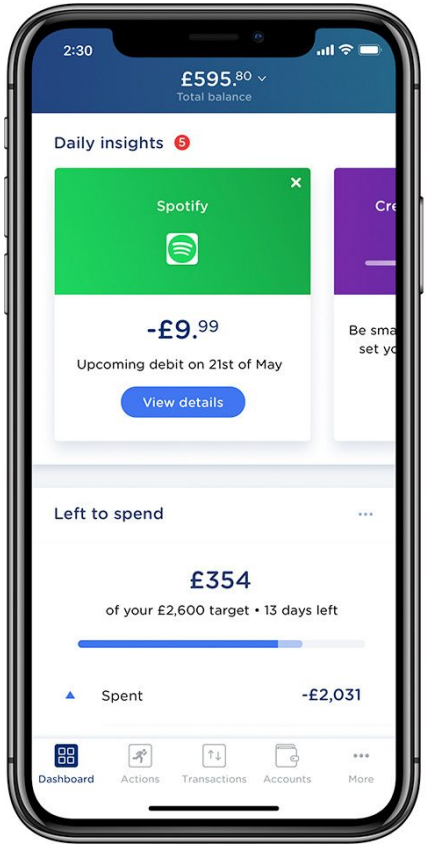
Many applications have already used Open Banking API to achieve new use cases for

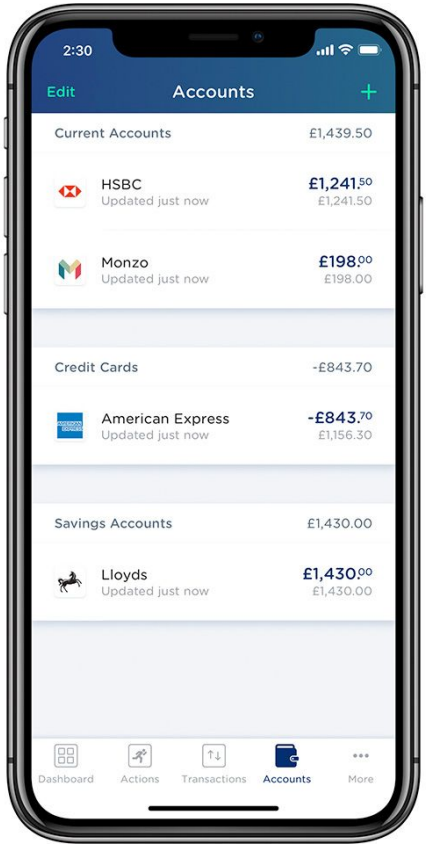
- For customers
  - personal finance management
  - a single view of all accounts in one place
  - debt management tools
- For businesses
  - tools to help with accounts
  - tools to help with cash flow management
  - tools to help with getting better loan

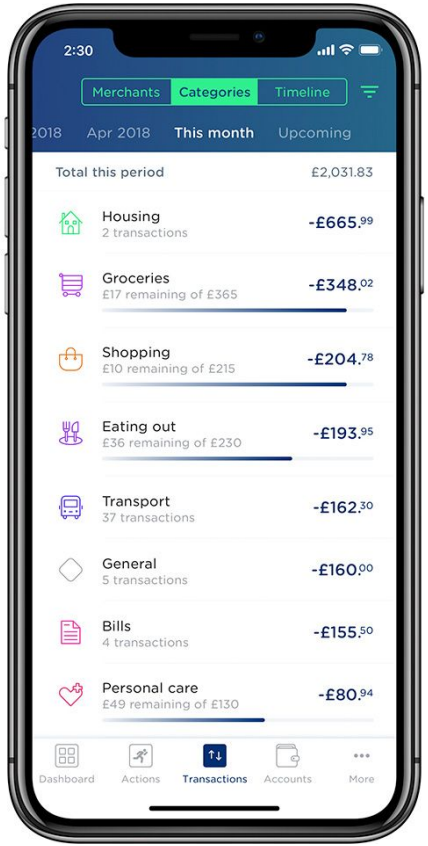
Why would you share your financial data? 2/2

Yolt

has been one of the first account aggrega tor







Why is Open Banking secure? 1/2

In order for a financial service provider like Yolt to be fully authorized through PSD2 to use Open Banking API, the Third Party Provider (TPP) have to be registered as one or both of the following

- **AISP** Account Information Service Provider
  - ask for permission to grab data about transaction
- **PISP** Payment Initiation Service Provider
  - ask for permission to make payments on the customer's behalf

Security Profiles have been developed together with the Open ID foundation and cover 3rd party on-boarding, re-direct and decoupled flows

- Open Banking Security Profile
- CIBA profile
- Financial-Grade API (FAPI) Profile
- Dynamic Client Registration (DCR) Specifications

Both banks and TPP **must** strictly follow the implementations in order to be compliant and avoid fines.

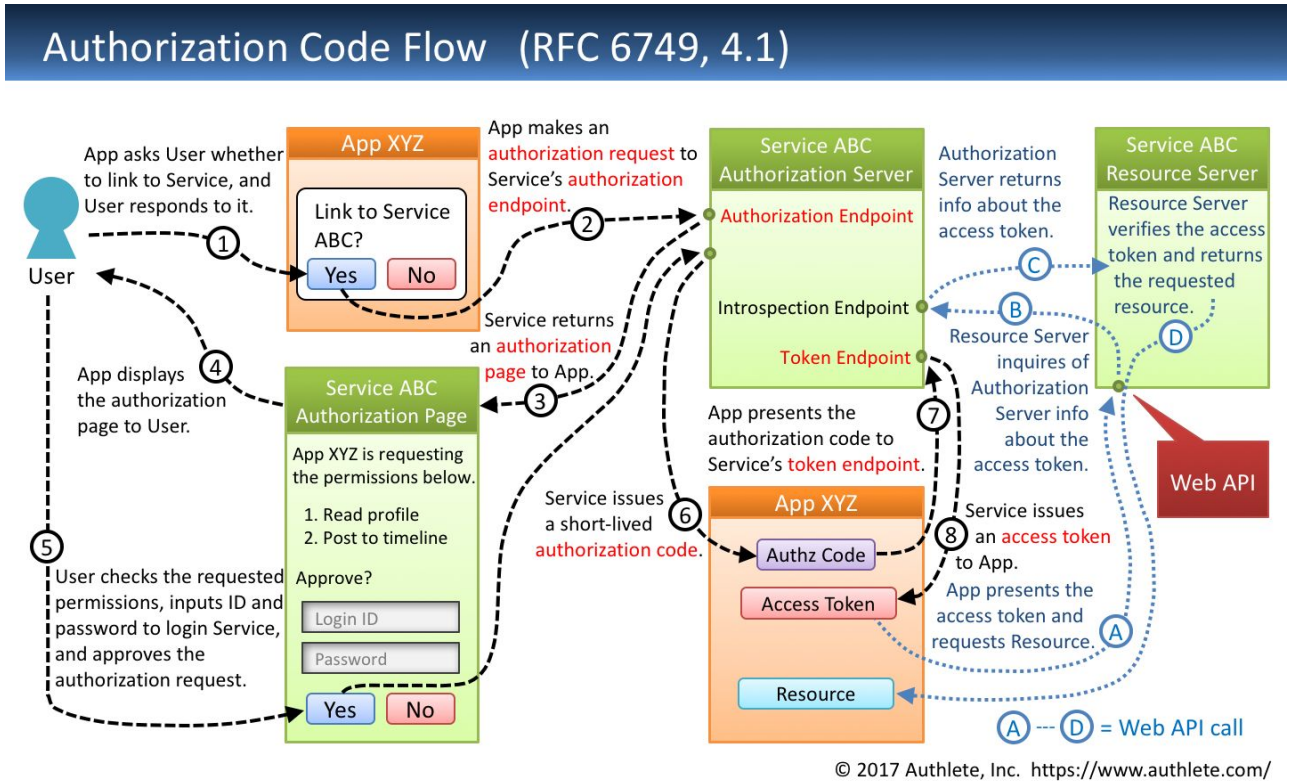
Why is Open Banking secure? 2/2

The following is a list of specifications that you should read at least once before the FAPI specification.

- RFC 6749 — The OAuth 2.0 Authorization Framework
- RFC 6750 — The OAuth 2.0 Authorization Framework: Bearer Token Usage
- RFC 7515 — JSON Web **Signature** (JWS)
- RFC 7516 — JSON Web **Encryption** (JWE)
- RFC 7517 — JSON Web Key (JWK)
- RFC 7518 — JSON Web Algorithms (JWA)
- RFC 7519 — JSON Web Token (JWT)
- RFC 7523 — JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants
- RFC 7636 — Proof Key for Code Exchange by OAuth Public Clients
- OpenID Connect Core 1.0
- OpenID Connect Discovery 1.0
- OpenID Connect Dynamic Client Registration 1.0
- OAuth 2.0 Multiple Response Type Encoding Practices
- OAuth 2.0 Form Post Response Mode

Credits here

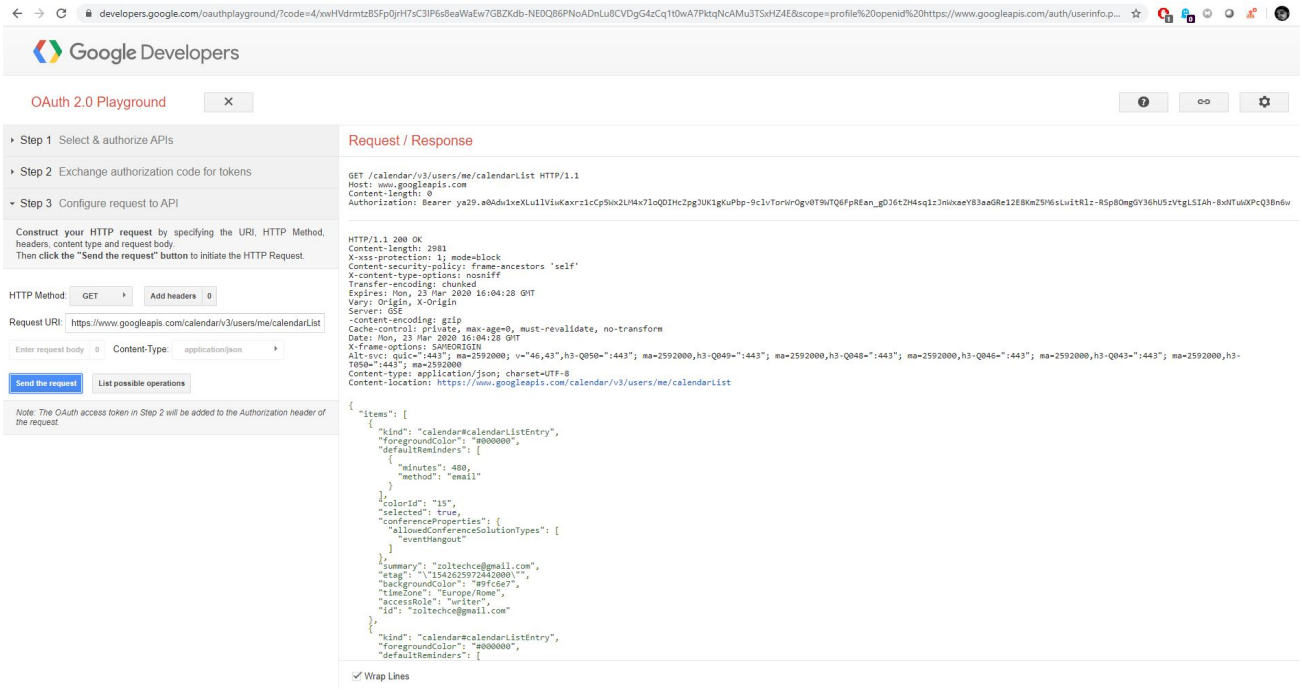
OpenID Connect: grant_type=code



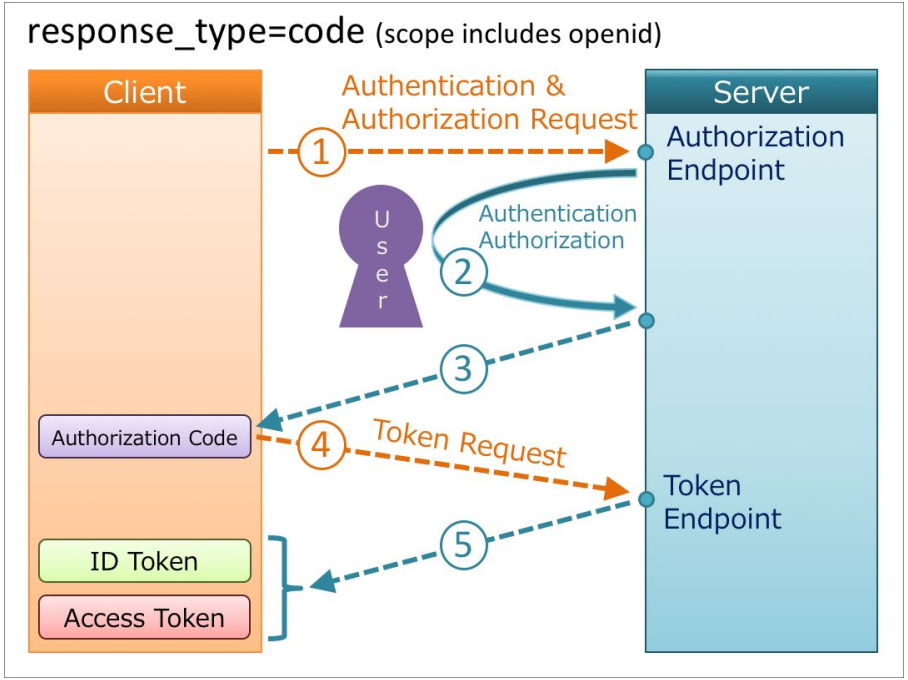
https://medium.com/@darutk/new-architecture-of-oauth-2-0-and-openid-connect-implementation-18f408f9338d

Google OAuth Playground Demo

https://developers.google.com/oauthplayground/
https://accounts.google.com/.well-known/openid-configuration
https://www.googleapis.com/oauth2/v3/certs



OpenID Connect: grant_type=code



Different grant_type available to cover multiple use cases accordingly to the application type.

ID token is a JWT issued by the Authorization Server that asserts the user identity

Access Token can be a JWT that authenticates the access to some resources accordingly to the scope chosen during the Authorization Request

https://medium.com/@darutk/diagrams-of-all-the-openid-connect-flows-6968e3990660

Hybrid Flow for Open Banking

Financial API Working Group of OpenID Foundation has defined Financial API (FAPI). When a client application complying with the FAPI specification makes a request for an access token for write operations, the value of response_type of the request must be either **code id_token** or **code id_token token**

/authorization endpoint is invoked by User Agent (web or mobile)

/token endpoint is invoked by a server

It requires 2 way **TLS** using a certificate issued by the Open Banking **Certificate Authority**

It requires **authentication** using credentials provided by the bank's **developer portal** to the TPP e.g. client_secret_basic (deprecated), private_key_jwt, tls_client_auth etc.

Revolut API example

Each financial institution implementing the Open Banking has a Developer Portal

- showing how to register for Open Banking
- providing a Sandbox to start testing the API
- listing down the different request and response for each of the API

Basically all you can do once you got an access_token.

Always start from the well-known endpoint

Account and Transaction API manages the consent and read the account balances and transactions of the customer

Payment Initiation API specification manages the domestic payment consents

Confirmation of funds allowing a Card Based Payment Instrument Issuer to check if funds are available

Revolut API