Sandbox Overview

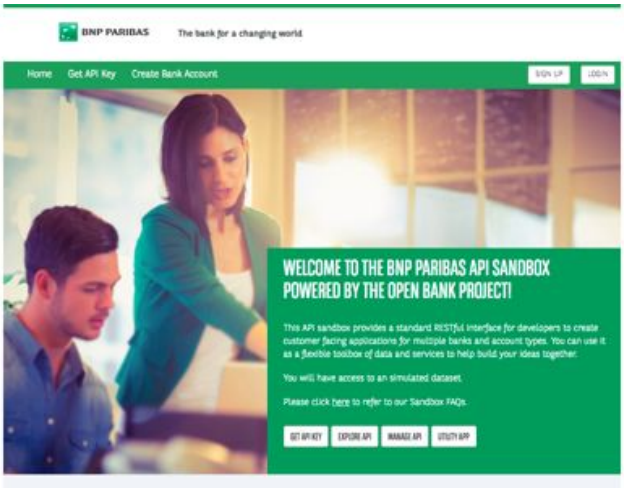
Open Bank Project provides a fully operational and self contained sandbox environment deployed either in the Cloud or on premises and using test data. This sandbox environments mimic the live environment with a **real world persistent data model** complete with constraints. For instance a payment debited on account A will be credited on account B. The sandbox environment represents a great training ground to experiment with TPPs and encompass everything needed to run a successful hackathon or Open Innovation programme.

1. API Catalogue

a) Catalogue Overview - Open Bank Project offer a standardized API catalogue of over 200 endpoints. Current capabilities (V3.0.0) include PSD2 requirements and functionalities beyond. For a full list of API categories see:

PSD2 Requirements	Beyond PSD2
• Banks	• KYC & Customer Onboarding
• Entitlements	• Branches / ATMs / Products
• Users & Customers	• CRM events
• Accounts	• Metadata Management
• Counterparties	• Capital Markets (FX, Debt, Equity, Basket, etc.)
• Transactions	• Customer Messages (e.g. for chatbots)
• Payments & Transaction Requests	• Card Management
• Strong Customer Authentication	• Data Analytics

b) Data Analytics APIs - Open Bank Project provides a set of APIs dedicated to enabling complex data analysis leveraging large data sets provided by the client. These APIs differ from the regular customer-facing APIs as they give “fire hose” and / or statistical only access to data and are suitable for data analytics applications such as credit scoring and fraud detection. Using these APIs, developers can apply full text search and advanced row based and statistical queries using a RESTful API that resembles the Elastic Search read-only APIs. For these APIs to be enabled, the client should supply a large dataset of real but anonymised data. The client controls who has access to these APIs so they can be restricted to internal developers.



c) Documentation - Each API endpoint is well documented and can be tested. Developers can use the provided API Explorer to discover and try out the APIs against the sandbox. See full list of APIs here https://apiexplorersandbox.openbankproject.com/

2. Developer Portal

Open Bank Project offers a white-labeled API portal where TPPs can register, deregister, request access for specific APIs. Developers apply for an API key granted by the client and access API documentation, SDKs and other tools through this one-stop-shop. The portal supports multiple organisations and each organisation included in the platform can have its own branding.

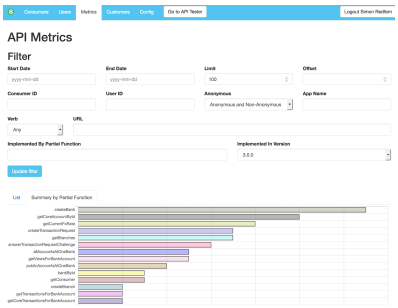
3. SDKs & Code Samples

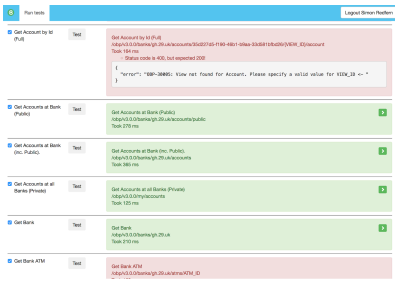
OBP sandbox offers a superior developer experience which boosts productivity by providing SDKs (Software Development Kits) & Code Samples developer can re-use in their programming language of choice. With these tools, developers can access transactions or make a payment in under few minutes.

The SDKs are Open Source (Apache, MIT or BSD style licenses) and regularly updated. They handle authentication (OAuth + Direct Login) and are easily accessible through the developer portal. Supported languages/platforms include: iOS, Android, Python, Django, Node, C#, PHP, Javascript.

4. Administration & Monitoring

The sandbox also provides an administrative interface to the client staff through the OBP API Manager. The OBP API Manager is a web application to view and manage the Apps and Users consuming the API sandbox and monitor API usage. Some of the features of the API Manager are:





- List applications registered on this sandbox and their description
- Revoke / Grant access to selected applications
- Search for Users and grant / revoke entitlements to API Roles (e.g. CanSeeUsers Role)
- View Configuration of the API
- Upload different datasets
- Monitor usage of APIs - monitor usage per API endpoint and per App/Consumer, filter by date etc. etc.
- Ability to draw up performance statistics and regulatory reports (e.g. Fraud reporting) and view data for billing.

5. Authorisation & Consent Management

Access to protected resources by a third party happens only with end-user consent and following the RTS guidelines. Customer credentials are always safely stored and are never disclosed to any third party. OBP uses OAuth, an industry standard, to handle this process.