Open Bank Project
Francisco Montenegro
Dylan Thiam

17.03.2021

La Guía Completa de las API para las Instituciones Financieras

El ecosistema de los servicios financieros bulle con palabras como "API" y "OAuth", los equipos de TI se preparan para lo peor, las partes interesadas agachan la cabeza pensando qué deben hacer con toda esta información.

Pues bien, no busques más. Hemos elaborado este artículo para explicar de principio a fin qué es una API y cómo encaja en Open Banking y Open Finance. Desde lo más básico hasta la monetización de las APIs, lea a continuación para empezar a aprender o utilice los enlaces para ir a secciones específicas.

Lo básico: ¿Qué es una API?

Las Interfaces de Programación de Aplicaciones (**Application Programming Interface** o **API**) son interfaces de software que permiten compartir datos entre sistemas y dentro de ellos. Las API permiten que dos componentes de software (o aplicaciones) se comuniquen/interactúen sin tener que saber cómo está implementado el otro, lo que acelera enormemente el desarrollo de aplicaciones.

Las APIs están en todas partes.

Cuando introduces **www.google.com** en la barra de búsqueda, estás haciendo una petición a la base de datos de Google para recuperar la página web, que la API te envía como respuesta.

Haciendo una analogía, las API son como los mayordomos. Toman tu pedido **(solicitud)**, van a la cocina para obtener tu orden, y luego sirven la comida **(respuesta)** a tu mesa.

La aplicación Uber, por ejemplo, utiliza la API de Google Maps para mostrarte dónde está tu conductor. Los desarrolladores pueden utilizar las API para acceder de forma segura a los datos almacenados en su base de datos y utilizarlos para **crear sus innovadoras aplicaciones**.

Las APIs en los servicios financieros: Finanzas abiertas

Las APIs han entrado recientemente en el espacio de los servicios financieros. Las primeras normativas que obligan a compartir datos en el sector de los servicios financieros fueron la PSD2 en Europa y la Banca Abierta (Open Banking) en el Reino Unido, pero otros países no tardaron en seguir con sus propios regímenes de banca y finanzas abiertas.

Las API de Open Finance se utilizan para compartir los datos financieros de los clientes y otras funciones bancarias.

Las aplicaciones de ahorro, como Spendee, por ejemplo, pueden conectarse a las cuentas de los consumidores y les permiten ver sus gastos en tiempo real en lugar de teclear manualmente los gastos. Spendee lo hace llamando a la API para recuperar la información de la cuenta del cliente.

Los marcos normativos garantizan que este intercambio de datos sólo se produzca en un **contexto seguro y con el consentimiento del cliente**.

A veces, los reguladores incluso proporcionan directrices técnicas, de consentimiento o de experiencia de usuario para ayudar a los desarrolladores a diseñar APIs basadas en las mejores prácticas. Normalmente, estas directrices se denominan como **estándares API.**

Estándares API de banca abierta

Los estándares API dirigen la forma en que los bancos y las instituciones de dinero electrónico (IFPE) diseñan las API e interactúan entre sí. Algunos ejemplos de normas API de banca abierta son:

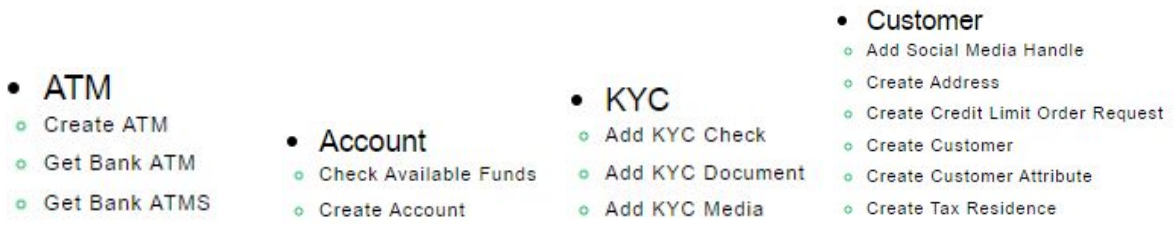
- Open Banking del Reino Unido
- Berlin Group NextGenPSD2 (Europa)
- CDR CX (Australia)

Los estándares de API son como planos que los desarrolladores pueden seguir al construir sus API. Estas directrices se basan en métodos probados y seguros. La definición de un marco común ahorra tiempo y dinero y garantiza que el sector bancario comparta datos de forma segura.

No todos los reguladores proporcionan directrices o normas, algunos lo dejan en manos del mercado.

APIs financieras abiertas - Ejemplos

A continuación se muestran algunos ejemplos de APIs financieras de nuestro sandbox de APIs.



Los desarrolladores interactúan con las APIs REST a través de los métodos de solicitud HTTP denominados GET, PUT, POST y DELETE, que les permiten acceder y utilizar los datos.

GET = Quiero leer estos datos/página web
PUT = Quiero actualizar o reemplazar la información
POST = Quiero crear una nueva entrada
DELETE = Quiero eliminar información

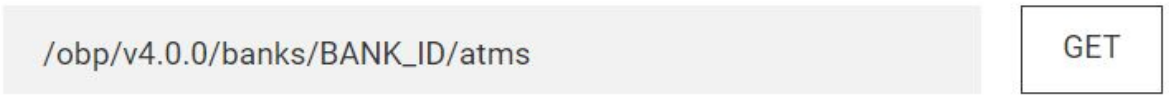
Por ejemplo, los desarrolladores podrían utilizar la API get ATMs para obtener una lista de cajeros automáticos y ayudar a los usuarios a encontrar el más cercano utilizando sus teléfonos.

Escenario 1: Leer (Read)
El Banco A quiere asociarse con el Banco B para permitir a sus clientes retirar dinero en los cajeros de ambos. Ambos bancos querrán incluir las ubicaciones de los cajeros automáticos de su socio en sus propias aplicaciones bancarias.

Para ello, pueden llamar al punto final de la API Get Bank ATMs y recibir una lista de ubicaciones de cajeros automáticos.

A continuación se muestra un ejemplo de lo que vería un desarrollador que creara una aplicación para cajeros automáticos antes de llamar a la API en nuestro sandbox:

(Sustituyendo BANK_ID por el ID del banco en el sandbox)



La API "obtiene" las ubicaciones de los cajeros automáticos y las entrega a la aplicación. En otras palabras, esta API le ayuda a solicitar permiso para leer (**read**) información.

Escenario 2: Read (Account Information Services)
El Banco A quiere que sus clientes puedan ver todas sus cuentas bancarias desde la aplicación bancaria nativa. El Banco A llama al endpoint Get Account by Id.

Ejemplo del Berlin Group:

Esta llamada proporciona el saldo y otros datos de la cuenta como

- IBAN
- BIC
- Moneda
- Tipo de producto
- etc.

A través de este punto final, el Banco A puede obtener información agregada de las cuentas, ofreciendo a los clientes una visión global de sus gastos.

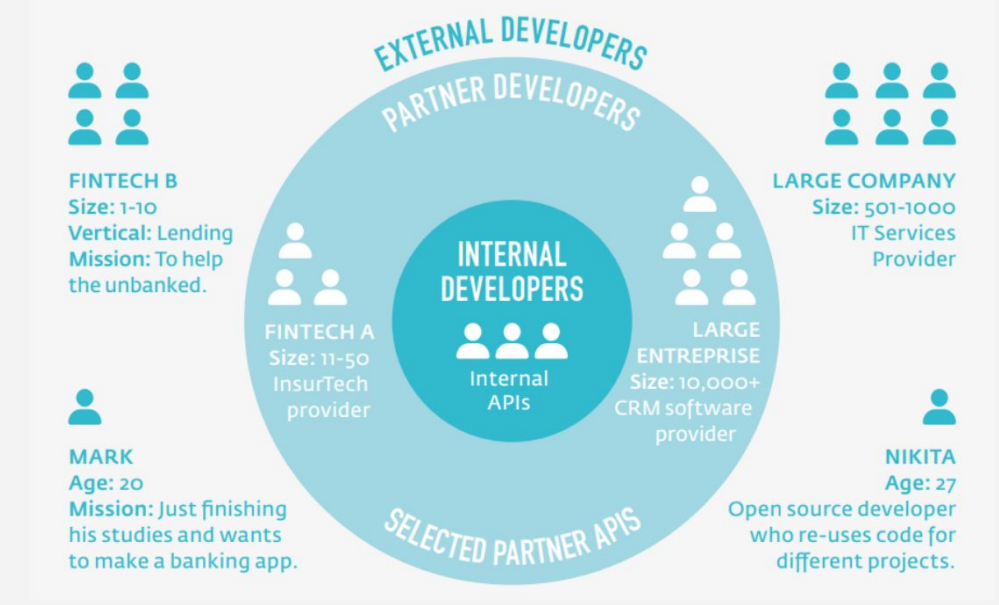
Tipos de API

En el contexto de la banca abierta existen normalmente tres tipos de API:

Internas: APIs privadas/cerradas (Internal APIs)
Las API internas sólo están disponibles para determinados empleados (desarrolladores) de la empresa.

De socios (Partner APIs)
Las API de socios están disponibles para determinados socios, pero no para desarrolladores externos. Por ejemplo, las API que se crean para necesidades específicas de los socios, como la integración de dos aplicaciones.

External APIs (Open APIs)
Las API externas están abiertas a desarrolladores ajenos a su organización y a su círculo de socios que quieran utilizar la API para crear, potenciar o mejorar aplicaciones nuevas o existentes. Los actores externos también pueden ayudar a las instituciones financieras a llegar a nuevos ecosistemas digitales compartiendo la API dentro de sus propias comunidades. Algunas de estas API deben ser abiertas y accesibles a los desarrolladores "certificados" debido a la normativa existente (PSD2 en Europa o Open Banking en el Reino Unido).



Estilos arquitectónicos de la API y formato de datos

Los estilos arquitectónicos de las APIs son un modelo para diseñarlas.

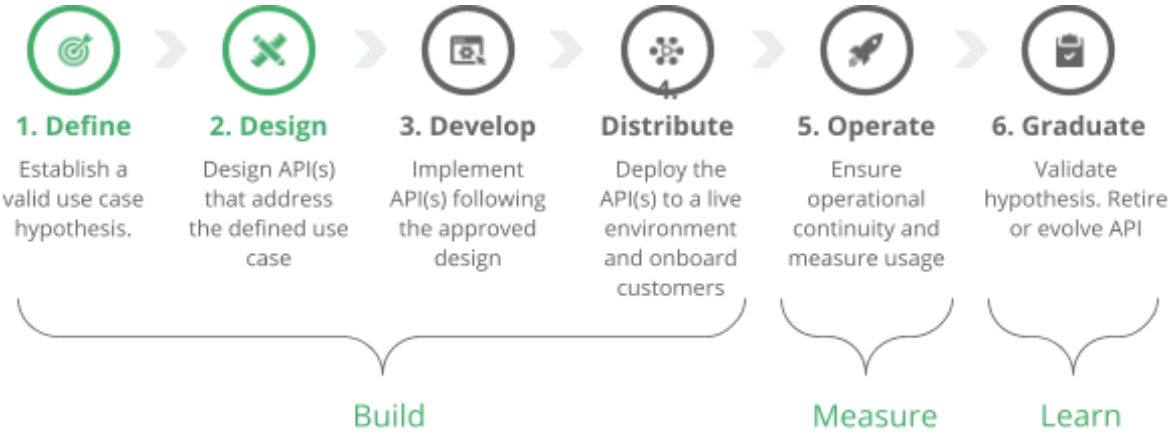
Hay varios estilos arquitectónicos para elegir, cada uno con sus propias ventajas y desventajas, pero normalmente se recomienda REST.

REST son las siglas de Representational State Transfer. Las APIs que se rigen por las reglas de REST se denominan RESTful y se consideran el protocolo estándar para las APIs web.

Los formatos de datos no son más que diferentes maneras de organizar los campos de datos. El formato de datos recomendado es JSON, ya que es ampliamente utilizado, y es tanto legible por la máquina como por el ser humano.

El ciclo de vida de la API

Cada API tiene un ciclo de vida. Como puede ver en la imagen siguiente, el ciclo de vida puede dividirse en tres fases: Construir, Medir, Aprender.



1. **Definir**

El equipo de la API analiza las necesidades técnicas y empresariales para definir un caso de uso válido.

2. **Diseñar**

El equipo decide los requisitos fundamentales de la API y aprueba las especificaciones de diseño y la documentación. El equipo debe esbozar:

- El lenguaje de la API,
- las normas de nomenclatura,
- el diseño,
- mensajería y
- arquitectura.
- Una vez que el equipo aborda estas preferencias, diseña las APIs que abordan el caso de uso definido.

3. **Desarrollar**

El equipo de API, es decir, los desarrolladores, codificarán las API de acuerdo con las especificaciones decididas utilizando herramientas de desarrollo.

En esta etapa del ciclo de vida, los desarrolladores realizan pruebas.

Testing demands careful attention. Developers should test functionality, performance and security of the API before publishing it in a live environment. Financial institutions usually use a sandbox to test APIs using realistic test data before going live.

4. **Distribuir**

Tras aprobar la API y decidir **cómo** se desplegará, el equipo de la API puede desplegarla en un entorno real y empezar a incorporar a los desarrolladores.

5. **Operar**

En esta fase, el equipo de la API debe garantizar la continuidad operativa y medir el uso de la API. Esto ayudará en la siguiente fase a la hora de elegir si se mejora o se retira una API.

6. **Graduar**

En esta fase, el equipo de la API valida su hipótesis. Pueden utilizar los datos de uso de la API para mejorarla o retirarla.

¿Qué es la gestión de API?

La gestión de APIs es el proceso de diseñar, construir, probar, publicar, mantener y analizar las APIs en un entorno seguro. En otras palabras, la gestión de todo el ciclo de vida de la API.

Las herramientas de gestión de APIs pueden comprarse o construirse internamente, pero normalmente una pila eficaz tiene las siguientes características, interfaces y capacidades:

- ✓ Una herramienta para agilizar el diseño de la API
- ✓ Una pasarela de API que garantice la autorización y la seguridad
- ✓ Un catálogo de APIs para mostrar sus APIs a la comunidad externa
- ✓ Análisis de la API para medir y mejorar continuamente el rendimiento

Herramienta de diseño de API

La mayoría de las soluciones ofrecen APIs listas para usar, pero rara vez son suficientes. Las nuevas oportunidades y casos de uso se pueden desbloquear a través de nuevas APIs. La herramienta de diseño de APIs debe ser capaz de crear nuevas APIs en pocos minutos y debe ser fácil de usar para el equipo no técnico.

API Gateway

Las pasarelas de API son herramientas para gestionar y controlar las APIs expuestas por el Portal de Desarrolladores de una institución, actuando como una puerta de entrada/ventanilla única para el programa de APIs del banco

Catálogo de APIs

El Catálogo de APIs o Marketplace es el lugar donde se exponen las APIs. Los desarrolladores lo utilizarán para saber qué APIs y servicios ofrece usted.

Análisis de la API

Los análisis de las API son indispensables. Disponer de una herramienta de análisis robusta le ayudará a entender su progreso, a mejorar sus APIs y a identificar los problemas antes de que se conviertan en un problema más serio.

Como podrás saber, las APIs son herramientas muy valiosas. Son muy eficaces para obtener y modificar información. Pero el sector de los servicios financieros maneja información sensible, que no debería caer en manos de los ciberdelincuentes, ni de nadie. Por eso, las normativas sobre finanzas abiertas de todo el mundo hacen hincapié en la necesidad de una seguridad eficaz de las API.

Seguridad de la API

Dado el nivel de información sensible, se presta mucha atención a los mecanismos de seguridad adecuados para el sector de los servicios financieros. En el lenguaje de las API, la seguridad suele traducirse en:

- **Mecanismos de autorización, autenticación y consentimiento**
- Sistemas de control de acceso
- Seguridad de la capa de transporte (Transport Layer Security)

Consentimiento del cliente

El consentimiento es el acto de aceptar la forma en que el proveedor procesa los datos. Los clientes consienten que la empresa de tecnología financiera lea su lista de transacciones para prestarles un servicio.

La normativa sobre banca abierta de todo el mundo exige que los datos se compartan únicamente con el consentimiento explícito del cliente. Esto significa que las instituciones financieras tienen que ofrecer las herramientas que permitan a los clientes optar por dar su consentimiento.

Cuando un cliente decide añadir una cuenta bancaria a una aplicación fintech, esto es lo que debería aparecer en la pantalla:

"Doy mi consentimiento para compartir la información de mi cuenta con <FinTech> para recibir los servicios que he solicitado".

Tras obtener el consentimiento del cliente, el proveedor de la API debe gestionar y administrar su ciclo de vida. En otras palabras, debe emplear una gestión eficaz del consentimiento.

Las diferentes normativas de Open Banking pueden prescribir cómo debe ser esta arquitectura. Por ejemplo, el Open Banking del Reino Unido es más estricto que otras normativas y tiene un flujo complejo. De hecho, en el lenguaje de las normas del Reino Unido, el consentimiento no es consentimiento hasta que se autoriza, razón por la cual utilizamos el término "Intención" a continuación.

Ejemplo de flujo de consentimiento de Open Banking en el Reino Unido

1. Obtener el consentimiento del cliente: El cliente expresa su deseo de compartir sus datos
2. Crear la "intención": Con el consentimiento del Consumidor en la bolsa el TPP puede ahora llamar a la API de Consentimiento y solicitar el Token de Acceso
3. El cliente es redirigido al Servidor de Autorización
4. El cliente se autentifica y autoriza el consentimiento
5. Cambia el código de autorización por el token de acceso
6. Obtiene los datos de la cuenta

Vea el diagrama completo aqui:
https://static.openbankproject.com/uk-auth-consent-flow/fapi-rw.html

Como se puede imaginar, preguntar a un cliente si da su consentimiento para compartir sus datos crea fricción en la experiencia del usuario, que es otro de los pilares de la banca abierta: Para crear una experiencia de usuario sin fricciones, las instituciones necesitan un mecanismo de consentimiento que

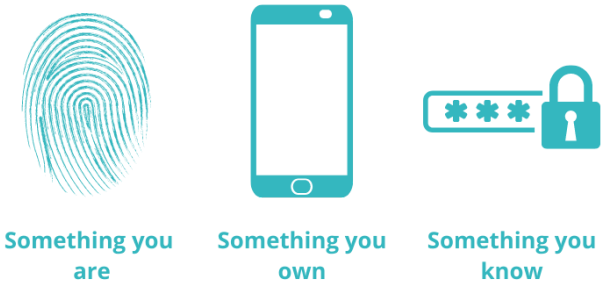
- capte el consentimiento en tiempo real
- se conecte sin problemas y de forma segura a los sistemas existentes
- genera recibos de consentimiento
- ofrezca plataformas fiables, escalables, flexibles y centradas en el usuario final
- permita a los clientes aceptar y revocar fácilmente el consentimiento

Autenticación

La **autenticación** es la forma en que los clientes pueden demostrar su identidad y, por lo tanto, demostrar que tienen derecho a autorizar a la tecnología financiera a acceder a sus datos (o a los desarrolladores a demostrar que pueden realizar una llamada específica a la API).

En la UE, el consentimiento tiene que ser validado a través de la Strong Customer Authentication o SCA (Autenticación Fuerte de Clientes). Tal y como se define en las RTS de la ABE, la SCA es una autenticación basada en el uso de dos o más elementos que son independientes.

El método se basa en la **autenticación multifactorial**, que requiere que los usuarios aporten dos o más pruebas: **conocimiento** (por ejemplo, la contraseña), **inherencia** (identificación biométrica, por ejemplo, la huella dactilar) y **posesión** (por ejemplo, el teléfono). En otras palabras, algo que se sabe, algo que se es y algo que se posee.



En el flujo de autenticación del Reino Unido, se envía al usuario una contraseña de un solo uso (OTP) a través del método SCA definido, que suele ser el correo electrónico o el móvil, y el usuario puede confirmar el código en la interfaz, demostrando así su identidad.

La autenticación de 4 factores es el mismo mecanismo, pero también incluye factores de localización. Los teléfonos inteligentes con dispositivos GPS pueden proporcionar ubicaciones precisas y disminuir las posibilidades de ser engañados por los ciberdelincuentes.

Autorización

La autorización es el acto de dar permiso oficial a un proveedor de servicios para acceder a los datos de la cuenta y las transacciones. Usted autoriza a una tecnología financiera a acceder a la información de su cuenta.

Existen varios mecanismos de autorización, pero no todos son adecuados para los servicios financieros.

OAuth 2.0 es un marco de autorización de estándar abierto que permite a las aplicaciones obtener un acceso limitado a la información de la cuenta de un cliente sin revelar información sensible como las credenciales del cliente.

El marco OAuth permite esencialmente a los usuarios autentificados dar a otro servicio un **token** de autentificación de acceso limitado para la autorización de acceso a los recursos.

¿Qué son los Tokens?

En lugar de utilizar contraseñas de cliente, OAuth utiliza tokens para acceder al servidor.

- **JWT:** JSON Web Token, un estándar abierto basado en JSON propuesto por la Internet Engineering Task Force (IETF) para la creación de tokens de acceso que permiten la propagación de la identidad y los privilegios.
- **Tokens de acceso:** Las credenciales utilizadas por las empresas FinTech para acceder a la información del cliente en la base de datos del banco.
- **Tokens de registro:** Identificadores alfanuméricos únicos que permiten a las FinTechs registrarse en los bancos.
- **Token de actualización:** Utilizado para obtener un nuevo token de acceso cuando el actual caduca.

Access Control

Dependiendo del stack de gestión de la API, a menudo encontrará diferentes sistemas de control de acceso.

Por ejemplo, a nivel de una **institución**, debería haber un permiso que diera acceso a diferentes funciones y APIs. Sin este permiso, los usuarios no deberían poder realizar determinadas llamadas a la API y suele llevarse a cabo con tokens OAuth2, basic Auth, etc.

En segundo lugar, a nivel de **recursos**. Los clientes deberían poder decidir quién puede acceder a sus datos y también poner un límite a la cantidad y el tipo de datos a los que puede acceder el tercero.

Transport Layer

Transport-Layer Security (TLS) es un protocolo criptográfico diseñado para garantizar la seguridad de la información comunicada a través de una red informática. Es un mecanismo que utilizamos para realizar conexiones seguras con los servidores web.

En cambio, las conexiones de servidor a servidor se basan en TLS mutuo (mTLS) para la autenticación mutua.

Es mucha información para asimilar. Tómate un tiempo para repasar lo que hemos hecho hasta ahora y empieza a entender cómo funcionan las APIs desde una perspectiva técnica. En la próxima actualización, cubriremos el lado comercial de las API: Casos de uso, la API como producto (API-as-a-Product), la estrategia de la API y la monetización de la API.

Si no puedes esperar a aprender más sobre las APIs, ve a nuestro sandbox y echa un vistazo a las APIs y sus respuestas de prueba.