

Guía Tink

Conectividad en el open banking

— Qué se necesita para conectarse a las APIs de open banking
y por qué no es tan simple como parece

tink'
A Visa Solution

A priori, conectarse a una API de open banking puede parecer una tarea sencilla. Desde que la legislación PSD2 entró en vigor en 2018, los ASPSPs (Account Servicing Payment Service Providers) de toda Europa están obligados a proporcionar acceso gratuito a los datos de los clientes a través de APIs. Cabe esperar, que una vez que te hayas conectado al banco o institución financiera en cuestión, la conexión debería funcionar sin problemas hasta el final. ¿Verdad?

Pues no.

Lo que falla en esta ecuación es el simple hecho de que los ASPSPs no obtienen beneficio económico por proporcionar acceso a los datos a través de las APIs. Si bien puede ser una inversión a largo plazo en la idea de un sistema financiero más abierto, no genera beneficios aquí y ahora. Esto significa que los equipos de ASPSPs encargados de administrar estas APIs, a menudo, no cuentan con suficiente personal.

Las plataformas de open banking como Tink forman parte de este nuevo ecosistema. Trabajan junto con los ASPSPs para monitorear continuamente sus conexiones, encontrar errores, informar de problemas y comunicarse con sus equipos de ingeniería de manera regular. Esto supone un desafío operativo y técnico, que requiere de importantes inversiones en tiempo, personas e infraestructura.

Esta guía explica todo el proceso y muestra por qué conectarse a una API de open banking es mucho más que realizar la conexión inicial.



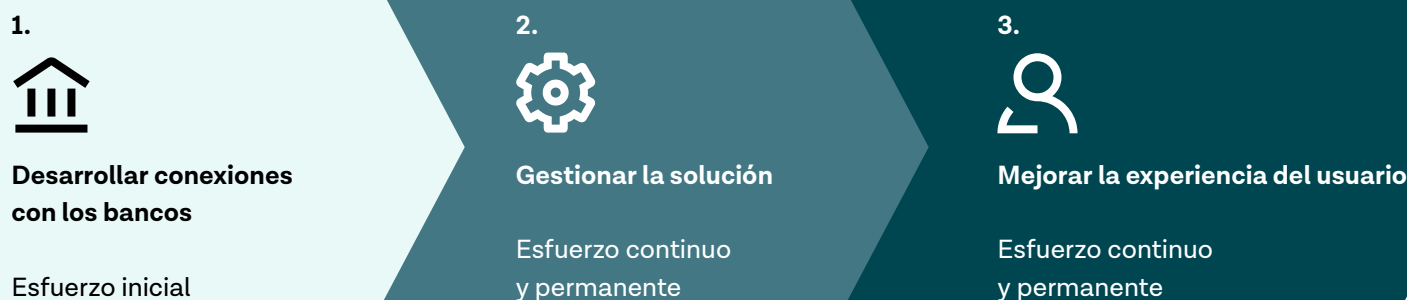
Qué encontrarás en esta guía

¿Qué significa realmente conectarse a las APIs de open banking?	4
1. Desarrollar conexiones con los bancos	5
2. Gestionar la solución	9
3. Mejorar la experiencia del usuario	13
Caso de estudio	16
Impulsando a la industria	19
Conclusión	22

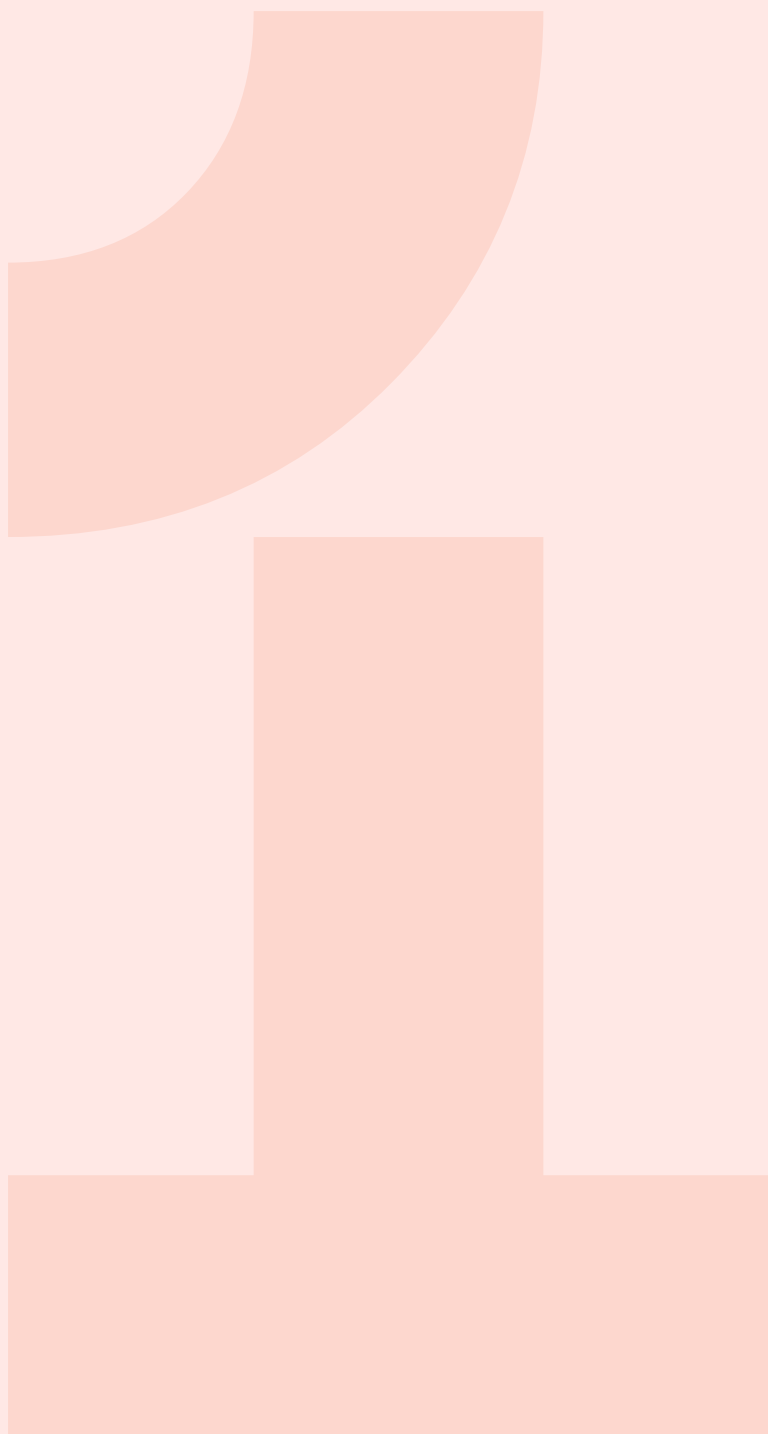
¿Qué significa realmente conectarse a las APIs de open banking?

Desarrollar la conectividad en varios países es un esfuerzo complejo que requiere importantes inversiones, especialmente en ingeniería, operaciones y asuntos legales. Para explicar esto correctamente, usaremos el ejemplo hipotético de un proveedor externo o Third Party Provider (TPP – por sus siglas en inglés) que se conecta a un ASPSP (Proveedores de Servicios de Pago de Servicios de Cuentas) en toda Europa. Analizaremos el proceso de optimización de conexiones a APIs bancarias, y te mostraremos que, conectarse a un banco, es solo el primer paso en la cadena de valor.

Conexión a una API de open banking

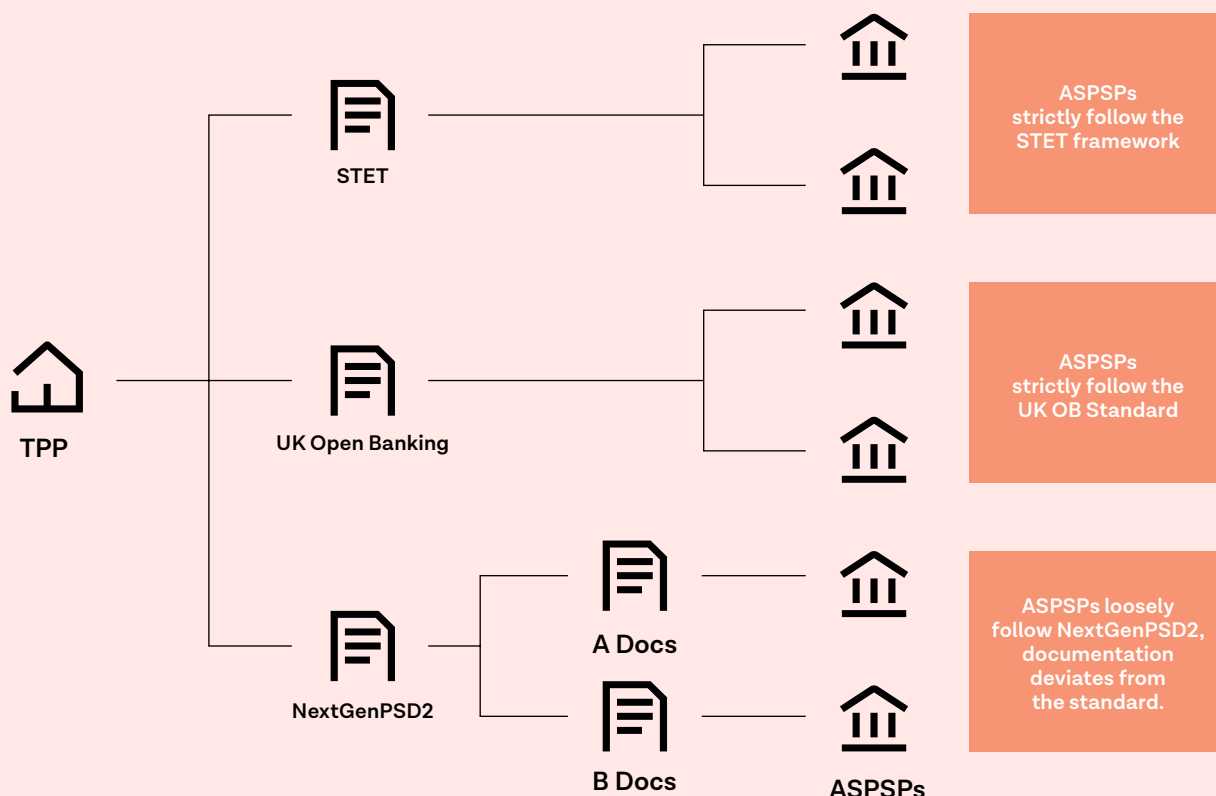


Desarrollar conexiones con los bancos



1.1 Comprensión de las normas europeas

Conectarse a una API de open banking exige un conocimiento profundo de los estándares que utilizan los bancos en diferentes países. En Europa Occidental, hay tres marcos generales:



STET: El marco de la API STET PSD2 se utiliza principalmente en Francia y es más estricto que el marco NextGenPSD2. La principal diferencia radica en el protocolo de solicitud de la firma, que se utiliza para validar que la información no ha sido alterada por el TPP.

Open Banking del Reino Unido: El Estándar de Open Banking del Reino Unido es el menos flexible, y la mayoría de los ASPSPs de UK lo implementan de manera casi directa con variaciones muy pequeñas. Este es el estándar más maduro ya que ha existido desde 2018, y ha sido testado exhaustivamente por cientos de TPPs. Además, su desarrollo e implementación ha sido monitoreado por la CMA y la FCA.

NextGenPSD2: El marco estándar de acceso a la cuenta (XS2A) NextGenPSD2 del Grupo de Berlín proporciona una vista arquitectónica de la API y permite una implementación flexible, donde los ASPSPs tienen la posibilidad de desviarse del estándar e implementarlo de acuerdo con sus propios requisitos. Aunque el Grupo de Berlín exige que las ASPSPs envíen solicitudes de cambio al comité que rige el marco, desafortunadamente esto rara vez se hace. En su lugar, esto ha propiciado una alta fragmentación de la implementación del estándar y un alto grado de variación entre las APIs de open banking. Este es el marco más común en Europa.

1.2 Registro en los ASPSPs

El segundo paso es registrarse en los ASPSPs y esto se puede hacer a través de registros manuales o dinámicos.

Los registros manuales requieren comunicación entre el TPP y el ASPSP, como registrarse en el portal para desarrolladores, crear una aplicación o enviar una y otra vez correos electrónicos a los ASPSPs para obtener acceso. Este proceso puede tardar en completarse desde unos días hasta meses, dependiendo del estado de la API PSD2. Lamentablemente, los registros manuales es lo más habitual en Europa y solo alrededor del 15% de los ASPSPs europeos ofrecen registros dinámicos.

Los registros dinámicos se realizan a través de una API y, si se realizan correctamente, el ASPSP registra el TPP automáticamente. Registrarse dinámicamente requiere una gran inversión inicial pero es altamente escalable, lo que permite el registro automático sin ningún esfuerzo adicional.



Tink ha invertido importantes recursos en la construcción de herramientas internas de registro dinámico, que nos permiten conectar y operar con diferentes APIs de registro, y dar acceso a nuestros clientes casi al instante.

1.3 Hacer la conexión

En teoría, el proceso de establecer una conexión es relativamente sencillo, ya que requiere que el TPP siga la documentación publicada por el ASPSP. La realidad, sin embargo, puede ser mucho más compleja.

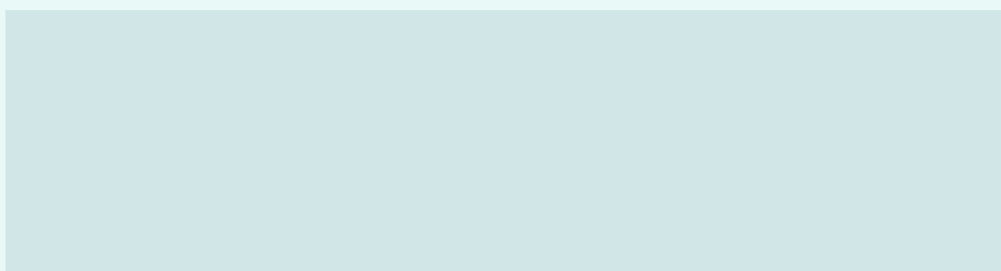
Los desafíos de conectarse a las APIs de open banking son diferentes para cada ASPSP y para cada país. Algunos ASPSPs son relativamente fáciles de conectar, mientras que otros requieren una inversión de tiempo sustancialmente mayor.

Afortunadamente, en la actualidad, la mayoría de las APIs de open banking han madurado hasta el punto en el que este tipo de inversiones ya no son necesarias y se pueden conectar mucho más rápido. En cualquier caso, estas son algunas de las acciones que los TPP deberían considerar:

- Establecer un equipo dedicado a comunicarse con el equipo de soporte del ASPSP cuando su documentación no sea clara o esté desactualizada.
- Familiarizarse con las especificaciones técnicas, tanto locales (específicas de ASPSP o del mercado: especificaciones de API en el Reino Unido) como más amplias (estándares más amplios, por ejemplo, métodos JWT). Esto ayudará a los desarrolladores a comprender los requisitos subyacentes de los programas que se están utilizando y resolver errores rápidamente.
- Diseñar una arquitectura central flexible para dar soporte a una variedad de conexiones ASPSP. Los estándares técnicos mencionados en la sección 1.1 proporcionan una base sobre cómo deben de ser diseñadas las API de open banking, pero la configuración para obtener acceso a la cuenta depende del ASPSP. La estructura subyacente es extremadamente importante, ya que pequeñas alteraciones pueden afectar otras conexiones, lo que resulta en cambios significativos.
- Los TPPs deben admitir todos los métodos criptográficos para facilitar la experiencia de los usuarios y conectarlos según el estándar requerido por cada ASPSP. Por ejemplo, UK Open Banking requiere 5 métodos criptográficos diferentes que se utilizan ampliamente en los ASPSPs.
- Invertir en formación para los desarrolladores y ofrecerles información detallada de los estándares, sistemas y procesos. La cantidad de código necesaria para realizar estas tareas es costosa y aumenta con cada nueva conexión.

El primer gran cliente de Tink utilizando APIs de open banking necesitó un equipo de 5 desarrolladores, haciendo pruebas y corrigiendo errores en la plataforma, en un solo mercado y durante 6 meses. Intercambiamos más de 1.500 correos electrónicos y abrimos docenas de incidencias con los bancos, antes de que la solución estuviese lista para usarse.

Gestionar la solución



2.1 Probando y estableciendo conexiones

Una vez que se han establecido las conexiones, éstas deben pasar por una serie de rigurosas pruebas para asegurarse de que sean estables y funcionen correctamente.

Un proceso de prueba común sería así:

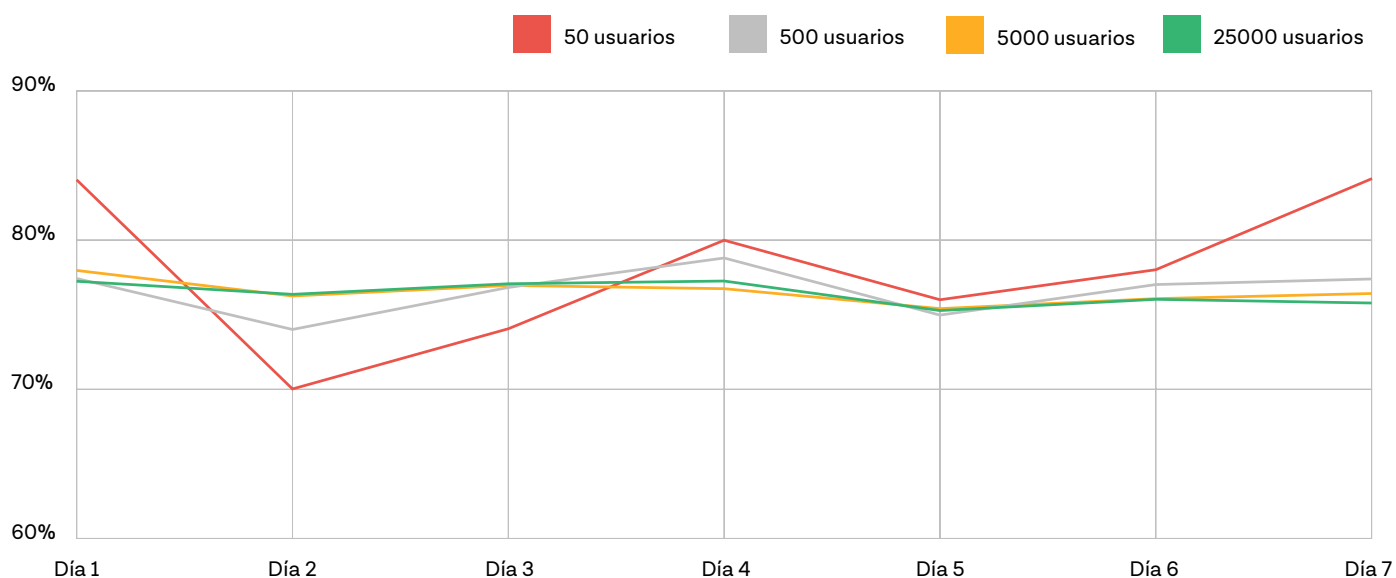
1. Abrir cuentas bancarias con todos los bancos de un país, probar la conexión con credenciales reales, y aportar feedback a los desarrolladores sobre la experiencia del usuario final.
2. Una vez completada esta ronda inicial de pruebas, trabajar en todos los casos puntuales o secundarios, con un mayor número de usuarios.
3. Registrar todos los 'journeys' de los usuarios finales, y recabar evidencias en caso de que falle alguna prueba.

Si un TPP planea dar soporte a una variedad de casos de uso, es importante tener una gran cantidad de tráfico a través de diversos tipos de clientes y casos de uso, ya que esto nos dará una imagen mucho más completa del rendimiento de una conexión. Por ejemplo, probar una conexión en una base de clientes con conocimientos digitales, capaces de superar obstáculos durante la autenticación, podría interpretarse falsamente como una conexión que funciona bien con altas tasas de conversión. En el mundo real, es posible que muchos usuarios no puedan sortear estos mismos obstáculos, lo que provocaría una gran caída en las tasas de conversión.

Esto obliga a los TPPs a pensar en todas las formas en que los clientes puedan verse afectados, y en cómo guiarlos a lo largo del proceso.

En el siguiente gráfico, usamos datos en tiempo real para ilustrar la importancia de aumentar el volumen de usuarios a la hora de probar la estabilidad de la conexión. La línea roja muestra la volatilidad de las tasas de éxito cuando hay 50 usuarios, mientras que la línea verde muestra una tasa de éxito relativamente estable una vez que el tráfico supera los 25.000 usuarios.

La tasa de éxito de una conexión se estabiliza a medida que aumenta el volumen



2.2 Operaciones diarias

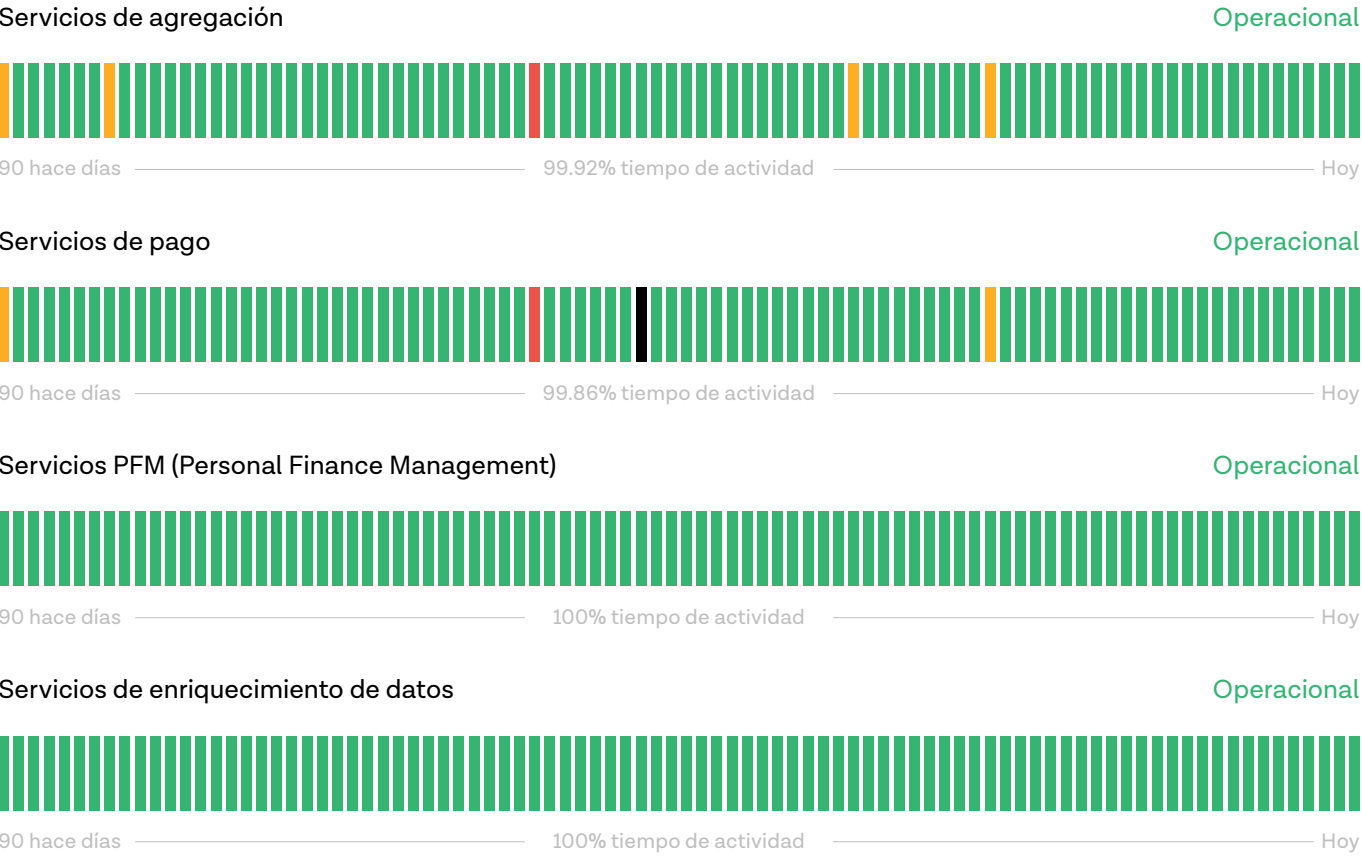
El siguiente paso es asegurarse de que las conexiones funcionen correctamente en el día a día, así como resolver problemas que surjan a largo plazo. Para hacer esto, los TPPs deben implementar un sistema para medir constantemente la calidad de cada conexión, generar alertas automáticas cuando las conexiones no cumplen con los estándares de calidad, y tener desarrolladores disponibles que estén capacitados para responder a tales situaciones.

Las alertas no siempre requieren atención inmediata, o incluso código, ya que ocasionalmente los servicios de ASPSP se caen. Sin embargo, los TPPs deberían asegurarse de identificar cada incidente y su riesgo, tener una comprensión clara de la causa del problema, e informar a los clientes cuando sea necesario.

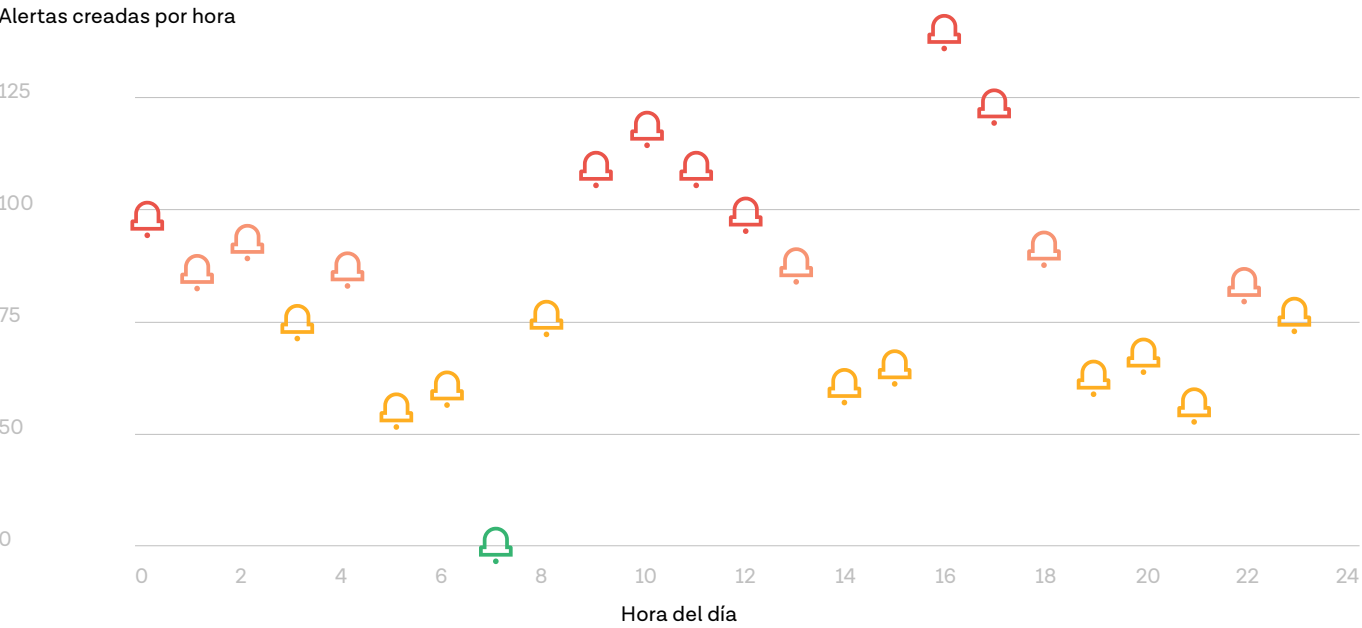
Gestionar una solución durante un largo período de tiempo, con las pruebas adecuadas y las rutinas del día a día es un proceso interminable y, a menudo, se infravalora cuando se decide crear la solución internamente.

En Tink, hemos creado exhaustivas alertas y un sistema de guardia para mantenerse al día con los constantes cambios. Nuestro sistema de alertas consta de un rango de prioridades, y unos umbrales que tienen en cuenta la gravedad del problema y el número de usuarios afectados. Tan pronto como el número de errores cruza el umbral, se envía un mensaje al equipo responsable de la API, para evaluar y priorizar en función de la gravedad del problema.

Página de estado del servicio en Tink.com



Panel de alertas

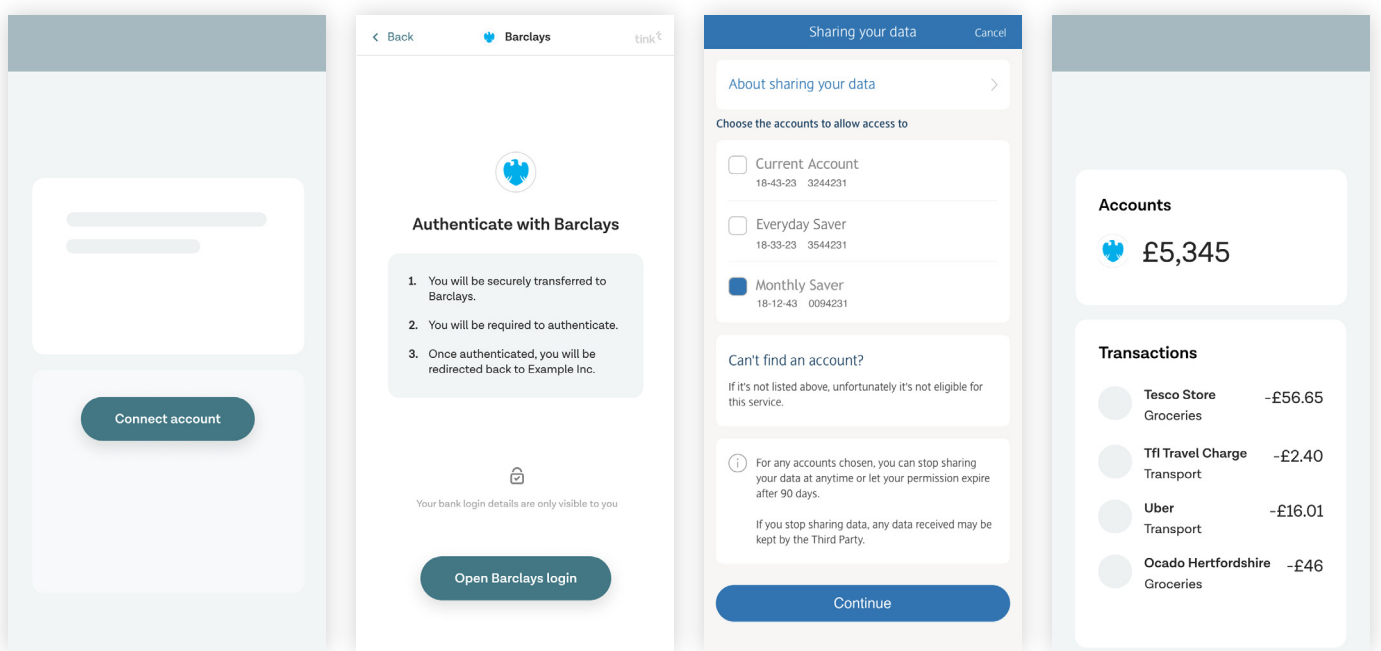


Mejorando la experiencia del usuario



Todo el tiempo y esfuerzo invertido en el establecimiento y activación de conexiones bancarias, conducen a ese punto de interacción tan importante donde los TPPs piden a los usuarios finales su consentimiento para acceder a sus cuentas bancarias. Aquí es donde entra en juego la experiencia de usuario. Proporcionar una buena experiencia de usuario requiere una combinación de conocimiento operativo de los flujos de autenticación, ocultando esa complejidad al usuario final, y haciendo que el proceso sea simple y sencillo.

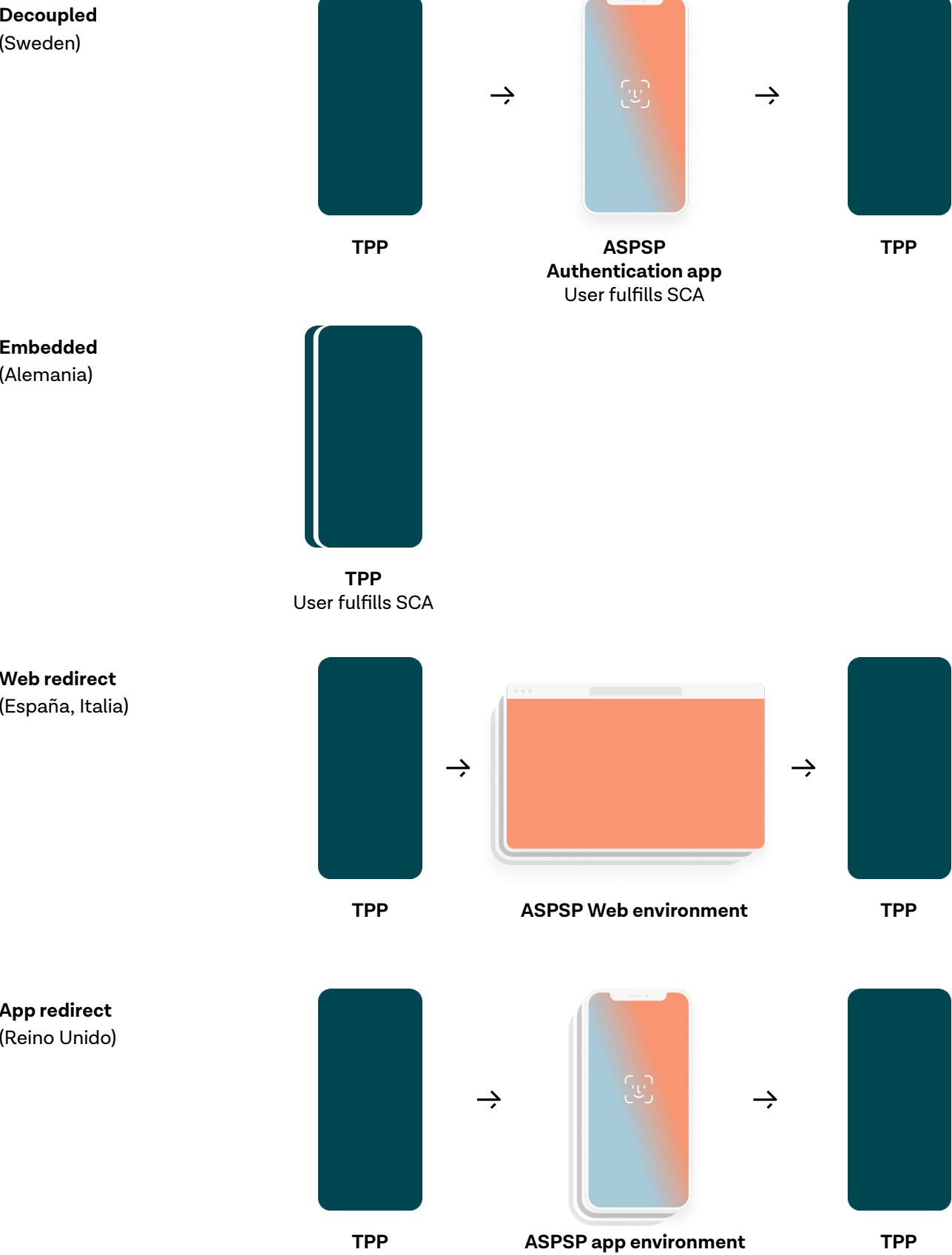
En Tink, hacemos esto a través de Tink Link, nuestro SDK front-end para administrar y optimizar la autenticación ASPSP.



El objetivo es garantizar que los usuarios finales cumplan con los requisitos de “Autenticación Reforzada de Clientes” (SCA por sus siglas en inglés), que estipulan que un usuario debe identificarse a través de dos de estos tres elementos: posesión (teléfono móvil), conocimiento (contraseña) e inherencia (biometría). Para la mayoría de los usuarios finales, esto puede parecer una simple secuencia de pantallas de inicio de sesión. La realidad es que hay bastante complejidad en segundo plano, como el tipo de conexión, el tipo de dispositivo, los países,

o los idiomas, entre otras variables. Pero quizás, la parte más compleja es que muchos pasos durante el viaje del usuario, están fuera del control de un TPP. Debido a la falta de consenso dentro de la industria sobre cómo los ASPSPs deben verificar la identidad del usuario, los TPPs a menudo necesitan crear flujos de autenticación a medida, lo que crea una cantidad asombrosa de combinaciones a considerar. Los escenarios más comunes incluyen redireccionamiento embedded, decoupled, web y app.

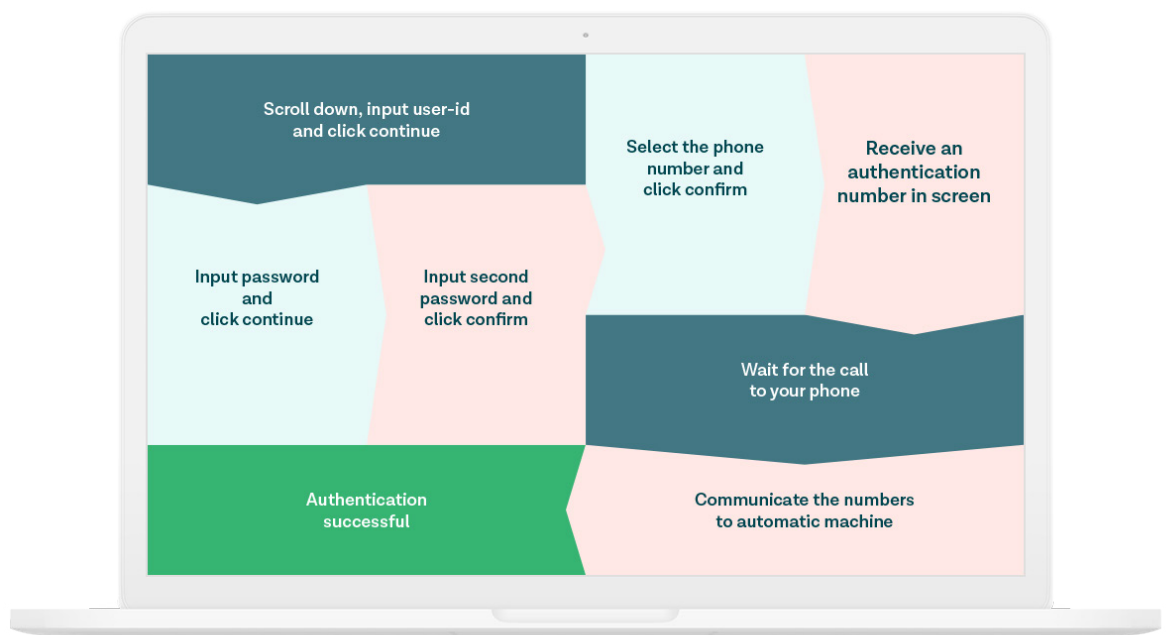
Flujos de autenticación comunes en Europa



Caso de estudio

Para explicar la complejidad a la hora de mejorar la experiencia del usuario final, veámoslo a través de un ejemplo de un cliente de Tink, que quería eliminar los procesos manuales de su onboarding. Mejorar el onboarding de nuevos usuarios es un caso de uso común del open banking, y desde Tink, hemos ayudado a varios clientes en este empeño. Autenticamos a los usuarios, obtenemos la información de su cuenta, conectamos las cuentas bancarias y ¡voilà!. Nuestros equipos dedicaron un par de meses al trabajo de integración, pero una vez que lo implementamos nos sorprendió descubrir que la tasa de conversión de los nuevos usuarios al terminar todo el proceso de onboarding, seguía siendo bajo. Entonces empezamos a profundizar en los datos para entender qué es lo que estaba pasando.

Curiosamente, la tasa de conversión de los usuarios móviles que completaron el proceso de onboarding estaba dentro de lo esperado. La caída real fue provocada cuando se comenzaba o se finalizaba el proceso de onboarding desde un ordenador. Esto se debe a que la mayoría de las instituciones financieras en el Reino Unido han realizado grandes inversiones para mejorar sus procesos bancarios en dispositivos móviles, pero sus procesos en ordenadores siguen siendo deficientes.



Como es de esperar, el resultado fue una tasa de abandono muy alta. Con esta información clave, comenzamos a recopilar flujos de inicio de sesión para cada banco en ese país. Destacamos los puntos débiles, realizamos una lluvia de ideas sobre cómo mejorarlos y participamos en conversaciones con los bancos relevantes, así como con el OBIE de Reino Unido. Después de varios experimentos, descubrimos que la mejor solución era utilizar códigos QR para redirigir a los usuarios del ordenador al móvil, y completar así el proceso de autenticación evitando todos los obstáculos en el proceso desde el ordenador.

La primera iteración de esta nueva "pantalla de transferencia de códigos QR" se implementó en pocos días. Reunimos a nuestro equipo de análisis de datos y confiamos en su veredicto: ¿mejoraron las tasas de éxito? Los resultados fueron alentadores, pero aún no cumplían con nuestras expectativas. El siguiente paso fue involucrar a los diseñadores. Nuestro equipo de diseño de producto realizó varias mejoras, desde reducir la densidad del código QR hasta proporcionar instrucciones más claras para el usuario. También eliminamos la opción del usuario a elegir entre realizar el proceso a través del ordenador o del móvil, y les pedimos que completaran el proceso de autenticación completamente en su dispositivo móvil.

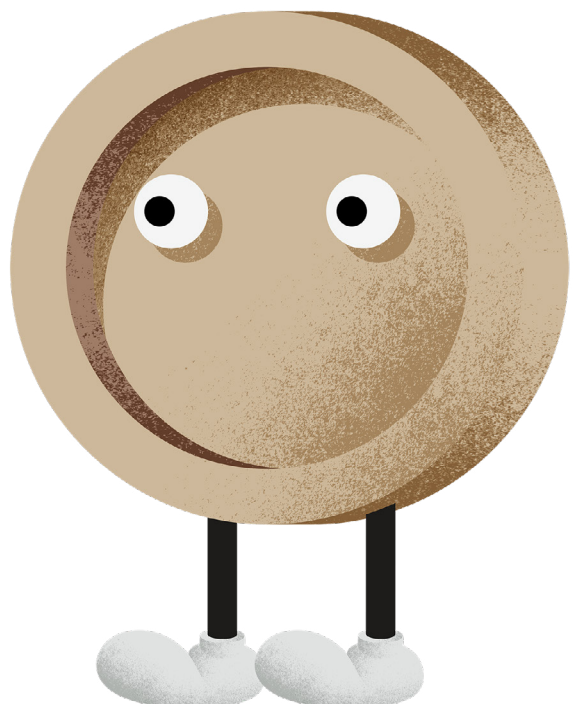
Los resultados finales fueron sobresalientes. Aquellos que utilizaron el código QR aumentaron su tasa de éxito en un 62% sobre los que utilizaron el ordenador.

Porcentaje de mejora en las tasas de éxito de extremo a extremo



Este ejemplo destaca dos cosas:

- La transición de la banca física a la digital es complicada, requiere un conocimiento profundo del mercado y, en muchos casos, soluciones únicas. Aunque esto puede parecer poco escalable, es donde nos encontramos en este momento.
- La importancia de las disciplinas multifuncionales para mejorar la experiencia del usuario. Los pilares de dicha mejora son una combinación de experiencia técnica y de diseño, y siempre con un enfoque basado en datos para comprender las dificultades experimentadas por los usuarios.



Impulsando la industria



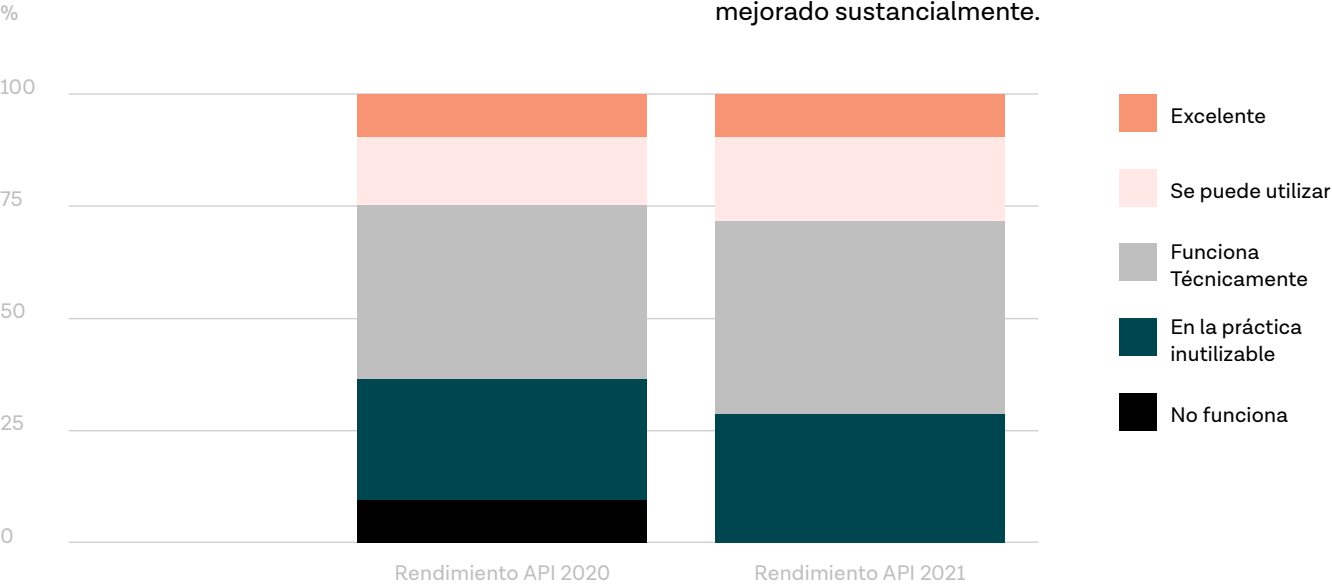
Impulsando la industria

Además del aspecto técnico del establecimiento y optimización de las conexiones, los TPPs deben también interactuar constantemente con los ASPSPs, los reguladores y las autoridades financieras. Las regulaciones como PSD2 y RTS son complejas, y los TPPs desempeñan un papel valioso al señalar los problemas a corto plazo, al responsabilizar a los ASPSPs cuando no se cumplen las regulaciones y al mantenerse enfocados en la visión a largo plazo del open banking.

A corto plazo

A corto plazo, los TPPs trabajan junto con los ASPSPs para resolver problemas que tienen un impacto inmediato, como cambios inesperados en las APIs, falta de documentación, entornos de prueba desactualizados, y caídas del servidor sin comunicación previa con los TPPs. En la mayoría de los casos, la comunicación directa con los ASPSPs es suficiente, pero en los casos en los que no se toman medidas, los TPPs tienen que escalar estos problemas a las autoridades pertinentes.

La buena noticia es que estas inversiones iniciales están empezando a dar sus frutos y, en los últimos años, el rendimiento de la API entre los ASPSPs ha mejorado sustancialmente.



El gráfico muestra el estado de las APIs PSD2 de los principales bancos en 12 países. Hacemos estas evaluaciones de forma periódica para medir las últimas mejoras en el rendimiento de la API.

- **No funciona:** la API PSD2 no existe o no funciona.
- **En la práctica inutilizable:** la API PSD2 funciona, pero el proceso de autenticación es extremadamente complejo para el usuario final, requiere varios pasos no intuitivos, múltiples SCAs y redireccionamiento web.
- **Funciona Técnicamente:** la API PSD2 funciona, pero el proceso de autenticación no ofrece redireccionamiento de aplicación a aplicación y tiene pantallas innecesarias.
- **Se puede utilizar:** la API PSD2 se puede utilizar y proporciona redirección de aplicación a aplicación. Sin embargo, el flujo de autenticación aún contiene pantallas innecesarias.
- **Excelente:** la API PSD2 ofrece redirección de aplicación a aplicación y no tiene pantallas innecesarias. Las pantallas están optimizadas para permitir que el usuario se autentique.

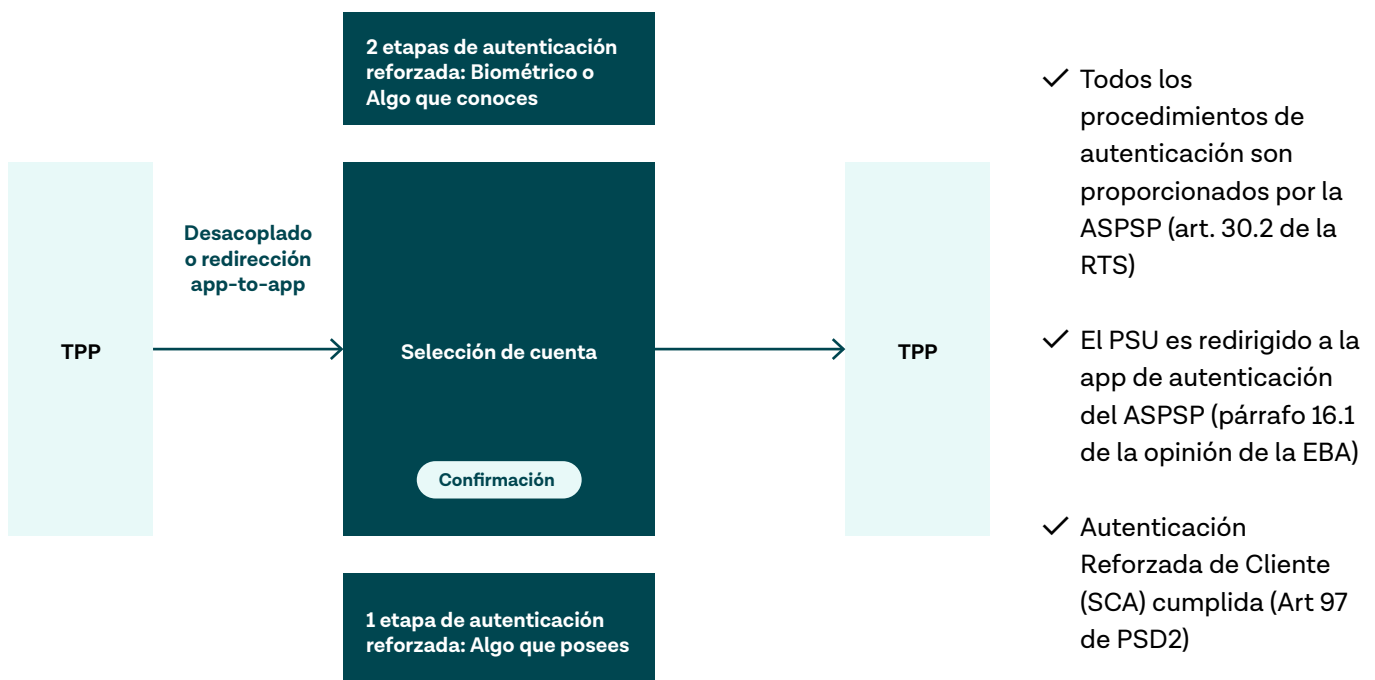
Visión a largo plazo

Las conexiones a las APIs bancarias no tiene sentido si la visión a largo plazo de una industria financiera más centrada en el cliente, competitiva e innovadora se diluye en los debates sobre regulación, tecnología y procesos. Esto requiere que los TPPs tengan una visión clara sobre la experiencia del usuario final e inviertan tiempo y recursos en hacer de este futuro una realidad.

La mejor forma de hacerlo es a través de los datos. Los TPPs deben crear una cultura de pruebas constantes, mapeando los obstáculos encontrados al conectarse a una API y compartiendo conocimientos y datos con el ASPSP.

La utilización de datos objetivos y cuantitativos sobre el impacto de los flujos de usuarios, por debajo del promedio, hace que sea más fácil entablar conversaciones constructivas con los ASPSP y los reguladores. Aunque pueda existir el dilema de que un TPP pueda beneficiarse del esfuerzo de lobbying de otros, las implicaciones a largo plazo de disponer de mejores flujos de usuarios, y experiencia del usuario final, son de gran beneficio para toda la industria.

Por ejemplo, una gran parte del lobbying de Tink, se centra en procurar que el ejemplo que mostramos a continuación se convierta en el estándar en Europa.



Con el fin de influir en la visión a largo plazo del open banking, Tink participa activamente en grupos de lobbying y asociaciones como ETPPA, PSD2 SIG, PayBelgium, Fintech Norway, UK Finance y la Asociación Europea de Pagos.

Conclusión

Si hay una conclusión clave de la experiencia de Tink, sería que desarrollar la conectividad es una inversión estratégica a largo plazo. La industria está evolucionando muy rápido y mantenerse al día con los cambios requiere foco y recursos.

Con Tink, no tienes que preocuparte de nada. Nuestra plataforma de open banking te permite conectarte con más de 3.400 bancos e instituciones en toda Europa y obtener datos financieros enriquecidos y categorizados, a través de una única API. Nos centramos en la conectividad para que tú puedas centrarte en la innovación y en ofrecer servicios financieros de calidad.

¿Quieres saber más sobre cómo puedes acceder a datos financieros en tiempo real? Nuestros expertos están encantados de responder a tus preguntas, escríbenos a:

partnerships@tink.com



